
République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur

Université 8 mai 1945 Guelma

Faculté des sciences et de la Technologie

Département d'Electronique et Télécommunications

Mémoire de fin d'études

Master



Domaine : **Sciences et Technologie**

Filière : **Electronique**

Spécialité : **Instrumentation**

L'empreinte palmaire multispectrale

Présenté par :

Zouied Nasreddine

sous Direction de :

Mr. Benjoudi Salim

Octobre 2020

Dédicace

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs : Marwā et Zina.

Pour leurs encouragements permanents, et leur soutien moral,

A mon cher frère, Karim Et Abd El Aziz pour leur appui et leur encouragement,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

A mes amis, Moussa Et Fateh et mokhtar.

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infailible,

Merci d'être toujours là pour moi.

Remerciement

*Tout d'abord, je remercie Dieu pour ma conciliation pour
terminer ce travail.*

*Je remercie tous les membres de ma famille pour leur soutien
financier et moral.*

*Je voudrais adresser toute ma reconnaissance à mon
encadreur de thèse, Mr. Bendjoudi salim, pour toute l'aide
qu'il m'a apportée au cours de la réalisation de ce travail.*

*Ses connaissances scientifiques et ses nombreux
encouragements ont constitué pour moi un apport très
important.*

*Je désire aussi remercier les membres de jury pour avoir
accepté d'être rapporteurs de ma thèse*

*Enfin je tiens à remercier tous ceux qui ont contribué de près
ou de loin à la réalisation de ce travail.*

Résumé :

Au cours des deux dernières décennies, l'identification personnelle est devenue une exigence importante et fondamentale dans plusieurs applications telles que : les systèmes de surveillance, de contrôle et d'identification ... etc., et cela est dû à plusieurs raisons telles que l'usurpation d'identité, les crimes, les vols, etc.

Afin de garantir la sécurité et la confidentialité, ces systèmes effectuent des traitements sur l'identité des personnes en fonction de plusieurs caractéristiques : physiques et biologiques, et ils se sont avérés être des techniques efficaces, plus sûres et plus fiables pour l'identification automatique des personnes, ce qui les a rendus bien meilleurs que les systèmes de reconnaissance traditionnels tels que les mots de passe, les cartes à puce ... etc.

En tant que modalité biométrique importante, l'empreinte palmaire a attiré beaucoup d'attention, car celle-ci présente des avantages tels que sa rapidité, sa convivialité, son faible coût et sa grande précision, ce qui a considérablement augmenté son utilisation dans l'identification des personnes et a été largement utilisée dans la société, en particulier dans les systèmes administratifs et bancaires.

Toutefois, les systèmes d'authentification par l'empreintes palmaires peuvent encore être améliorés du point de vue précision et la possibilité d'attaques par usurpation. Une solution à ces problèmes peut être l'imagerie multispectrale, qui capte une image dans diverses bandes spectrales. Chaque bande spectrale met en évidence les caractéristiques spécifiques et distinctives de la paume, ce qui permet de recueillir plus d'informations pour améliorer la précision et la capacité de non appropriation de ces systèmes d'empreintes palmaires.

Dans notre travail, nous présentons l'empreinte palmaire multispectrale, ses différentes caractéristiques, un exemple de système d'authentification, et une comparaison de certaines méthodes d'authentification.

على مدى العقدين الماضيين، أصبح تحديد الهوية الشخصية مطلبًا مهمًا وأساسيًا في العديد من التطبيقات مثل: أنظمة المراقبة والتحكم وتحديد الهوية. هذا يرجع إلى عدة أسباب مثل اغتصاب الهوية والجريمة والسرقة وما إلى ذلك. من أجل ضمان الأمن والسرية، تقوم هذه الأنظمة بإجراء علاجات على هوية الأشخاص وفقًا لعدة خصائص: جسدية وبيولوجية، وقد أثبتت أنها تقنيات فعالة وأكثر أمانًا وموثوقية للتعرف التلقائي على الأشخاص، مما جعل أفضل بكثير من أنظمة التعرف التقليدية مثل كلمات المرور والبطاقات الذكية وما إلى ذلك. كطريقة بيومترية مهمة، جذبت بصمة النخيل درجة كبيرة من الاهتمام، حيث أنها تتمتع بمزايا مثل السرعة وسهولة الاستخدام والتكلفة المنخفضة والدقة العالية، مما زاد بشكل كبير من استخدامها في تحديد الأشخاص وكانت على نطاق واسع تستخدم في المجتمع، وخاصة في الأنظمة الإدارية والمصرفية.

ومع ذلك، لا يزال من الممكن تحسين أنظمة المصادقة ببصمة اليد من حيث الدقة وإمكانية هجمات الانتحال. قد يكون أحد الحلول لهذه المشاكل هو التصوير متعدد الأطياف، الذي يلتقط صورة في نطاقات تردد طيفية مختلفة. يسلط كل نطاق طيفي الضوء على الخصائص المحددة والمميزة لراحة اليد، مما يسمح بجمع المزيد من المعلومات لتحسين الدقة والقدرة على عدم العبث لأنظمة طباعة الكف هذه.

في عملنا، نقدم بصمة النخيل متعددة الأطياف، وخصائصها المختلفة، ومثال لنظام المصادقة ومقارنة بين بعض طرق المصادقة.

Abstract:

Over the last two decades, personal identification has become an important and fundamental requirement in several applications such as: surveillance, control and identification systems. This is due to several reasons such as identity usurpation, crime, theft, etc.

In order to guarantee security and confidentiality, these systems carry out treatments on the identity of people according to several characteristics: physical and biological, and they have proven to be effective, safer and more reliable techniques for the automatic identification of people, which has made them much better than traditional recognition systems such as passwords, smart-cards, etc.

As an important biometric modality, the palm print has attracted a significant degree of attention, as it has advantages such as speed, user-friendliness, low cost and high accuracy, which has significantly increased its use in the identification of persons and has been widely used in society, particularly in administrative and banking systems.

Nevertheless, palmprint authentication systems can still be improved in terms of accuracy and the possibility of spoofing attacks. One solution to these problems may be multispectral imaging, which captures an image in various spectral bandwidths. Each spectral band highlights the specific and distinctive characteristics of the palm, allowing more information to be collected to improve the accuracy and the non-tampering capability of these palm print systems.

In our work, we present the multispectral palm print, its different characteristics, an example of an authentication system, and a comparison of some authentication methods.

TABLE DE MATIRES

Introduction générale

1	Introduction	1
2	Un bref aperçu historique	2
3	Contexte et motivations	2

CHAPITRE I

1 La biométrie

1.1	Introduction	6
1.2	Définition	6
1.3	Pourquoi la biométrie ?	7
1.4	Les caractéristiques d'une modalité biométrique	7
1.5	Modalités biométriques	7
1.5.1	Modalités Morphologiques	9
1.5.1.1	Empreinte digitale	10
1.5.1.2	L'empreinte palmaire	11
1.5.1.3	Les articulations des doigts (FKP)	12
1.5.1.4	La géométrie de main	12
1.5.1.5	Le visage	13
1.5.1.6	L'iris	13
1.5.1.7	La rétine	14
1.5.2	Modalités comportementales	14
1.5.2.1	La signature dynamique	14
1.5.2.2	La dynamique de frappe au clavier	15
1.5.2.3	La voix (Reconnaissance vocale)	15
1.5.2.4	La démarche	16
1.5.3	Modalités biologiques	17
1.5.3.1	L'AND	17
1.5.3.2	L'oreille	18
1.5.3.3	Les veines	18
1.6	Etude comparative entre les modalités biométriques	19
1.7	Les types de systèmes biométriques	21
1.7.1	Les systèmes multimodaux	21
1.7.2	L'architecture des systèmes multimodaux	21
1.8	La fusion	22
1.8.1	Les niveaux de fusion	23
1.8.2	La fusion pré-classification	24
1.8.3	La fusion post-classification	24
1.9	Principe de fonctionnement d'un système biométrique	25
1.10	Domaine d'Applications	25
1.10.1	Service public	25
1.10.2	Pouvoir judiciaire	26
1.10.3	Secteurs des banques	26

TABLE DE MATIRES

1.11	Conclusion	26
CHAPITRE II		
2	L'Empreinte Palmaire	
2.1	Introduction	27
2.2	Reconnaissance par empreintes palmaires	27
2.2.1	Définition de l'empreinte palmaire	28
2.2.2	Caractéristique des empreintes palmaires	29
2.2.2.1	Caractéristiques géométriques	29
2.2.2.2	Les lignes principales	30
2.2.2.3	Les rides (plis secondaires)	30
2.2.2.4	Les points des références	30
2.2.2.5	Les caractéristiques de minutie	31
2.3	Les différentes empreintes palmaires	32
2.3.1	Empreinte palmaire avec contact	32
2.3.2	Empreinte palmaire sans contact	33
2.4	Les différents types d'images	35
2.4.1	La reconnaissance d'empreintes palmaires à haute résolution	35
2.4.2	La reconnaissance d'empreintes palmaires à basse résolution	35
2.4.3	La reconnaissance d'empreintes palmaires à trois dimensions	36
2.4.4	La reconnaissance d'empreintes palmaires multispectrale	36
2.5	Le système de reconnaissance palmaire	36
2.6	Conclusion	36
CHAPITRE III		
	Système d'authentification de l'empreinte palmaire multispectrale	39
3.1	Introduction	39
3.2	L'architecture du système d'authentification de l'empreinte palmaire multispectrale	41
3.3	Algorithme d'extraction du ROI	44
3.4	Fusion d'images	47
3.5	Analyse multispectrale des images d'empreintes palmaires	49
3.5.1	Extraction et appariement des caractéristiques	49
3.5.2	Programme de fusion au niveau des scores	51
3.6	Conclusion	53
	Bibliographie	54

Liste de Figures

Chapitre I

Figure 1.1 Quelques Modalités Biométrie	8
Figure 1.2 Classification d'un certain nombre de modalités biométrique	10
Figure 1.3 L'empreinte digitale	11
Figure 1.4 Système biométrique basé sur les empreintes palmaires	11
Figure 1.5 Système biométrique basé sur les articulations des doigts	12
Figure 1.6 Lecteur de la forme de la main	12
Figure 1.7 La reconnaissance de visage [9]	13
Figure 1.8 L'iris	13
Figure 1.9 La rétine	14
Figure 1.10 Dynamique de signature	15
Figure 1.11 Dynamique de frappe au clavier	15
Figure 1.12 La voix	16
Figure 1.13 Système biométrique basé sur la démarche	17
Figure 1.14 Exemple de l'ADN	17
Figure 1.14 Empreintes d'oreille	18
Figure 1.16 Système biométrique basé sur les veines	18
Figure 1.17 Architecture de fusion en parallèle	22
Figure 1.18 Architecture de fusion en série (incrémentale ou séquentielle)	23
Figure 1.19 Les différents niveaux de fusion	23
Figure 1.20 Schéma de fusion au niveau du capteur	24
Figure 1.21 Schéma de fusion au niveau de l'extraction des caractéristiques	24
Figure 1.22 Schéma de fusion au niveau de la décision	25
Figure 1.23 Schéma de fusion au niveau de scores. [10]	25

Chapitre II

Figure 2.1	Paume de la main	28
Figure 2.2	Caractéristiques géométriques de palmaire	29
Figure 2.3	Les plis de flexions de la paume de la main	30
Figure 2.4	Les points de référence de l’empreinte palmaire	31
Figure 2.5	Minuties de palmaire	31
Figure 2.6	Le dispositif d’acquisition CCD bidimensionnel à base contact: (a) le dispositif; (b) exemple d'acquisition. [10]	33
Figure 2.7	Vue extérieure du système d’acquisition d’images palmaire et main posée sur la plateforme [11]	34
Figure 2.8	Le dispositif d’acquisition d’empreintes palmaires [12].	34
Figure 2.9	L'empreinte palmaire est présente dans une image haute résolution	35
Figure 2.10	L'empreinte palmaire est présente dans une image basse résolution[13].	36
Figure 2.11	Dispositif d'acquisition d'images 3D basé sur la lumière et un exemple d’image de palmaire 3 D	36
Figure 2.12	Étapes d'identification du système palmaire	37

Chapitre III

Figure 3.1	Anatomie de la peau en coupe transversale	41
Figure 3.2	La structure interne du dispositif d'acquisition multispectrale de l'empreinte palmaire	43
Figure 3.3	Prototype du système d'empreinte palmaire multispectral.	43
Figure 3.4	Un échantillon typique d'empreinte palmaire multispectrale. (a) Bleu ; (b) Vert ; (c) Rouge ; (d) NIR, le carré blanc est la région d'intérêt	44
Figure 3.5	Les ROIs de la Fig. 3.4. (a) Bleu ; (b) Vert ; (c) Rouge ; (d) NIR	44
Figure 3.6	Les principales étapes du prétraitement. (a) Image originale, (b) image binaire, (c) le suivi des limites, (d) la construction d'un système de coordonnées, (e) l'extraction de la partie centrale en tant que sous-image, et (f) le résultat du prétraitement	46
Figure 3.7	Schéma du système en ligne de vérification	47
Figure 3.8	Carte des caractéristiques extraites de la Figure 3.5. Les différentes valeurs de gris représentent des caractéristiques d'orientation différentes. Les trois cartes dans chaque colonne de gauche à droite sont toutes extraites du même ROI mais en utilisant trois paramètres différents. Ainsi, a-c est extrait du bleu ; d-f est extrait du vert ; et g-i est extrait du rouge. Les cartes de la quatrième colonne, j-l, sont	51
Figure 3.9	Un exemple de fusion de la somme des scores	52
Figure 3.10	Caractéristiques de chevauchement entre différents spectres. (Les pixels noirs représentent les éléments qui se chevauchent, tandis que les pixels blancs représentent les éléments qui ne se chevauchent pas)	53

Liste de Tableaux

Chapitre I

Tableau 1.1 Comparaison entre les techniques biométriques [6]	9
Tableau 1.2 Comparaison entre les modalités biométriques	20

Chapitre III

Tableau 3.1 Représentation en bits du codage d'orientation	51
---	-----------

Liste des acronymes

ADN : Acide Désoxyribo Nucléique.

CCD : Récepteurs à transferts de charge ("Charge Coupled Device").

DWT: La transformée en ondelettes discrète ("Discrete Wavelet Transform").

FKP : Empreintes des articulations des doigts ("Finger-Knuckle-Print").

LBP-HF: Local Binary Pattern Histogram Fourier Features.

LED: Diode électroluminescente ("Light- Emitting Diode").

NIR : Near-infrared.

NFS : (Numération Formule Sanguine).

PIN : Numéro d'Identification Personnel ("Personnal Identification Number").

ROI : Région d'intérêt ("Region Of Interest").

TPTSR: Two-Phase Test Sample Representation.

1. Introduction

La biométrie est une technologie en pleine expansion qui est de plus en plus utilisée dans notre vie quotidienne. Elle vise à établir l'identité d'une personne de la manière la plus fiable possible en utilisant ses caractéristiques corporelles afin de garantir la sécurité des personnes dans les lieux publics. Finalement, nous présentons les avantages ainsi que les défis de la modalité manuelle [1].

Etymologiquement, le terme biométrie se compose du terme « bio » (du grec ancien βίος qui signifie « vie ») et du terme « métrie » (du grec ancien μέτρον, qui signifie « mesure »). Ainsi, dans son premier sens, la biométrie signifie « mesure du vivant » et fait référence à l'étude scientifique et quantitative du monde vivant et des êtres vivants. La biométrie fait maintenant surtout référence à l'ensemble des techniques utilisées pour identifier un individu grâce à certaines de ses caractéristiques physiques, biologiques, et comportementales.

2. Un bref aperçu historique

La littérature scientifique sur la mesure quantitative de l'homme pour l'identification pure remonte aux années 1870 et au système de mesure d'Alphonse Bertillon [2]. Le système de mesures corporelles de Bertillon, y compris des mesures telles que le diamètre du crâne et la longueur du bras et du pied, a été utilisé aux États-Unis pour identifier les prisonniers jusqu'aux années 1920. Henry Faulds, William Herschel et Sir Francis Galton ont proposé l'identification quantitative par les empreintes digitales et les mesures faciales dans les années 1880. Le développement des techniques de traitement des signaux numériques dans les années 1960 a immédiatement conduit à travailler à l'automatisation de l'identification humaine. Les systèmes de reconnaissance d'empreintes digitales et de la voix ont été parmi les premiers à être explorés. Le potentiel d'application de cette technologie au contrôle d'accès de haute sécurité, aux serrures personnelles et aux transactions financières a été reconnu au début des années 1960. Les années 1970 ont vu le développement et le déploiement de systèmes de géométrie de la main, le début d'essais à grande échelle et un intérêt croissant pour l'utilisation par les gouvernements de ces technologies. Les systèmes de vérification de la rétine et de

Introduction générale

la signature sont apparus dans les années 1980, suivis par les systèmes de face. Les systèmes de reconnaissance de l'iris ont été développés dans les années 1990.

L'authentification biométrique a fait l'objet de nombreuses recherches de pointe dans les domaines suivants le contexte des applications de sécurité. L'augmentation du financement industriel et gouvernemental à ce sujet en fait un domaine en pleine expansion. Il existe plusieurs traits biométriques (p. ex. l'ADN, et l'empreinte palmaire) qui peuvent être exploitées dans les systèmes d'authentification. Chacun a ses propres avantages et inconvénients, et il n'y a donc pas une seule caractéristique optimale qui satisfasse toutes les applications et exigences [2]. En conséquence, en fonction des contraintes et des conditions du mode opérationnel, une ou plusieurs caractéristiques biométriques peuvent être employées. Il y a plusieurs avantages qui font que l'authentification par empreinte palmaire est plus appropriée pour les applications du monde réel.

3. Contexte et motivations

La sécurité et la sûreté des personnes, des biens et des informations doivent être garanties, et présentent en fait l'une des préoccupations majeures de nos sociétés, en particulier après la grande propagation du terrorisme dans le monde entier. En fait, les personnes souhaitant traverser des frontières doivent prouver leur identité à l'aide de leur passeport. Les personnes souhaitant traverser des bâtiments ou des établissements d'enseignement doivent valider leur carte d'accès. Les personnes souhaitant utiliser les services bancaires doivent se connecter avec un identifiant (login) et un mot de passe. Néanmoins, ces méthodes traditionnelles montrent de grandes faiblesses pour la vérification de l'identité. En effet, l'identité d'une personne est directement liée à celle qu'elle possède (passeport, carte d'accès, etc.) ou/et qu'elle connaît (mot de passe, code PIN, etc.) [3].

Toutefois, les codes PIN et les mots de passe peuvent être oubliés ou compromis et les cartes d'accès peuvent être falsifiées ou dupliquées, ce qui entraîne une usurpation d'identité.

À cet égard, les experts recherchent une technologie permettant de résoudre ces problèmes en donnant plus de commodité et de confort aux personnes en leur assurant un accès hautement sécurisé, en liant l'identité d'une personne à ce qu'elle est et non à celle qu'elle possède ou savoir. La biométrie est la technologie la plus appropriée pour

Introduction générale

la vérification et/ou l'identification de personne en utilisant leurs caractéristiques physiologiques, notamment biologiques, caractéristiques morphologiques et comportementales. Cette technologie crée des données d'identité dont le vol est plus difficile et accroît donc la confiance de l'utilisateur à mesure que la présence physique est nécessaire lors de l'identification.

Historiquement parlant, la biométrie est apparue pour succéder à la technique anthropométrique (Techniques de mesure des proportions morphologiques pratiquées sur le corps humain.) de reconnaissance. La plus ancienne était l'analyse par empreinte digitale, utilisée par la police pour l'identification des personnes. Dans le 19^{ème} siècle, un criminologue français a inventé une méthode scientifique appelée « anthropologie médico-légale » pour identifier les criminels sur la base de mesures de leurs caractéristiques physiologiques.

En fait, cet usage n'a jamais été abandonné et les empreintes digitales sont encore utilisé pour une identification criminelle. De nos jours, la puissance croissante des ordinateurs peut contribuer à la reconnaissance individuelle grâce à des algorithmes informatiques complexes utilisé dans les appareils. Par conséquent, la biométrie est en réalité une science en développement qui vise à identifier les individus au moyen de systèmes technologiques, en utilisant leurs caractéristiques corporelles.

Elle ne se limite plus aux empreintes digitales et à l'identification criminelle. Nombreuses d'autres modalités sont utilisées aujourd'hui, à savoir l'iris, le visage, la forme de la main, la démarche, etc. pour des applications d'accès de contrôle. L'utilisation de cette technique est répandue dans le monde entier et prend une place importante dans notre vie quotidienne. Dans les années à venir, la biométrie sera probablement l'une des techniques les plus utilisées, tout d'abord pour identifier ou authentifier des particuliers et ensuite de contrôler l'accès aux espaces publics tels que les banques, aéroports, hôpitaux, musées, gares ferroviaire et routière.

Au début, différents systèmes biométriques unimodaux basés sur une modalité biométrique unique ont été mis au point. Bien que les techniques biométriques unimodales promettent d'être très efficient, cependant, nous ne pouvons pas garantir un excellent taux de reconnaissance. En effet, ils présentent trois limitations principales, qui sont les suivantes : limitation en termes de performances, limitation en termes d'universalité d'utilisation et limitation en termes de détection de fraude. La première

Introduction générale

limitation concerne les performances de reconnaissance dues à d'éventuelles variations des modalités biométriques lors de leur acquisition ou aussi naturellement.

Par exemple, dans le cas de la biométrie faciale, le visage varie selon les expressions, les conditions d'éclairage et les positions de capture. En effet, il n'est pas possible de trouver deux images identiques correspondant à la même personne. Cette variabilité des caractéristiques biométriques peut nuire aux performances de reconnaissance d'identité. La deuxième limitation est attribuée à la non-universalité de certaines modalités biométriques.

Cela signifie qu'un sujet peut ne pas posséder certaines modalités pour être authentifié ou peut ne pas disposer d'une modalité suffisamment informative permettant leur vérification d'identité.

Par exemple, une personne muette ne peut pas utiliser un système biométrique vocal ou une personne handicapée ne peut pas utiliser un système biométrique de démarche. Par conséquent, certains systèmes biométriques sont inaccessibles pour ces sujets, et ils peuvent être exclus si aucune autre solution est offerte.

En ce qui concerne la troisième limitation, elle concerne la détection des fraudes. En fait, la fraude ou le vol d'identité est un problème qui se produit assez souvent. La biométrie a réduit ce problème (puisque'il est plus facile de falsifier un mot de passe ou un papier d'identité que de reproduire une main ou un visage), mais ne l'a pas éradiqué. Il est possible, par exemple, de voler des empreintes digitales (car elles laissent des traces) ou de les reproduire (en utilisant du silicone).

Toutes ces limitations peuvent être résolues ou supprimées en utilisant plusieurs modalités biométriques appelés systèmes biométriques multimodaux. Dans ce contexte, les œuvres présentées dans cette thèse sont localisés. Différentes approches multimodales sont proposées ici, en utilisant différentes fusions multi-types qui sont multi-représentations, multi-biométriques et des fusions multi-instances pour les modes d'identification et de vérification. Ces approches reposent essentiellement sur la l'empreinte palmaire. En réalité, notre motivation à utiliser cette modalité est due à la popularité de la biométrie de la main. Comparé à d'autres modalités biométriques, la main a plusieurs avantages qui font que l'authentification par les traits de la main sont plus appropriée pour les applications du monde réel.

Avantages :

i) Les dispositifs d'acquisition des empreintes palmaires sont simples et peu coûteux.

Introduction générale

- (ii) Les informations sur les mains peuvent être extraites à l'aide d'images à basse et haute résolution ;
- (iii) Leur caractère discriminatoire y compris les crêtes et les plis ;
- (iv) La vaste région d'intérêt ;
- (v) Les propriétés uniques et fiables ;
- (vi) Peu affecté par l'âge ; et

Chapitre I

La Biométrie

1.1. Introduction :

La biométrie est une alternative aux deux précédents modes d'identification. Elle consiste à identifier une personne à partir de ses caractéristiques physiques ou comportementales. Le visage, les empreintes digitales, les empreintes palmaires, l'iris, etc. sont des exemples de caractéristiques physiques. La voix, l'écriture, le rythme de frappe sur un clavier, etc. sont des caractéristiques comportementales. Ces caractéristiques, qu'elles soient innées comme les empreintes digitales ou bien acquises comme la signature, sont attachées à chaque individu et ne souffrent donc pas des faiblesses des méthodes basées sur une connaissance ou une possession.

En effet, un attribut physique ou comportemental ne peut être oublié (cf. le slogan de Nuance [1] : « No PIN to remember, no PIN to Forget ») ou Perdue. En général, ils sont très difficiles à « deviner » ou à « voler » ainsi qu'à « dupliquer » [2].

Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans notre société. Notre identité est vérifiée quotidiennement par de multiples organisations : lorsque nous utilisons notre carte bancaire, lorsque nous accédons à notre lieu de travail, lorsque nous nous connectons à un réseau informatique, etc.

La biométrie tend à réaliser deux buts importants dans notre vie courante. Le premier but est de garantir la sécurité en éliminant le doute sur l'identité d'une personne et le second est de faciliter l'identification des individus. En effet, la biométrie est de plus en plus préférée par rapport aux méthodes traditionnelles impliquant les mots de passe ou les badges [3].

1.2. Définition :

La biométrie est composée de deux termes : bio / métrie c'est la « mesure du vivant ». Elle est une technique globale visant à établir l'identité d'une personne en mesurant une ou plusieurs de ses caractéristiques physiologiques ou comportementales. Il peut y avoir plusieurs types de caractéristiques, les unes plus fiables que d'autres, mais toutes doivent être *infalsifiables* et *uniques* pour pouvoir être représentatives d'un et un seul individu. La biométrie consiste à vérifier ou déterminer l'identité d'un individu à

partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la voix) ou morphologiques (comme l'empreinte digitale ou l'empreinte palmaires).

1.3. Pourquoi la biométrie ?

Les arguments pour la biométrie se résument en 2 catégories :

Praticité : Les mots de passe comme les cartes de crédit, les cartes de débit, les cartes d'identité ou encore les clés peuvent être oubliés, perdus, volés et copiés.

De son côté la biométrie serait immunisée contre ce genre de maux en plus qu'elle serait simple et pratique, car il n'y a plus ni cartes ni mots de passe à retenir. La biométrie serait capable de réduire, le crime.

La biométrie est basée sur l'analyse de données liées à l'individu et peut être classée en trois grandes catégories :

- **L'analyse morphologique** : les empreintes palmaires, les empreintes digitales, la forme de la main, l'iris, les traits du visage, le réseau veineux de la rétine.
- **L'analyse biologique** : l'ADN, le sang, la salive, l'urine, l'odeur, la thermographie.
- **L'analyse comportementale** : la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de signature, la manière de marcher. [4]

1.4. Les caractéristiques d'une modalité biométrique :

Les caractéristiques 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 : modalités biologiques, comportementales et morphologiques. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.). La biométrie comportementale se base sur l'analyse des comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.). La biométrie morphologique se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et uniques (empreinte palmaire, digitale, visage, etc.). Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut

être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes [5] :

- **Universalité** : toutes les personnes à identifier doivent la posséder,
- **Unicité** : l'information doit être la plus différente possible entre les différents individus,
- **Permanence** : l'information collectée doit être présente pendant toute la vie d'un individu,
- **Collectabilité** : l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons,
- **Acceptabilité** : acceptation par les utilisateurs.

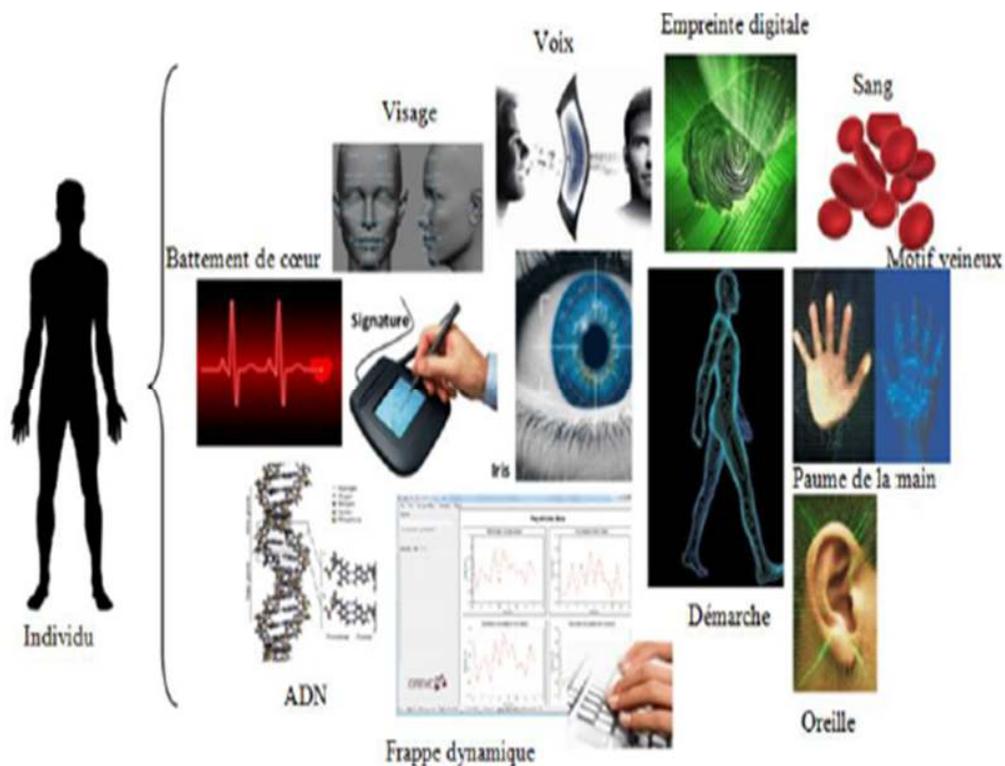


Figure 1.1 : Quelques modalités biométrie

Biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Circonvension
DNA	Haute	Haute	Haute	Faible	Haute	Faible	Faible
Oreille	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Haute	Moyenne
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Haute
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible		Moyenne
Géométrie Main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veine Main	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Haute	Faible	Faible
Frappe Clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Faible	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Tableau 1.1 : Comparaison entre les modalités biométriques [6].

1.5. Les modalités biométriques :

De nombreuses méthodes biométriques peuvent être utilisées dans divers secteurs, elles ont été classées en trois classes différentes selon leurs caractéristiques comme suit :

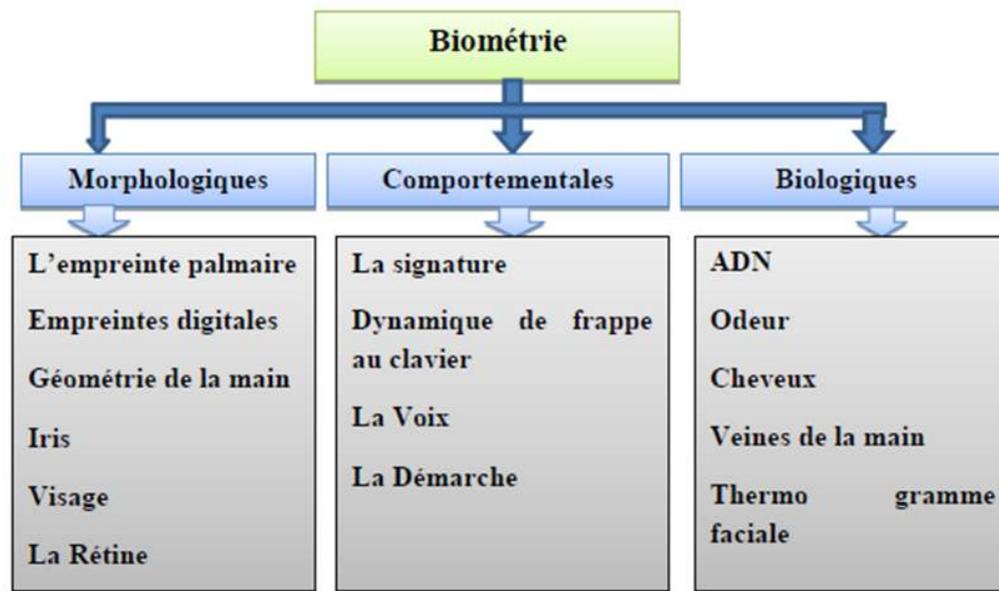


Figure 1.2 : Classification d'un certain nombre de modalités biométriques

1.5.1. Modalités morphologiques :

Cette catégorie comprend la paume de la main ou les empreintes digitales, la forme de la main, traits du visage et l'iris, etc. [9]

1.5.1.1. Empreinte digitale :

L'identification à l'aide des empreintes digitales est l'une des premières techniques biométriques qui se base sur le fait que chaque personne a des empreintes uniques. Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties [7].

Il existe plusieurs types de minuties :

Lac, bifurcation, delta ou impasse...etc. Ce type de technique biométrique est utilisé par les institutions financières pour leurs clients et on le trouve aussi dans les hôpitaux, les écoles et les aéroports... etc. [8].

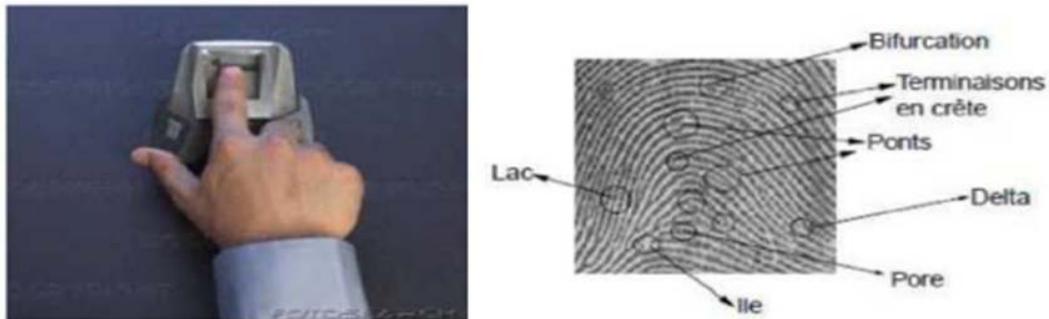


Figure 1.3 : L’empreinte digitale [8]

1.5.1.2. L’empreinte palmaire :

Les systèmes à base de l’empreinte palmaire utilisent la surface intérieure de la paume pour identifier ou vérifier les personnes. Ils sont convenables, assez acceptables, de sécurité et de protection modérées, et sont généralement acceptables. Ils sont utilisés pour le contrôle physique et logique. On les trouve principalement dans les aéroports et les entreprises à sensibilité moyenne etc.



Figure1.4 : Système biométrique basé sur les empreintes palmaires

1.5.1.3. les articulations des doigts (FKP) :

C'est une technologie biométrique basée sur la surface arrière du doigt, Dans un système biométrique FKP, un individu est vérifié par l'extraction des lignes, des plis et de la texture sur l'impression de jointure qui se trouvent à proximité des articulations des doigts. Elle est considérée comme une technique biométrique acceptable.

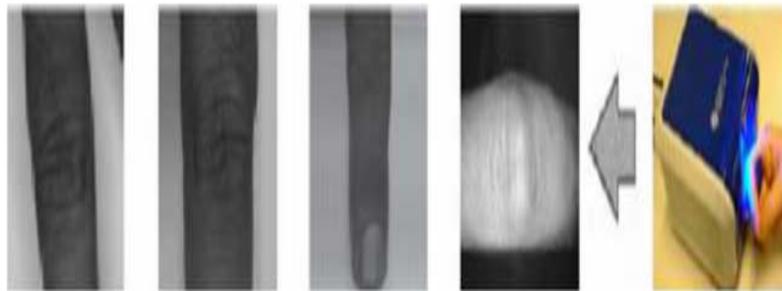


Figure 1.5: système biométrique basé sur les articulations des doigts.

1.5.1.4. La géométrie de la main :

La biométrie par la forme de la main est une technologie populaire qui est largement employée pour le contrôle d'accès physique ou le pointage horaire. Le système prend une photo de la main et examine 90 caractéristiques, y compris la forme tridimensionnelle de la main, de la longueur et de la largeur des doigts et de la forme des articulations. Pour utiliser la géométrie de la main, l'utilisateur place sa main sur une platine possédant des guides pour positionner les doigts. Sa subtilité le rend acceptable mais cela peut poser problème dans de rares situations familiales.



Figure 1.6 : Lecteur de la forme de la main

1.5.1.5. Le visage :

Il n'y a rien de plus naturel que d'utiliser le visage pour reconnaître une personne. La fonction biométrique est peut-être la plus populaire. Utilisé par les humains pour créer une identité personnelle, d'en dégager certaines particularités. Selon le système utilisé, l'individu doit être positionné devant l'appareil ou peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier de référence.



Figure 1.7 : La reconnaissance de visage [9]

1.5.1.6. L'iris :

L'iris est la région annulaire située entre la pupille et le blanc de l'œil. Les iris sont uniques et les deux iris d'un même individu sont différents. Dans l'iris de l'œil, il est possible de compter plus de 200 paramètres indépendants.



Figure 1.8 : L'iris

1.5.1.7. La rétine :

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique. La rétine est constituée de 4 couches de cellules et est située au fond de l'œil. La grande variété de configurations des vaisseaux sanguins présenterait la même diversité que les empreintes digitales. L'aspect des vaisseaux peut être modifié par l'âge ou la maladie, mais la position respective des vaisseaux reste inchangée durant toute la vie de l'individu.

[4]

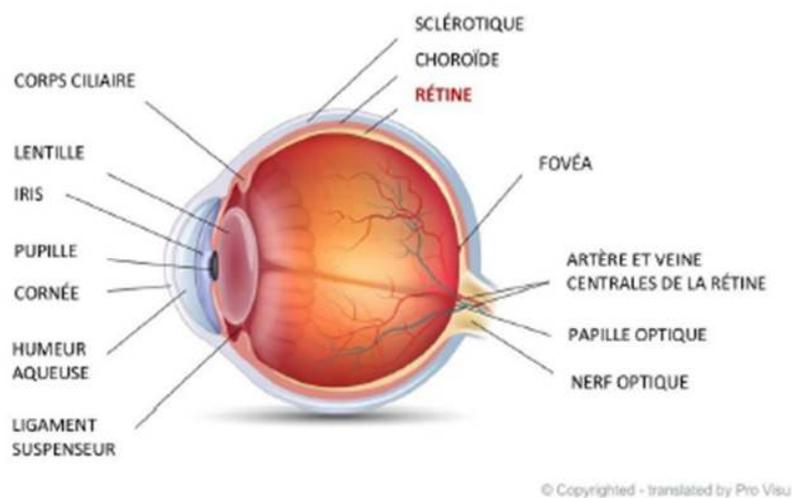


Figure 1.9 : La rétine

1.5.2. Modalités comportementales :

Ce sont certains comportements de plusieurs personnes.

1.5.2.1. La signature dynamique :

Cette technique est encore peu répandue, et peu de constructeurs la proposent. La vérification dynamique de signature est basée sur la différenciation entre les parties d'une signature qui sont habituelles et celles qui changent avec presque chaque signature.



Figure 1.10 : Dynamique de signature

1.5.2.2. La dynamique de frappe au clavier :

Il s'agit d'une technique de reconnaissance des personnes basée sur le rythme de frappe qui leur est propre.

Les frappes au clavier sont affectées par plusieurs facteurs : durée entre frappes, fréquence des erreurs ou durée globale nécessaire pour taper un texte.



Figure 1.11 : Dynamique de frappe au clavier

1.5.2.3. La voix (Reconnaissance vocale) :

Chaque personne possède une voix propre caractérisée par une fréquence, une intensité et une tonalité et que l'on peut analyser par enregistrement avec un microphone. Même si deux voix peuvent sembler similaires pour l'oreille, le traitement informatique permet de les isoler.

La reconnaissance du locuteur vise à déterminer les caractéristiques uniques de la voix de chaque individu.

La reconnaissance des locuteurs est particulièrement utilisée par les téléphones, les corps policiers, dans les hôpitaux...etc.

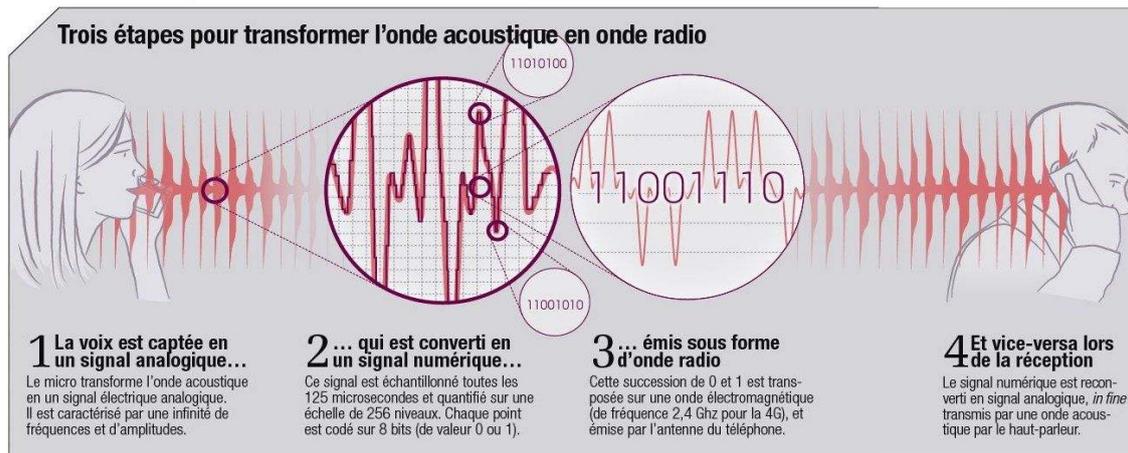


Figure 1.12 : La voix

1.5.2.4. La démarche :

Chaque personne a une façon particulière de marche, nous pouvons identifier les individus à partir de la nature du mouvement des jambes, des bras et des articulations.

Des photos de l'individu peuvent être prises et la vitesse et l'accélération sont déterminées.

Cette méthode est rarement utilisée et acceptée par l'utilisateur.

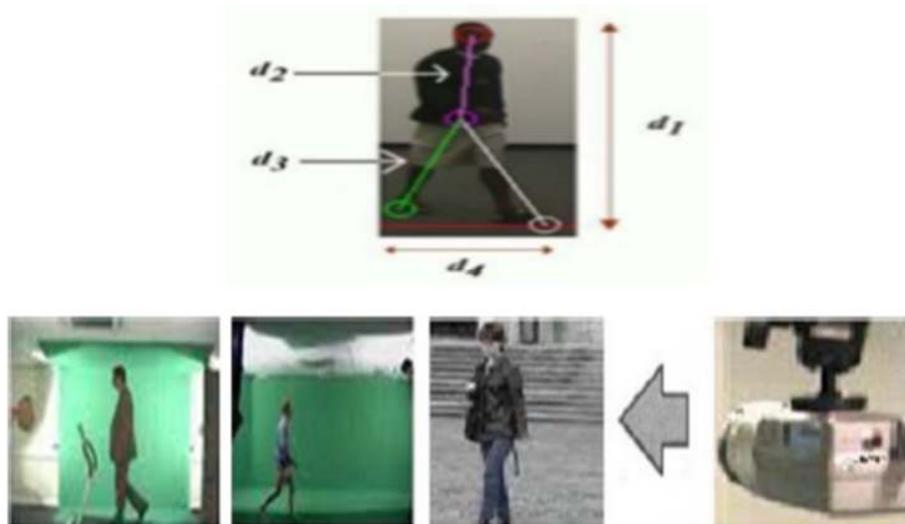


Figure 1.13 : Système biométrique basé sur la démarche.

1.5.3. Modalités biologiques :

Ce sont des caractéristiques biologiques différentes qui diffèrent d'une personne à l'autre.

1.5.3.1. L'ADN :

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire.

L'information génétique d'un individu est unique, car aucun membre de l'espèce ne possède la même combinaison de gènes codés.



Figure 1.14 : Exemple de l'ADN

1.5.3.2. L'oreille :

Cette technique consiste à comparer les empreintes d'oreille que peuvent laisser certains individus dans le cadre d'un délit.

Cette méthode est rarement utilisée et est principalement utilisée par la police et la justice.



Figure1.15 : Empreintes d'oreille

1.5.3.3. Les veines :

Parmi les techniques utilisées en biométrie figurent les veines, et elles comprennent les veines de la main, les veines de la paume et même les veines des doigts. Cette technologie a ses caractéristiques distinctives comme les autres technologies, et elle diffère d'une personne à l'autre.

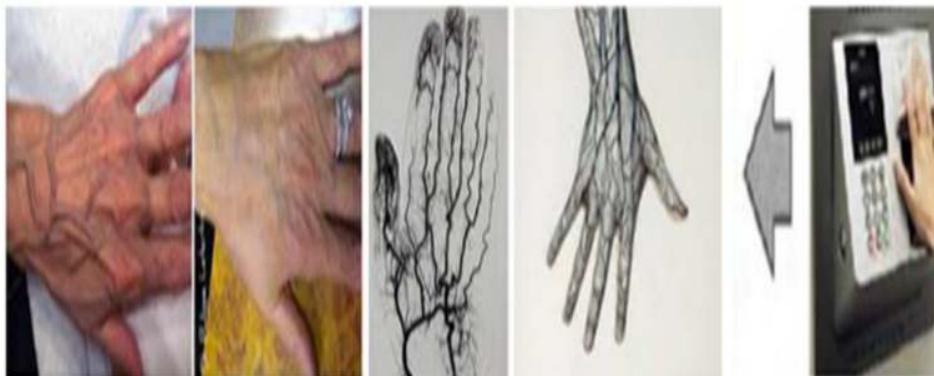


Figure 1.16: Système biométrique basé sur les veines.

1.6. Etude comparative entre les modalités biométriques :

Il existe de nombreuses techniques biométriques différentes qui sont utilisées
Applications : Chaque technologie biométrique a ses forces et ses faiblesses, le choix dépend donc de la technologie la plus avantageuse et la moins désavantageuse, car aucune technologie ne répond pleinement à toutes les exigences.

Chaque technique diffère par ses avantages et ses inconvénients d'une autre technologie, car elle diffère dans le mode d'utilisation, il y a des choses faciles et il y a des difficultés et il y a des acceptables et il y a des rejets.

Les modalités biométriques	Avantages	Inconvénients
Empreintes digitales	-Cout. -Ergonomie moyenne. -La plus éprouvée. -Facilité d'utilisation et traitement rapide.	-Perturbation possible par des blessures. -Système encombrant
Géométrie de la main	-Très Ergonomique. -Bonne acceptabilité. -Pas d'effet en cas d'humidité ou d'impropriété des doigts.	-Perturbation possible par des blessures. -Système encombrant.
les articulations des doigts	- Technique acceptable. - Utilisation simple. - En combinant tous les doigts de la main, il est possible de présenter un système biométrique robuste et précis.	- Très similaire pour les jumeaux - Problème dans le cas d'une coupure d'un doigt. - Pose incorrecte du doigt sur le lecteur provoquant une grande erreur.
Visage	-cout. - Bonne acceptabilité.	-Technologie sensible à l'environnement (éclairage, position...) - Jumeaux identiques.
Rétine	-Fiabilité. -Pérennité.	- Acceptabilité très faible. - Coûteuse

Iris	<ul style="list-style-type: none"> -Fiabilité. -Contient grande quantité d'information. -Pas de confusion pour les vrais jumeaux. 	<ul style="list-style-type: none"> -Acceptabilité moyenne. -Possibilité d'attaque. -Sensible en cas d'humidité ou malpropreté des doigts.
La signature	<ul style="list-style-type: none"> -Acceptation forte par l'utilisateur. 	<ul style="list-style-type: none"> -Dépendant de l'état émotionnel de la personne peu fiable. -Coûteuse
La dynamique de frappe au clavier	<ul style="list-style-type: none"> - Acceptation forte par l'utilisateur. 	<ul style="list-style-type: none"> - Dépendant de l'état physique de la personne peu fiable
La voix	<ul style="list-style-type: none"> -Facilité. 	<ul style="list-style-type: none"> -Sensible à l'état physique et émotionnel d l'individu.
La démarche	<ul style="list-style-type: none"> -Peut être repérée à grande distance à l'aide d'une caméra à faible résolutions. -Observée ainsi de n'importe quel angle. 	<ul style="list-style-type: none"> -Il est sensible aux changements d'habits, chaussures et surface.
ADN	<ul style="list-style-type: none"> -Distinguer les individus avec une grande précision. -Il facilite la détection des délinquants. 	<ul style="list-style-type: none"> -Analyse trop lente à donner des résultats. -Coût élevé.
L'oreille	<ul style="list-style-type: none"> -Il a une grande capacité de sécurité. 	<ul style="list-style-type: none"> -Il n'a pas beaucoup de portabilité. - Technologie coûteuse.
Les veines	<ul style="list-style-type: none"> - Ne nécessite pas de contact. - Difficile à falsifier. 	<ul style="list-style-type: none"> - Très coûteuse.

Tableau 1.2: Comparaison entre les modalités biométriques.

1.7. Les types de systèmes biométriques :

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leur fiabilité et leurs cours d'évolution.

- **Mono modalité.**
- **Multi modalité.**

1.7.1. Les systèmes multimodaux :

Peuvent se référer à de nombreux systèmes différents :

- **Systèmes multi algorithmes.**
- **Systèmes multi échantillons.**
- **Systèmes multi capteurs.**
- **Systèmes multi instances.**
- **Systèmes multi caractères.**

1.7.2. L'architecture des systèmes multimodaux :

Les systèmes multimodaux associent plusieurs systèmes biométriques unimodaux et nécessitent donc l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle alors d'architecture en série, ou simultanément, on parle alors d'architecture en parallèle. L'architecture est en réalité surtout liée au traitement. En effet, l'acquisition des données biométriques est en général séquentielle pour des raisons pratiques. Il est difficile d'acquérir en même temps une empreinte digitale et une image d'iris dans de bonnes conditions. Il existe cependant certains cas où les acquisitions peuvent être faites simultanément lorsque les différentes données utilisent le même capteur par exemple les capteurs d'empreintes multi-doigts qui permettent d'acquérir les images de plusieurs doigts simultanément ou même l'empreinte palmaire et les empreintes digitales. L'architecture est donc en général liée au traitement et en particulier à la décision. En effet la différence entre un système multimodal en série et un système multimodal en parallèle réside dans le fait d'obtenir un score de similarité à

l'issue de chaque acquisition (fusion en série) ou de procéder à l'ensemble des acquisitions avant de prendre une décision (fusion en parallèle). L'architecture en parallèle (figure 1.17) est la plus utilisée car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'acquisition et le traitement d'un grand nombre de données biométriques est coûteux en temps et en matériel, et réduit le confort d'utilisation. C'est pour cela que l'architecture en série (figure 1.18) peut être privilégiée dans certaines applications ; par exemple si la multimodalité est utilisée pour donner une alternative pour les personnes ne pouvant pas utiliser l'empreinte digitale par exemple. Pour la majorité des individus seule l'empreinte est acquise et traitée mais pour ceux qui ne peuvent pas être ainsi authentifiés on utilise un système à base d'iris alternativement.

1.8. La fusion :

La fusion est un bon moyen pour améliorer la précision et la robustesse des systèmes [11]. De manière générale, il existe deux types de fusion. La première est la fusion de plusieurs caractéristiques d'une seule modalité. Comme les différentes caractéristiques d'une même image sont corrélées, l'amélioration sera limitée. L'autre type est multimodal.

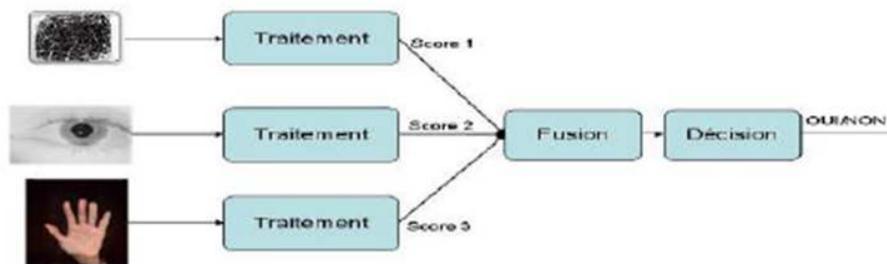


Figure 1.17 : Architecture de fusion en parallèle

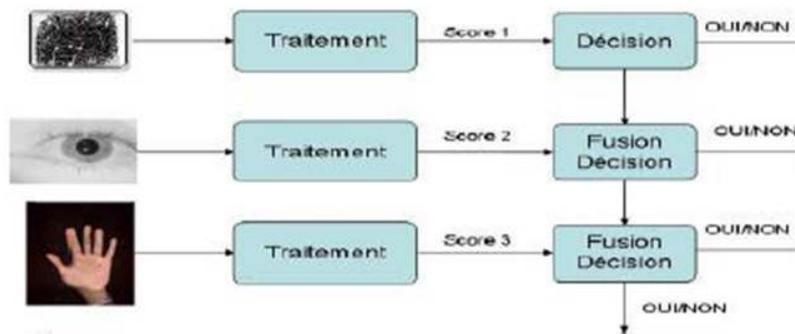


Figure 1.18 : Architecture de fusion en série (incrémentale ou séquentielle)

1.8.1. Les niveaux de fusion :

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision (figure 1.19).

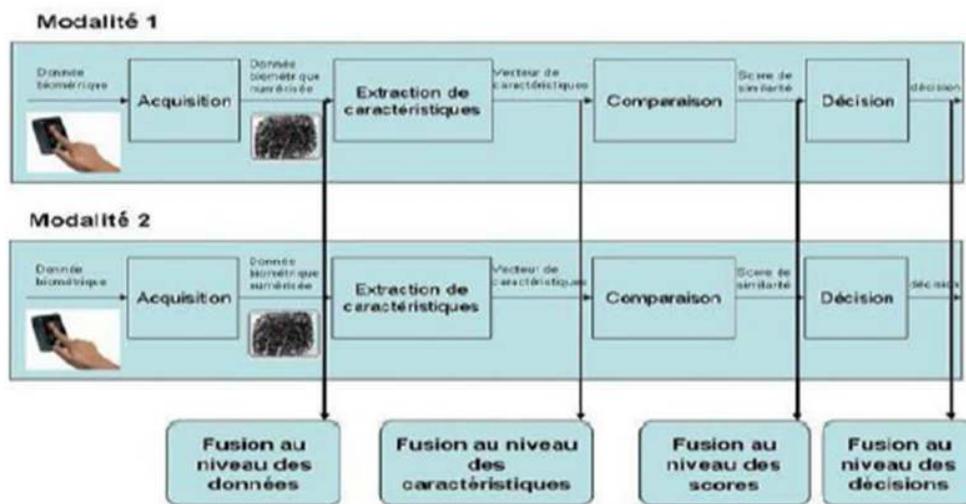


Figure 1.19 : Les différents niveaux de fusion.

Ces quatre niveaux de fusion peuvent être classés en deux sous-ensembles :

- la fusion pré-classification (avant comparaison),
- la fusion post-classification (après la comparaison).

1.8.2. La fusion pré-classification :

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur (images brutes) ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

- Niveau du capteur (Sensor Level) : (figure 1.20),
- Niveau Caractéristiques (Feature Level) : (figure1.21).

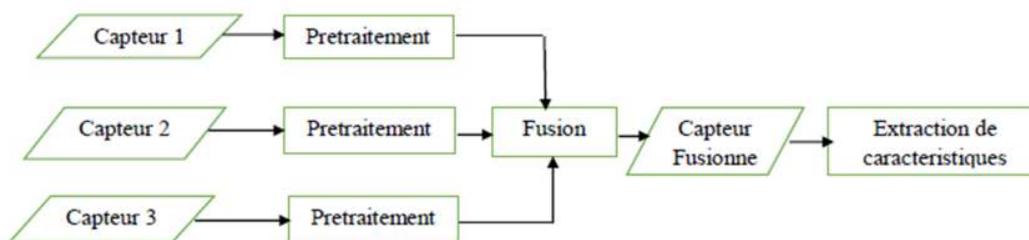


Figure 1.20 : Schéma de fusion au niveau des capteurs

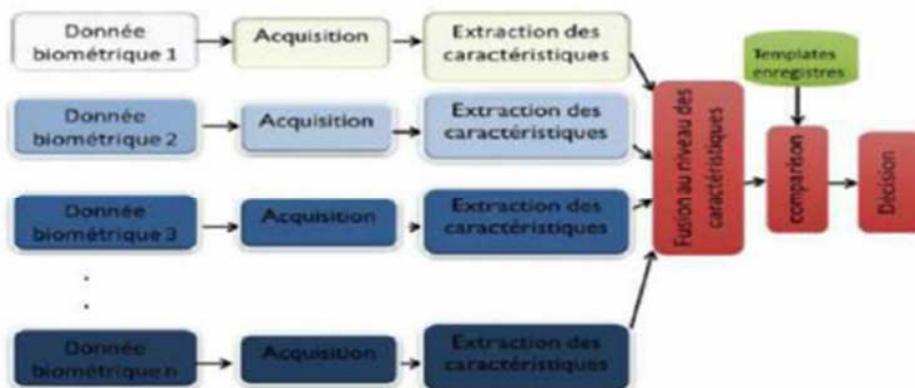


Figure 1.21 : Schéma de fusion au niveau de l'extraction des caractéristiques

1.8.3. La fusion post-classification :

La fusion post-classification peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions. Dans les deux cas, la fusion est en fait un problème bien connu de la littérature sous le nom de "Multiple Classifier systems".

- Niveau Décision (Décision Level) : (figure1.22).
- Niveau Score (Score Level) : (figure1.23).

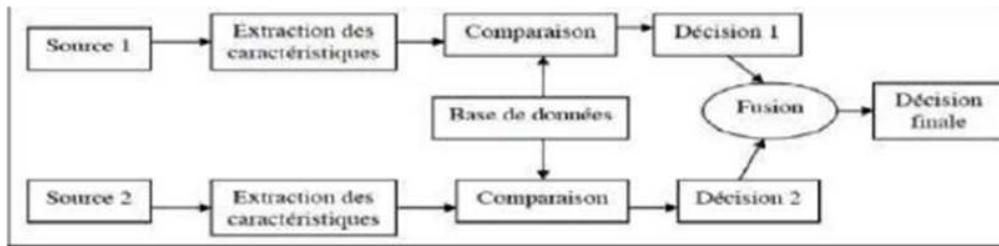


Figure 1.22 : Schéma de fusion au niveau de la décision

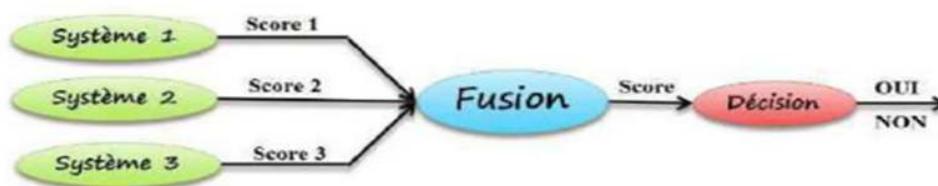


Figure 1.23 : Schéma de fusion au niveau des scores [10]

1.9. Principe de fonctionnement d'un système biométrique :

En matière de fonctionnement, tous les systèmes biométriques fonctionnent comme suit :

- Capture des caractéristiques.
- Extraction de caractéristiques.
- Comparaison.
- Décision.

1.10. Domaine d'Applications :

Il existe quatre domaines d'application de la biométrie.

1.10.1. Service public :

La biométrie est utilisée dans la vie ordinaire dans de nombreux endroits gouvernementaux tels que :

- Surveiller les frontières, les bâtiments et les entreprises importantes,
- Elle est utilisée dans les aéroports lors de l'entrée d'immigrants et de touristes,
- Assistance dans les domaines de l'assurance sociale et des établissements de santé.

1.10.2. Pouvoir judiciaire :

La biométrie est largement utilisée dans les centres gouvernementaux et les juridictions depuis longtemps :

- L'utilisation d'empreintes digitales dans les circonstances de crimes tels que meurtre, vol, etc.
- Utiliser de l'ADN extrait de sang ou de cheveux pour découvrir le criminel.

1.10.3. Secteurs des banques :

- La biométrie est utilisée dans les banques pour leur capacité de sécurité.
- Les transactions bancaires de toutes les manières et de tous les moyens.
- Réduction de la fraude grâce à l'intégration de cartes avec empreintes digitales.

1.10.4. Accès physique et logique :

Elle aide avec des assurances matérielles telles que les chambres et les coffres forts d'argent et la sécurisation des sessions technologiques.

1.11. Conclusion :

La biométrie est aujourd'hui la méthode de sécurité la plus sûre. Elle est de plus en plus appliquée dans différents secteurs grâce à ses avantages. Dans ce chapitre, Nous avons défini la biométrie et fait référence aux différentes méthodes de mesure pour identifier les personnes et comparer différentes techniques biométriques qui résument les avantages et inconvénients de chacune d'elles, à la fin nous avons présenté les domaines d'application de la biométrie.

Chapitre II

L'Empreinte Palmaire

2.1. Introduction

Ces dernières années, la reconnaissance des empreintes palmaires a suscité un intérêt croissant de la part de beaucoup de chercheurs [19, 20]. Probablement, la raison principale de cet intérêt est que cette modalité biométrique renferme beaucoup d'informations d'un caractère unique, et qu'elle est aussi très prometteuse pour l'authentification d'identité. Une image d'empreinte palmaire à faible résolution se compose généralement de lignes principales et de rides [1].

En général, la plupart des personnes ont trois lignes principales : la ligne du cœur, la ligne de tête et la ligne de vie. Les rides sont considérées comme les modèles de ligne les plus fins et les plus irréguliers [2].

D'autres informations telles que la texture, les indentations et les marques sont aussi adoptées lorsqu'on compare des empreintes palmaires.

En général, les méthodes d'extraction d'éléments d'empreinte palmaire comportent principalement la ligne principale, la méthode de codage, la méthode de texture, l'apprentissage sous-espace, le descripteur local et le réseau convolutionnel. Ces méthodes permettent normalement d'obtenir un taux de reconnaissance extraordinaire sur les bases de données d'empreintes palmaires avec ou sans contact [1].

Au cours des 15 dernières années, diverses technologies de reconnaissance d'empreintes palmaires ont été développées, telles que la reconnaissance d'empreintes palmaires à basse résolution, à haute résolution, à trois dimensions (3D) et multispectrale. Différents types de technologies de reconnaissance d'empreintes palmaires se concentrent essentiellement sur différents niveaux de fonctionnalités d'empreintes palmaires [3].

Dans ce chapitre, nous avons traité de la définition de l'empreinte palmaire, de ses caractéristiques et de la définition de ses différents types. Nous avons également présenté l'empreinte palmaire multi-spectre et comment classer le système proposé et utilisé.

2.2. Reconnaissance par empreintes palmaires

Avant d'identifier une empreinte palmaires biométrique, nous devons d'abord fournir les informations et les caractéristiques qui y sont liées.

2.2.1. Définition de l’empreinte palmaire :

Introduite par David Zhang et Shu [4] (chercheurs et professeurs à l’université polytechnique de Hong Kong) en 1996 pour remédier aux problèmes liés à : (i) la non visibilité d’une empreinte digitale, ou bien (ii) le coût élevé des appareils de capture des images de l’iris et de la rétine, ou encore (iii) les faibles taux de reconnaissance des autres modalités biométriques [4].

L’empreinte palmaire représente le modèle de la paume de la main humaine illustrant les caractéristiques physiques du motif de sa peau tels que : les lignes (principales et rides), les points, les minuties et sa texture. En d’autre terme, si la partie intérieure de la main qui est non visible lorsque la main est fermée, du poignet aux racines des doigts, comme le montre la figure.2.1 [4, 5].



Figure 2.1 : Paume de la main.

Avantages :

- Facile à utiliser, elle a une grande acceptation,
- Après l’utilisation, la main reste propre et ne laisse aucune trace,
- Pratiquement elle est disponible chez tous les individus.

Inconvénients :

- Pourrait être similaire chez les jumeaux ou des membres de la famille.

2.2.2. Caractéristique des empreintes palmaires :

L’empreinte palmaire est une surface très large et interne dans la main, elle contient plusieurs traits de caractéristiques qui peuvent être exploités dans la reconnaissance des individus. Grâce à cette large surface et la richesse des traits de caractéristiques, nous prévoyons que les empreintes palmaires sont très robustes aux bruits et uniques pour chaque individu. En comparaison aux autres caractéristiques physiques, l’identification par les empreintes palmaires a plusieurs avantages [4, 6, 7, 8] :

- Traitement d’image à basse résolution,
- Peu de risque d’intrusion,
- Les traits des lignes sont stables,
- Taux élevé d’acceptation par les utilisateurs.

2.2.2.1. Caractéristiques géométriques :

Comme toute image, l’empreinte palmaire présente aussi des caractéristiques géométriques telles que : la longueur, la largeur, et la surface. Ces caractéristiques utiles pour une première vérification.

- Traitement d’image à basse résolution.
- Peu de risque d’intrusion.
- Taux élevé d’acceptation par les utilisateurs.

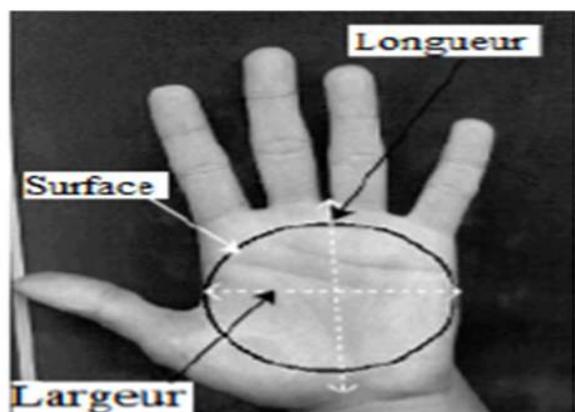


Figure 2.2 : Caractéristiques géométriques de l’empreinte palmaire

2.2.2.2. Les lignes principales :

L'empreinte palmaire est caractérisée par trois lignes principales, dites : plis de flexion (figure.2.3) :

- La ligne de tête.
- La ligne de vie.
- La ligne du cœur.



Figure.2.3 : Les plis de flexions de la paume de la main.

2.2.2.3. Les rides (plis secondaires) :

L'empreinte palmaire contient de nombreux autres plis qui diffèrent de ceux de flexion du fait qu'ils sont plus minces et plus irréguliers. Certains d'entre eux sont congénitaux, d'autres sont dus aux activités musculaires. Les lignes principales et les rides peuvent être observées facilement sur les images capturées à basse résolution. Comme les lignes principales seules ne fournissent pas une information distinctive suffisante, les rides jouent un rôle important dans la reconnaissance palmaire. Combinées aux lignes principales, elles fournissent une information distinctive pour la reconnaissance.

2.2.2.4. Les points de références :

Les points de référence représentant les deux extrémités de la paume de la main *a* et *b* comme le montre la Figure 2.4.

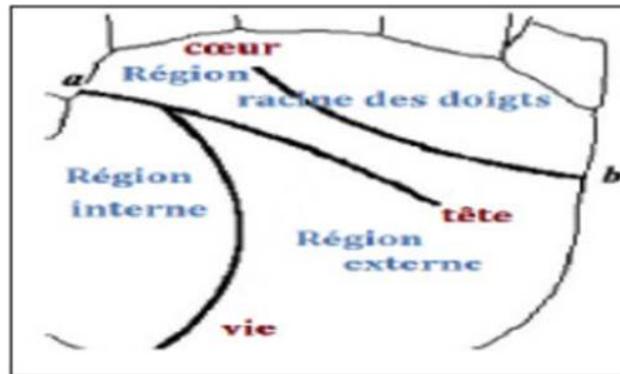


Figure.2.4 : Les points de référence de l'empreinte palmaire

Ils servent de point de repère lors de l'alignement et l'extraction des caractéristiques de l'empreinte palmaire. La taille de cette dernière peut être aussi estimée grâce à ces deux points.

2.2.2.5. Les caractéristiques de minutie :

Les minuties de l'empreinte palmaire sont généralement similaires aux minuties de l'empreinte digitale. Elles sont utilisées pour la reconnaissance leur acquisition nécessite l'utilisation d'appareils à haute résolution (voir figure 2.5).

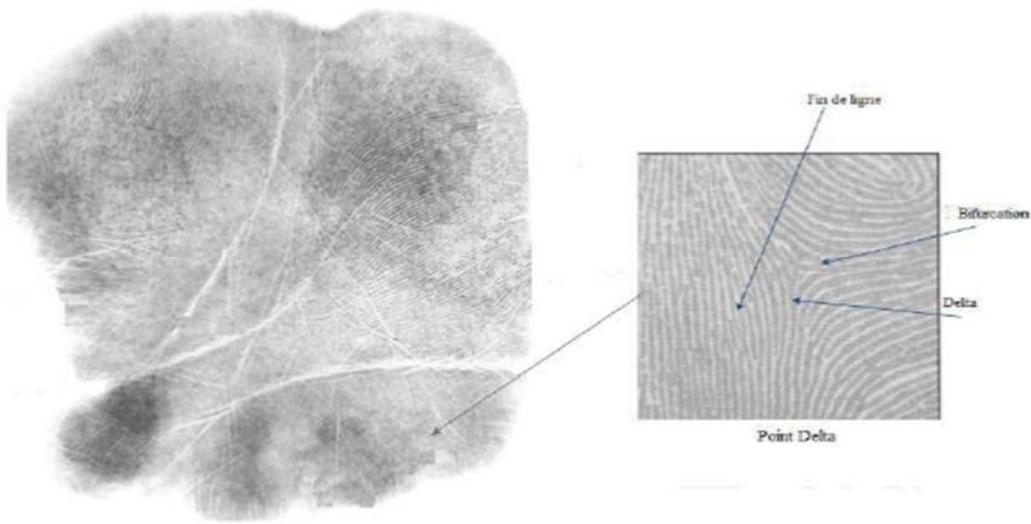


Figure 2.5. Minuties de l'empreinte palmaire

2.3. Les différentes empreintes palmaires :

L'attention de la recherche récente s'est concentrée sur l'amélioration de l'empreinte palmaire [9].

La reconnaissance d'empreintes palmaires peut être réalisée pour les méthodes avec ou sans contact, en fonction du type de contact avec le capteur requis pour réaliser l'acquisition. De plus, ces approches peuvent être regroupées en méthodes fondées sur des échantillons bidimensionnels et tridimensionnels [10].

2.3.1. Empreinte palmaire avec contact :

À l'heure actuelle, la majorité des approches présentées dans la documentation font appel à la reconnaissance par acquisition bidimensionnelle au contact avec des scanners à plat ou des dispositifs à base de CCD. Les scanners à plat sont particulièrement utiles pour les systèmes peu coûteux, tandis que les appareils à base de CCD offrent des échantillons de bonne qualité et des temps d'acquisition minimums. Des dispositifs d'acquisition tridimensionnels au contact basés sur des caméras CCD et des caméras ont été proposés afin d'accroître la précision de la reconnaissance, même s'ils exigent une installation complexe et plus coûteuse [10].

Les principaux inconvénients des méthodes avec contact sont la déformation, la saleté et la non acceptabilité par l'utilisateur. Les déformations sont causées par une pression non uniforme de la main sur le capteur. La saleté s'accumule après des acquisitions répétées et peut réduire la qualité des acquisitions. L'acceptabilité par l'utilisateur peut être problématique si les personnes n'aiment pas toucher des surfaces qui ont été touchées par d'autres personnes pour des raisons d'hygiène [10].

D'autres dispositifs d'acquisition bidimensionnelle avec contact basés sur des caméras numériques ont été aussi décrits. Par exemple, un dispositif comprenant une caméra CMOS à faible coût, un illuminateur annulaire et un boîtier qui fournit un support transparent pour la paume de la main est décrit dans la figure (figure 2.6a). L'appareil a été conçu pour être petit afin de pouvoir être utilisé comme dispositif d'identification personnelle pour les applications en ligne. Les appareils capturent des images avec une résolution de 65 dpi (figure 2.6b). En plus la (figure 2.6) [10] décrit un autre dispositif similaire de reconnaissance à faible coût.

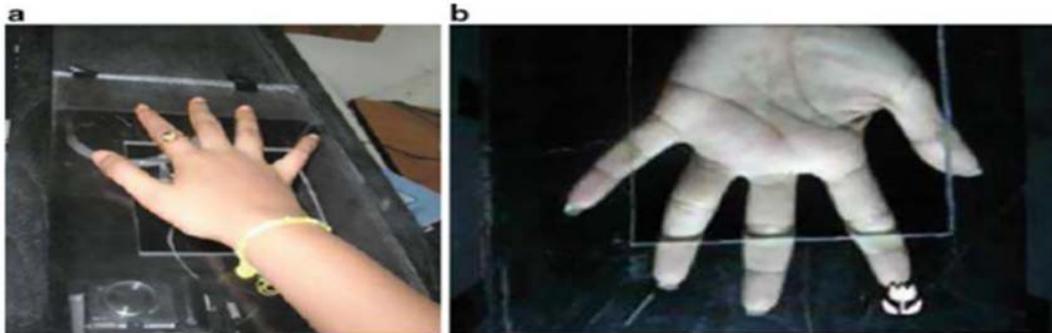


Figure 2.6: Le dispositif d'acquisition CCD bidimensionnel à base contact :
(a) le dispositif ; (b) exemple d'acquisition [10]

2.3.2. Empreinte palmaire sans contact :

Pour surmonter les inconvénients susmentionnés, des dispositifs d'acquisition sans contact ont été mis au point. Cependant, les méthodes sans contact peuvent être influencées par des inconvénients, notamment un contraste plus faible, un arrière-plan plus complexe et des distances d'acquisition non uniformes. De plus, les approches sans contact sont sensibles aux conditions d'éclairage. Pour résoudre les questions relatives à ces problèmes, des méthodes tridimensionnelles sans contact ont dernièrement été étudiées [10].

Ces méthodes sont plus efficaces et peuvent prendre en compte différentes distances d'acquisition, les conditions d'éclairage, les arrière-plans, le bruit et les attaques par spoofing.

Cependant, ils exigent des installations plus complexes et plus coûteuses que les méthodes bidimensionnelles sans contact [10].

Au cours de la dernière décennie, un grand nombre de nouvelles bases de données ont été créées. Sauf que certaines bases de données utilisent des appareils photo traditionnels et des méthodes d'acquisition classiques, c'est-à-dire des scanners à CCD (dispositif à couplage de charge), des appareils photo numériques, des caméras vidéo, pour recueillir des images d'empreintes palmaires, de nombreuses bases de données sont construites en choisissant des dispositifs qui saisissent des images sur diverses plateformes. Par exemple, les auteurs [11] ont utilisé une caméra CCD, un objectif à diaphragme automatique à courant continu (DC), une plateforme de placement manuel et

des sources lumineuses LED (diode électroluminescente) uniformes pour réaliser l'acquisition d'images en ligne, ce qui a été révélé par la figure (2.7) [11].

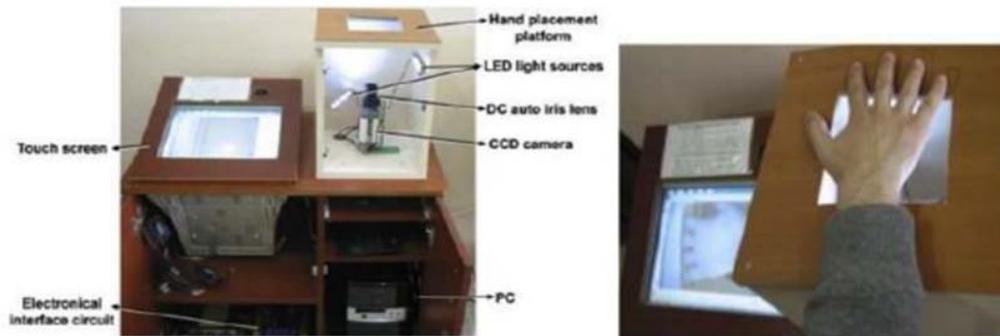


Figure 2.7: Vue extérieure du système d'acquisition d'images palmaire
Avec main posée sur la plateforme [11]

Il existe aussi un appareil photo numérique qui a été adopté pour acquérir des images d'empreintes palmaires sur un fond foncé. Dans leur système, deux lampes 3U de 23 watts ont été utilisées pour fournir l'éclairage et étaient disposées dans des lieux choisis (figure 2.8) [12].



Figure 2.8: Le dispositif d'acquisition d'empreintes palmaires [12]

2.4. Les différents types d’images :

Au cours des 15 dernières années, diverses technologies de reconnaissance d'empreintes palmaires ont été développées, telles que la reconnaissance d'empreintes palmaires à basse résolution, à haute résolution, à trois dimensions (3D) et multispectrale. Différents types de technologies de reconnaissance d'empreintes palmaires se concentrent essentiellement sur différents degrés de fonctionnalités d'empreintes palmaires [3].

Nous définissons brièvement ces technologies :

2.4.1. La reconnaissance d'empreintes palmaires à haute résolution :

La haute résolution signifie que la résolution d'une image peut atteindre 400 dpi ou plus, comme l'illustre la figure (2.9), ce qui est tout indiqué pour la criminalistique et les applications légitimes. Il existe deux méthodes principales pour la reconnaissance d'empreintes palmaires à haute résolution : les méthodes basées sur les détails et les méthodes basées sur la fusion régionale [13]. La reconnaissance d'images d'empreintes palmaires haute résolution consomme beaucoup de temps en raison de la grande capacité de l'image et du prétraitement complexe [3].

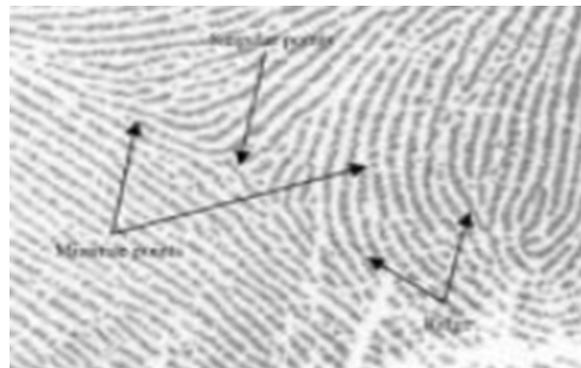


Figure2.9 : L'empreinte palmaire est présente dans une image haute résolution

2.4.2. La reconnaissance d'empreintes palmaires à basse résolution :

La reconnaissance d'empreintes palmaires à faible résolution a une large gamme d'applications civiles et commerciales en raison de ses nombreux avantages. Par exemple, les images d'empreintes palmaires à faible résolution peuvent être facilement capturées à l'aide d'appareils photo ordinaires [3].

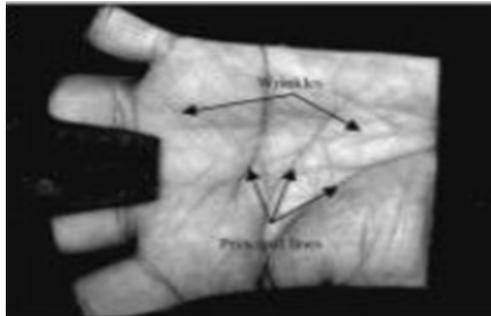


Figure 2.10 : L'empreinte palmaire est présente dans une image basse résolution [13]

2.4.3. La reconnaissance d'empreintes palmaires à trois dimensions (3D) :

La reconnaissance d'empreintes palmaires en 3D a également connu des progrès notables [13]. Les travaux existants montrent que l'information 3D sur la carte palmaire peut être convertie en images 2D basées sur la texture pour la reconnaissance. Par conséquent, les méthodes conventionnelles de reconnaissance d'empreintes palmaires en deux dimensions ont également été adoptées avec succès pour la reconnaissance d'empreintes palmaires en trois dimensions [3].

Palmaire 3D contrairement au palmaire 2D ne peuvent pas être facilement falsifiées.

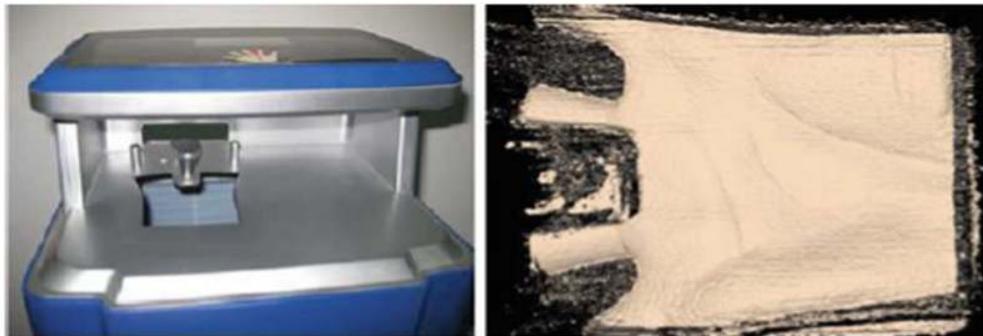


Figure 2.11. Dispositif d'acquisition d'images 3D basé sur la lumière et un exemple d'image de palmaire 3 D.

2.4.4. La reconnaissance d'empreintes palmaires multispectrales :

La reconnaissance de l'empreinte palmaire multispectrale est une technologie biométrique prometteuse en raison de son caractéristique stable et unique. La richesse de l'information de texture de l'empreinte palmaire multispectrale offre l'un des moyens les

plus importants pour la reconnaissance personnelle. En effet, la texture de l'empreinte palmaire multi-spectrale a plusieurs avantages, telle que : l'image à basse résolution, le faible coût, les caractéristiques structurelles stables et son acceptation élevée par les utilisateurs [14].

2.5. Les systèmes de reconnaissance de l'empreinte palmaire proposé :

De tels systèmes dénombrent généralement quatre étages, comme le montre la figure 2.12.

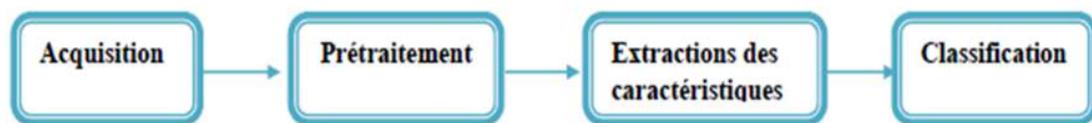


Figure 2.12 : Les différents étages des systèmes d'identification de l'empreinte palmaire

- **Le bloc d'acquisition d'image** : Chargé de prendre des photos de la paume de la main ou en fournir des photos.
- **Le prétraitement** : Chargé d'établir un système de coordonnées pour aligner les images et segmenter la partie nécessaire à l'extraction de ses caractéristiques de l'empreinte palmaire (cette étape dépend du type d'application).
- **L'extraction des caractéristiques, et la comparaison** : Au cours de cette étape, les caractéristiques de l'image sont extraites et comparées à d'autres qui en sont une référence.
- **La classification** : Après la comparaison des caractéristiques avec d'autres qui sont référencées dans des bases de données, la classe à laquelle elles appartiennent est déterminée.

2.6. Conclusion :

Dans ce chapitre, nous avons présenté l'empreinte palmaire, ses caractéristiques, les différentes technologies utilisées ainsi que les méthodes biométriques employées pour la reconnaissance des individus. Cette technologie présente une mesure de sécurité et de stabilité. Nous avons également exposé certaines de ses technologies qui ont été atteintes par la science, telles que technologie multi-spectrale, avec et sans contact.

Nous avons également souligné que la technologie sans contact est la plus appropriée car elle est très bien acceptée par les utilisateurs.

Chapitre III

**Systeme d'authentification de
l'empreinte palmaire multispectrale**

3.1. Introduction

La biométrie fait référence à l'étude des méthodes de reconnaissance des humains basées sur un ou plusieurs traits physiques ou comportementaux [1, 2]. En tant que caractéristique biométrique importante, l'empreinte palmaire a attiré beaucoup d'attention [3], car elle présente des avantages tels que sa rapidité, sa convivialité, son faible coût et sa grande précision. Toutefois, les systèmes d'empreintes palmaires en ligne peuvent encore être améliorés en ce qui concerne la précision et la possibilité d'attaques par usurpation [4]. Bien que l'imagerie 3D pourrait être utilisée comme solution à de tels problèmes, son dispositif coûteux et encombrant fait qu'elle soit mal recommandée aux applications réelles.

Une solution à ces problèmes peut être l'imagerie multispectrale [5-7], qui capte une image dans diverses bandes spectrales. Chaque bande spectrale met en évidence les caractéristiques spécifiques de la paume, ce qui permet de recueillir plus d'informations pour améliorer la précision et la capacité de non appropriation des systèmes d'empreintes palmaires. L'analyse multispectrale a été utilisée pour l'authentification liée aux empreintes palmaires [8-12].

Rowe et al. [10] ont proposé un système biométrique multispectrale pour la main entière. L'objectif de ce système était de recueillir des informations sur les empreintes palmaires avec des caractéristiques claires des empreintes digitales, et la résolution de l'image a été fixée à 500 dpi. Cependant, la faible vitesse d'extraction et de comparaison des caractéristiques l'ont rendu inadapté aux applications en temps réel. Likforman-Sulem et al. [11] ont utilisé des images multispectrales dans un système d'authentification multimodal ; toutefois, leur système utilisait un scanner optique de bureau et une caméra thermique, ce qui a rendu ce système très coûteux.

La résolution de l'image est également trop élevée (600 dpi) pour répondre aux exigences en temps réel des systèmes biométriques pratiques. Wang et al. [12] ont proposé un système de fusion d'empreintes palmaires et de veines palmaires, qui pourrait acquérir deux types d'images simultanément. Le système utilise une caméra couleur et une caméra proche infrarouge (NIR) et nécessite une procédure d'enregistrement d'environ 9 s. Hao et al. [8, 9] ont développé un capteur d'empreinte palmaire multispectrale sans contact. Cependant, sa qualité d'image est limitée et sa précision de reconnaissance n'est donc pas très élevée. Dans l'ensemble, la

numérisation multispectrale des empreintes palmaires est un sujet relativement nouveau et les travaux susmentionnés représentent l'état de l'art.

Les informations présentées par de multiples mesures biométriques peuvent être consolidées à quatre niveaux : au niveau de l'image, au niveau des caractéristiques, au niveau du score de correspondance et au niveau de la décision Ross et al. [13]. Wang et al. [12] ont fusionné des images d'empreintes palmaires et des veines des mains en utilisant une nouvelle méthode de fusion par ondelettes qui préserve les bords et améliore le contraste pour l'utilisation du système de reconnaissance personnelle. De bons résultats en termes de précision ont été signalés, mais la procédure d'enregistrement des images prend 9 s, ce qui l'empêche de son exploitation en temps réel. Hao et al. [19] ont évalué plusieurs schémas de fusion au niveau de l'image bien connus pour les images palmaires multispectrales. Cependant, leur ensemble de données était trop petit (84 images) pour être concluant. En 2008, Hao et al. [9] ont étendu leurs travaux à une base de données plus importante et ont proposé une nouvelle méthode d'enregistrement au niveau des caractéristiques pour la fusion d'images. Les résultats obtenus par les différentes méthodes de fusion d'images ont également été améliorés. Bien que la fusion d'images et de caractéristiques puisse intégrer les informations fournies par chaque bande spectrale, la procédure d'enregistrement requise est souvent trop longue Wang et al. [12]. En ce qui concerne la fusion au niveau des scores de correspondance et la fusion au niveau décisionnel, il a été souligné dans Ross et al. [13] que la première fonctionne mieux que la seconde parce que les scores de correspondance contiennent plus d'informations sur le modèle d'entrée et qu'il est facile d'accéder et de combiner les scores générés par les différents correspondants. C'est pour ces raisons, que la fusion d'informations au niveau du score est l'approche la plus couramment utilisée dans les systèmes biométriques multimodaux et les systèmes d'empreintes palmaires multispectrales Rowe et al. et Likforman-Sulem et al. [10, 11].

Dans ce chapitre, nous présentons un système d'authentification de l'empreinte palmaire multispectrale peu coûteux qui peut fonctionner en temps réel et acquérir des images de haute qualité. Ce système collecte des images d'empreintes palmaires dans les spectres visibles et proche infrarouge. Par rapport aux approches traditionnelles de reconnaissance d'empreintes palmaires, ce système peut améliorer considérablement la précision de la reconnaissance en fusionnant les informations fournies par l'empreinte palmaire multispectrale des images au niveau du score. D'autre part, en

utilisant la corrélation entre les spectres, ce système est robuste aux attaques anti-spoof.

3.2. L'architecture du système d'authentification de l'empreinte palmaire multispectrale :

Dans cette section, nous décrivons les constituantes du système retenu et ses paramètres. Deux considérations fondamentales dans la conception d'un système d'empreinte palmaire multispectrale sont les caractéristiques d'absorption et de réflexion des couleurs de la peau humaine et les spectres lumineux à utiliser lors de l'acquisition des images. La peau humaine est composée de trois couches : l'épiderme, le derme et la sous-cutanée, comme le montre la figure 3.1.

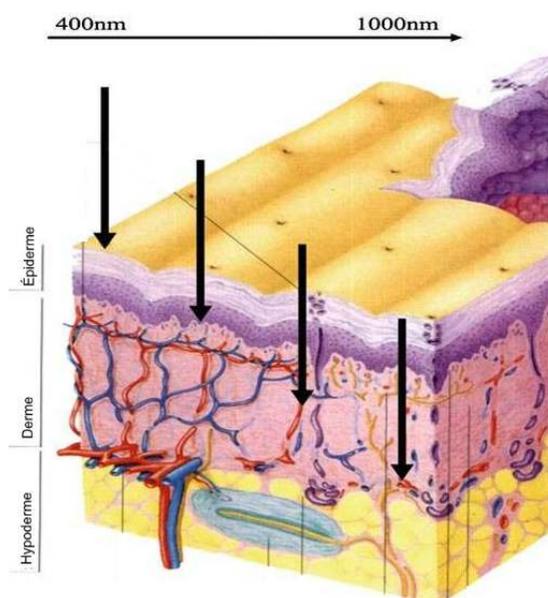


Figure. 3.1: Anatomie de la peau en coupe transversale

Chaque couche contiendra une proportion différente de sang et de graisse. L'épiderme contient également de la mélanine, tandis que la sous-cutané contient des veines Gawkrödger [14]. Différentes longueurs d'ondes lumineuses pénètrent dans différentes couches de la peau et s'illuminent dans différents spectres. La lumière proche infrarouge pénètre les tissus humains plus loin que la lumière visible, et le sang absorbe plus d'énergie proche infrarouge que les tissus environnants (par exemple, la graisse ou la mélanine) Zharov et al. [15]. Ce système acquiert des informations spectrales des trois couches cutanées en utilisant à la fois les bandes visibles et la bande NIR. Dans le spectre visible, un réseau de trois diodes

électroluminescentes (DEL) monochromes est utilisé, avec un pic bleu à 470 nm, un pic vert à 525 nm à et un pic rouge à 660 nm.

Dans le spectre NIR, il a été utilisé un réseau de LEDs NIR culminant à 880 nm. Il a été aussi démontré que la lumière dans la gamme 700-1000 nm peut pénétrer la peau humaine, tandis que les 880-930 nm offrent un bon contraste des veines sous-cutanées Zharov et al. [15].

La figure 3.2 montre la structure interne du dispositif d'acquisition des images multispectrales des empreintes palmaires multispectrales. Tandis que la figure 3.3 montre le prototype de cet appareil. Il est composé d'une caméra à dispositif à couplage de charge (CCD), un objectif, un convertisseur analogique-numérique (A/D), une source de lumière multispectrale, et un contrôleur de lumière. Un CCD monochromatique est placé au bas de l'appareil. Le convertisseur A/N relie le CCD et l'ordinateur.

Le contrôleur de lumière est utilisé pour contrôler la lumière multispectrale. Le système peut capturer des images d'empreintes palmaires dans une résolution de 352 par 288 ou 704 par 576. L'utilisateur est invité à poser sa main sur la plate-forme. Plusieurs chevilles ont été placées pour servir comme point de repère pour le placement des mains des utilisateurs. Quatre images d'empreintes palmaires de la main sont recueillies en même temps sous différentes lumières spectrales.

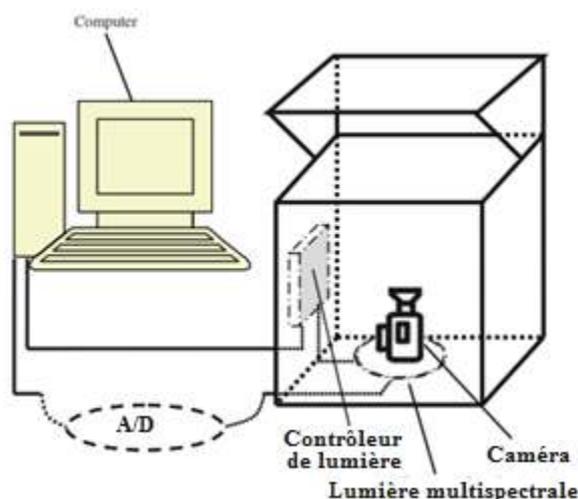


Figure 3.2 : La structure interne du dispositif d'acquisition multispectrale de l'empreinte palmaire



Figure 3.3 : Prototype du système d'empreinte palmaire multispectrale

Les deux lumières consécutives sont très courtes et les quatre images peuvent être capturées en très peu de temps (<1 s).

La figure 3.4 montre un échantillon typique d'empreinte palmaire multispectrale dans les bandes (a) bleue, (b) verte, (c) rouge et (d) NIR

Il à noter que les caractéristiques des lignes sont plus clair dans les bandes bleues et vertes que dans les bandes rouges et NIR. Alors que la bande rouge peut révéler une certaine structure veineuse, la bande NIR peut montrer la structure des veines de la paume ainsi que des informations sur les lignes partielles. Dans ce système, la structure des veines de la paume acquise dans la bande NIR n'est pas aussi claire que celle rapportée dans Zharov et al. [15] parce que le CCD de ce système est une caméra standard de télévision en circuit fermé (CCTV), au lieu d'une caméra sensible au proche infrarouge, pour réduire les coûts. Il est aussi recommandé d'éviter d'ajouter de filtre infrarouge devant le CCD car le filtre infrarouge couperait la lumière visible et affecterait l'acquisition d'images claires d'empreintes palmaires sous le spectre visible.

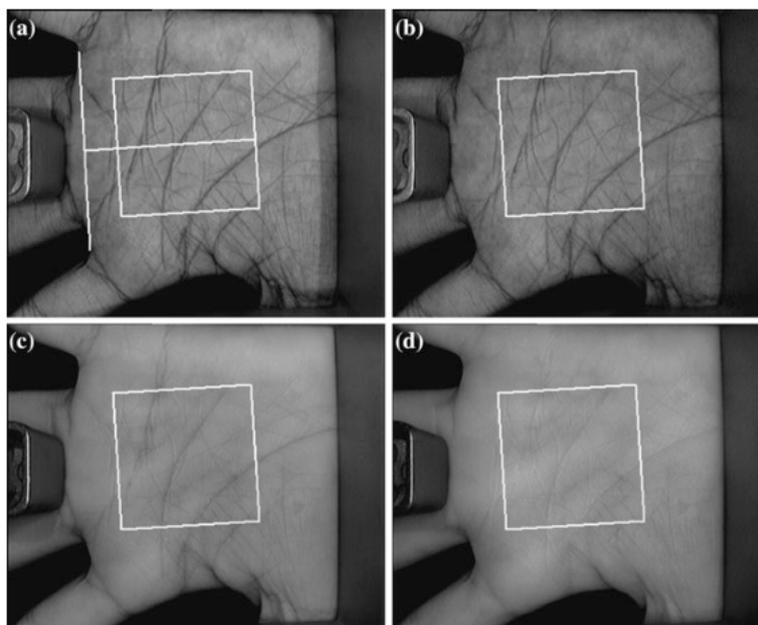


Figure 3.4 : Un échantillon typique d'empreinte palmaire multispectrale. (a) Bleu ; (b) Vert ;

(c) Rouge ; (d) NIR, le carré blanc est la région d'intérêt (ROI) de l'image

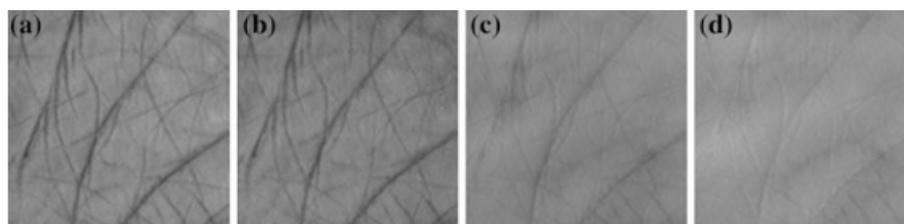


Figure 3.5 : Les ROIs de la Fig. 6.4. (a) Bleu ; (b) Vert ; (c) Rouge ; (d) NIR

Une région d'intérêt (ROI) sera extraite de l'image d'empreinte palmaire pour établir une correspondance plus poussée des caractéristiques. Cela peut réduire la quantité de données dans les caractéristiques de l'extraction et la mise en correspondance et réduire l'influence de la rotation et de translation des paumes. Dans ce travail, l'algorithme d'extraction du ROI de Zhang et al. [16] est utilisé et appliqué à la bande bleue pour trouver le système de coordonnées du ROI.

3.3. Algorithme d'extraction du ROI [16] :

- ✓ Étape 1. Appliquez un filtre passe-bas, $L(u, v)$, tel qu'un lissage gaussien, à l'image originale, $O(x, y)$. Un seuil A, T_p , est utilisé pour convertir l'image convoluée en une image binaire, $B(x, y)$, comme le montre la figure 3.6b.

- ✓ Étape 2. Obtenez les limites des espaces, (Fix_j, Fiy_j) ($i = 1 ; 2$), entre les doigts en utilisant un algorithme de suivi des limites (voir Fig. 3.6c). La limite de l'espace entre l'annulaire et le majeur n'est pas extraite car elle n'est pas utile pour le traitement suivant.
- ✓ Étape 3. Calculez la tangente des deux espaces. Soit (x_1, y_1) , et (x_2, y_2) , des points quelconques sur $(F1x_j, F1y_j)$ et $(F2x_j, F2y_j)$, respectivement. Si la ligne ($y = mx + c$) passant par ces deux points satisfait à l'inégalité, $Fiy_j \leq mFix_j + c$, pour tous les i et j (voir figure 3.6d), alors la ligne ($y = mx + c$) est considérée comme la tangente des deux écarts.
- ✓ Étape 4. Alignez (x_1, y_1) et (x_2, y_2) pour obtenir l'axe Y du système de coordonnées de l'empreinte palmaire, et utilisez une ligne passant par le milieu de ces deux points, qui est perpendiculaire à l'axe Y, pour déterminer l'origine du système de coordonnées (voir Fig. 3.6d).
- ✓ Étape 5. Extrayez une sous-image de taille fixe basée sur le système de coordonnées. La sous-image est située dans une certaine zone de l'image d'empreinte palmaire pour l'extraction des caractéristiques (voir les figures 3.6e et 3.6f).

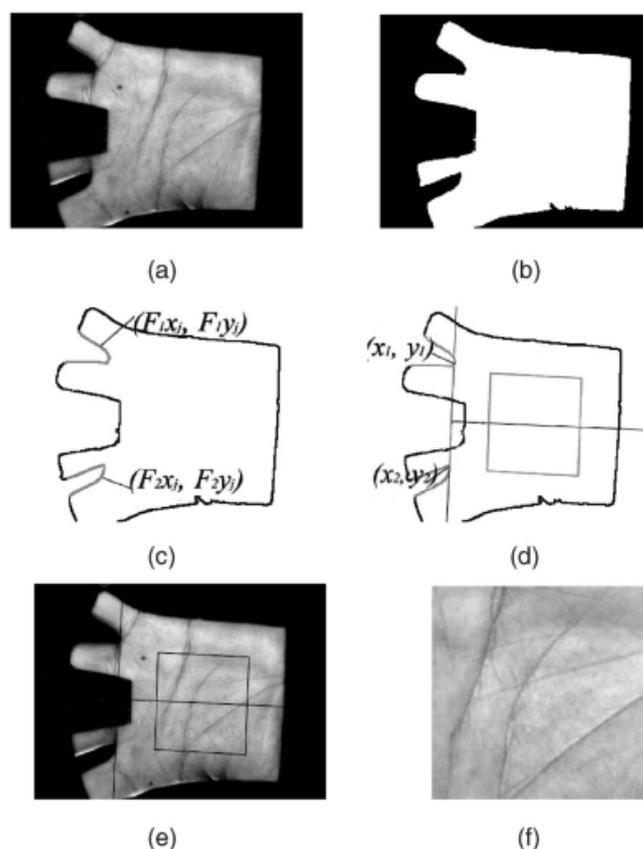


Figure 3.6 : Les principales étapes du prétraitement. (a) Image originale, (b) image binaire, (c) le suivi des limites, (d) la construction d'un système de coordonnées, (e) l'extraction de la partie centrale en tant que sous-image, et (f) le résultat du prétraitement.

Après l'extraction du ROI, l'effet de la translation ou de la rotation est généralement faible entre deux images. Ainsi, aucune procédure d'enregistrement supplémentaire n'est nécessaire. La figure 3.4 montre les ROIs de l'empreinte palmaire et la figure 3.5 montre les images ROIs recadrées.

Après avoir obtenu le ROI pour chaque bande, l'extraction et la mise en correspondance des caractéristiques seront appliquées à ces images de ROI. La décision finale de vérification sera prise par fusion de toutes les bandes au niveau du score. La figure 3.6 montre le schéma du système de vérification en ligne proposé.

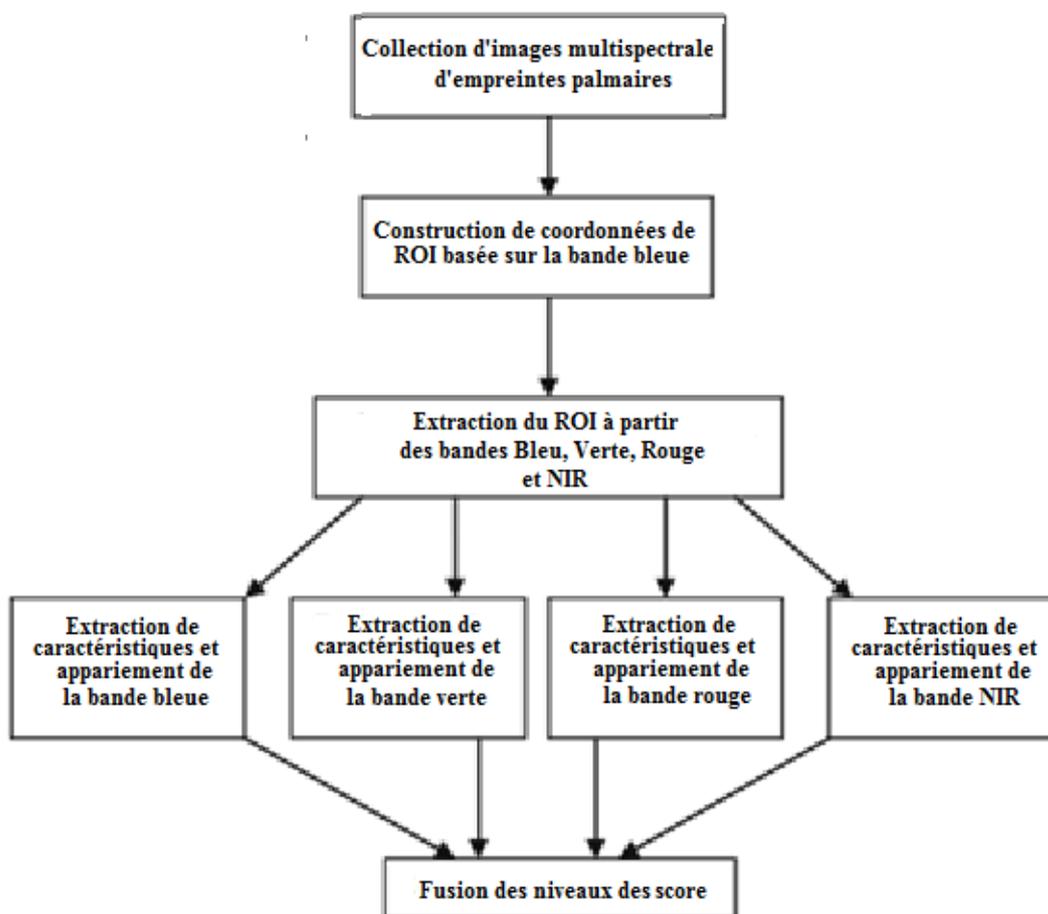


Figure 3.7 : Schéma du système en ligne de vérification

3.4. Fusion d'images :

La fusion est un bon moyen pour améliorer la précision et la robustesse des systèmes [17]. De manière générale, il existe deux types de fusion. La première est la fusion de plusieurs caractéristiques, à partir d'une seule image d'empreinte palmaire. Comme les différentes caractéristiques d'une même image sont corrélées, l'amélioration sera limitée. L'autre type est multimodal, c'est-à-dire la fusion de l'empreinte palmaire avec d'autres traits biométriques.

Au cours de la dernière décennie, de nombreux systèmes multimodaux différents ont été proposés, notamment la surface du doigt + empreinte palmaire, la géométrie de la main + empreinte palmaire, le visage + empreinte palmaire, l'empreinte digitale + empreinte palmaire et l'iris + empreinte palmaire.

La fusion d'images est un processus qui consiste à combiner les informations provenant d'un ensemble d'images, en une seule image, l'image fusionnée résultante

sera plus informative et plus complète que toutes les images d'entrée [18], le résultat de la fusion d'images est une nouvelle image qui convient mieux à la perception des humains et des machines ou au traitement ultérieur des images telles que la segmentation, l'extraction de caractéristiques et la reconnaissance des objets

L'image fusionnée est une image multispectrale à haute résolution spatiale obtenue en intégrant une image haute résolution monochrome et une image couleur multispectrale basse résolution constituée de la collection de bandes RVB (rouge, vert, bleu). Il est question de réaliser en appliquant une séquence d'opérateurs sur les images qui ferait la bonne information dans chacune des images proéminentes. L'image résultante est formée en combinant de telles informations agrandies à partir des images d'entrée dans une image unique [19]. L'un des objectifs des logiciels de fusion est l'amélioration continue des estimées et des prévisions, et par l'évaluation du besoin en sources additionnelles ou de modification du procédé lui-même, afin d'atteindre des résultats améliorés. Tous les algorithmes de fusion ont des objectifs communs comme indiqué ci-dessous :

1. Préserver toutes les informations pertinentes dans l'image fusionnée.
2. Supprimer les parties non pertinentes de l'image et le bruit.
3. Réduire au minimum les artefacts ou les incohérences dans l'image fusionnée utilisée.
4. Affinez les images.
5. Améliorer les corrections géométriques.
6. Remplacer l'image d'information manquante par des signaux à partir d'une autre image [20].

La fusion d'images se fait à trois niveaux différents, à savoir le niveau des pixels, le niveau des caractéristiques et le niveau de décision. Les méthodes de fusion d'images peuvent être classées en deux grandes catégories : la fusion de domaines spéciaux et la fusion de domaines transformés, le calcul de la moyenne, la méthode de Brovery, l'analyse en composantes principales (ACP). Les méthodes basées sur l'ACP sont des méthodes de domaines spéciaux. Mais ces méthodes produisent une distorsion spéciale dans l'image fusionnée, ce problème peut être résolu par une approche de transformation de domaine. L'analyse multi-résolution est devenue un outil très utile pour l'analyse des images. La transformée en ondelettes discrètes est devenue un outil très utile pour la fusion. Les images utilisées dans la fusion d'images

devraient déjà être enregistrées. Cependant, un mauvais enregistrement est une source majeure d'erreur dans la fusion d'images.

La technique de fusion au niveau du pixel est utilisée pour augmenter la résolution spatiale de l'image multispectrale. Au niveau le plus bas, la fusion au niveau des pixels utilise les données des pixels enregistrés de tous les ensembles d'images pour effectuer des fonctions de détection et de classification. Ce niveau a le potentiel d'atteindre les meilleures performances de fusion uniquement aux coûts de calcul les plus élevés.

Au niveau intermédiaire, la fusion au niveau des caractéristiques combine des caractéristiques qui sont détectées et segmentées dans les différentes sources de données.

3.5. Analyse multispectrale des images d'empreinte palmaires :

Dans cette section, nous décrivons d'abord comment les caractéristiques sont extraites et mises en correspondance pour chaque bande spectrale des images d'empreintes palmaires multispectrales, puis nous analysons la corrélation entre les bandes spectrales. Enfin, un schéma de fusion au niveau du score est présenté pour la prise de décision.

3.5.1. Extraction et appariement des caractéristiques pour chaque bande :

Il existe principalement trois types d'algorithmes actuellement utilisés pour l'authentification des empreintes palmaires : l'apprentissage sous-spatial [3, 21-22], la détection de lignes [23-24] et le codage basé sur la texture [16, 25-27]. Les systèmes en ligne utilisent généralement un codage basé sur la texture car il est très précis, robuste à l'illumination et rapide pour la mise en correspondance. Le système présenté utilise un codage basé sur l'orientation [26] (Kong et Zhang 2004), un algorithme de codage de pointe basé sur la texture, pour l'extraction des caractéristiques.

En visualisant les traits des images d'empreintes palmaires comme des lignes négatives, six filtres de Gabor ont été appliqués dans différentes directions ($\theta_j = j\pi/6$, où $j = \{0, 1, 2, 3, 4, 5\}$) aux images d'empreintes palmaires pour l'extraction des traits d'orientation. Pour chaque pixel, l'orientation correspondant à la réponse minimale est prise comme caractéristique à ce pixel Kong et al. [25]. Le filtre de Gabor utilisé est le suivant :

$$\Psi(x, y, \omega, \theta) = \frac{\omega}{\sqrt{2\pi k}} e^{-\frac{\omega^2}{8k^2}(4x'^2 + y'^2)} \left(e^{i\omega x'} - e^{-\frac{k^2}{2}} \right) \quad (3.1)$$

où

$$x' = (x - x_0) \cos \theta + (y - y_0) \sin \theta, y' = -(x - x_0) \sin \theta + (y - y_0) \cos \theta \quad (3.2)$$

est le centre de la fonction, ω est la fréquence radiale en radians par unité de longueur, θ est l'orientation de la fonction de Gabor en radians $k = \sqrt{2 \ln 2} \left(\frac{2^\varphi + 1}{2^\varphi - 1} \right)$ et φ est la largeur de de la demi bande passante d'amplitude de la réponse en fréquence. Pour réduire l'influence de rayonnement, le courant continu (DC) est retiré du filtre. La figure 3.7 montre certaines cartes de caractéristiques extraites de la figure 3.5 en utilisant divers paramètres.

Comme il y a au total six orientations différentes, nous pouvons les coder en utilisant 3 bits comme l'indique le tableau 3.1. Ce système de codage vise à rendre la différence binaire proportionnelle à la différence angulaire Kong et al. [24]. Ainsi, la différence entre deux cartes d'orientation pourrait être mesurée en utilisant la distance de Hamming :

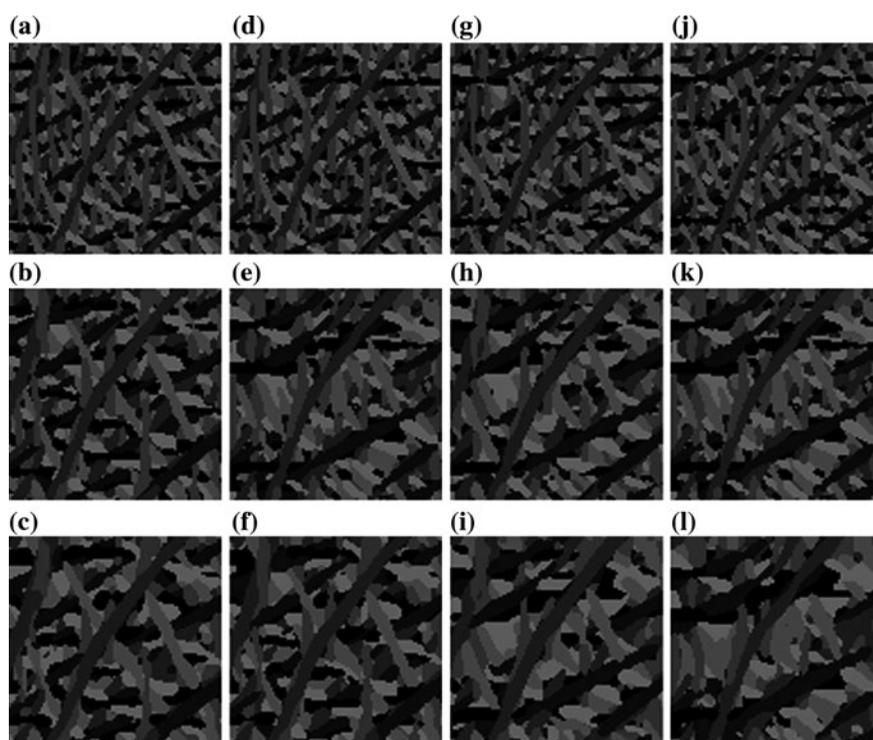


Figure 3.8 : Carte des caractéristiques extraites de la Figure 3.5. Les différentes valeurs de gris représentent des caractéristiques d'orientation différentes. Les trois cartes dans chaque colonne de gauche à droite sont toutes extraites du même ROI mais en utilisant trois paramètres différents. Ainsi, a-c est extrait du bleu ; d-f est extrait du vert ; et g-i est extrait du rouge. Les cartes de la quatrième colonne, j-l, sont extraites du RNI. Le même paramètre est utilisé pour chaque ligne

Orientation value	Bit 0	Bit 1	Bit 2
0	0	0	0
$\pi/6$	0	0	1
$\pi/3$	0	1	1
$\pi/2$	1	1	1
$2\pi/3$	1	1	0
$5\pi/6$	1	0	0

Tableau3.1: Representation en bits du codage d'orientation

3.5.2. Programme de fusion au niveau des scores :

En général, on utilise plus d'informations, ce qui permet d'obtenir de meilleures performances. Cependant, comme les informations discriminantes se chevauchent quelque peu entre les différentes bandes, la simple somme des scores correspondants de toutes les bandes peut ne pas améliorer beaucoup la précision finale. Supposons qu'il existe k types de caractéristiques ($F_i^X, i = \{1, 2, \dots, k\}$).

Pour deux échantillons X et Y, la distance utilisant la simple règle de la somme est définie comme suit :

$$d_{sum}(X, Y) = \sum_{i=1}^k d(F_i^X, F_i^Y) \quad (3.3)$$

où $d(F_i^X, F_i^Y)$ est la distance pour la $i^{\text{ème}}$ caractéristique.

La figure 3.8 montre un exemple de fusion de points par sommation. Il existe deux types de caractéristiques ($F_i^X, i = \{1, 2\}$) pour trois échantillons $\{X1, X2, Y1\}$, où X1 et X2 appartiennent à la même classe et Y1 appartient à une autre classe. Avec l'équation 3.3, nous pouvons obtenir $d_{sum}(X1, X2) = 9$ et $d_{sum}(X1, Y1) = 8$. En fait, les distances réelles entre X1 et X2, et X1 et Y1 sans chevauchement d'informations devraient être respectivement 5 et 6.

Comme il y a un chevauchement entre les deux caractéristiques, il sera compté deux fois en utilisant la règle de la somme (Eq. 3.3). Parfois, ce type de surcharge de calcul peut faire échouer la fusion simple au niveau du score, comme le montre l'exemple ci-dessus. Pour les images d'empreintes palmaires multispectrales, la plupart des caractéristiques de chevauchement entre deux bandes spectrales se situent sur les lignes principales, comme le montre la figure 3.9. En utilisant la règle de la somme (Eq. 3.3), ces caractéristiques de lignes seront sur-comptées de sorte qu'il peut ne pas être possible de classer deux paumes avec des lignes principales similaires.

L'analyse ci-dessus montre que si l'on peut trouver une stratégie de fusion au niveau du score pour réduire l'effet de chevauchement, on peut s'attendre à un meilleur résultat de vérification.

$$\begin{array}{l}
 \begin{array}{cccccccc}
 F_1^{X1} & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 \\
 & & & & & & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0
 \end{array}
 \xrightarrow{\begin{array}{c} F_1 \cup F_2 \\ F_2^{X1} \end{array}}
 \begin{array}{cccccccc}
 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0
 \end{array} \\
 \\
 \begin{array}{cccccccc}
 F_1^{X2} & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 \\
 & & & & & & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0
 \end{array}
 \xrightarrow{\begin{array}{c} F_1 \cup F_2 \\ F_2^{X2} \end{array}}
 \begin{array}{cccccccc}
 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0
 \end{array} \\
 \\
 \begin{array}{cccccccc}
 F_1^{Y1} & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
 & & & & & & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1
 \end{array}
 \xrightarrow{\begin{array}{c} F_1 \cup F_2 \\ F_2^{Y1} \end{array}}
 \begin{array}{cccccccc}
 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1
 \end{array}
 \end{array}$$

Figure. 3.9 : Un exemple de fusion de la somme des scores

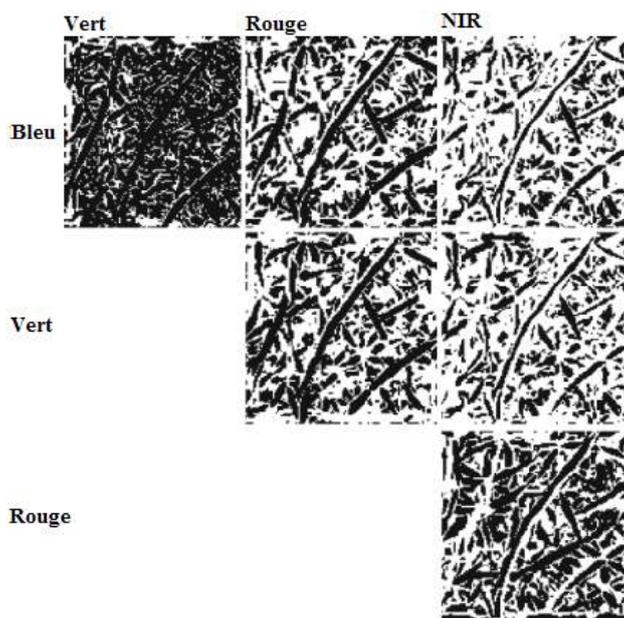


Figure. 3.10 : Caractéristiques de chevauchement entre différents spectres. (Les pixels noirs représentent les éléments qui se chevauchent, tandis que les pixels blancs représentent les éléments qui ne se chevauchent pas).

3.6. Conclusion :

L'empreinte palmaire est une caractéristique biométrique unique et fiable d'une grande facilité d'utilisation. Avec la demande croissante des systèmes d'authentifications d'empreintes palmaires très précis et robuste, l'imagerie multispectrale a été utilisée pour acquérir des informations plus discriminantes et augmenter la capacité de non appropriation de l'empreinte palmaire. Dans ce chapitre nous avons présenté un système d'empreinte palmaire multispectrale en ligne qui pourrait répondre aux exigences d'une application en temps réel. Son dispositif d'acquisition de données est conçu pour capturer les images d'empreintes palmaires sous des illuminations bleues, vertes, rouges et proche infrarouge (NIR) en moins d'une seconde. Les résultats expérimentaux établis sur ce système montrent que le canal rouge donne le meilleur résultat, tandis que les canaux bleu et vert ont des performances comparables mais sont légèrement inférieurs au canal NIR. Nous avons également expliqué la fusion d'une manière succincte et présenté un schéma de fusion au niveau du score pour intégrer les informations multispectrales.

Bibliographie

Introduction

[1]

<https://www.thalesgroup.com/fr/europe/france/dis/gouvernement/inspiration/biometrie>

[2] Wayman, James L., Jain, Anil K., Maltoni, Davide, *et al.* (ed.). *Biometric systems: Technology, design and performance evaluation*. Springer Science & Business Media, 2005.

[3] Charfi, Nesrine. Biometric recognition based on hand shape and palmprint modalities. 2017. Thèse de doctorat.

Chapitre I

[1] Nuance, <http://www.nuance.com>

[2] S. Liu, M. Silver man, « A Practical Guide to Biometric SecurityTechnology », IEEE Computer Society, IT Pro-Security, Janvier-Février 2001.

[3] Charfi, N. (2017). Reconnaissance biométrique basée sur les modalités de la forme de la main et de l'empreinte palmaire(Doctoral dissertation, Ecole nationale supérieure Mines- Télécom Atlantique Bretagne Pays de la Loire).

[4] <http://www.biometrie-online.net>

[5] El-Abed, M. (2011). Évaluation de système biométrique (Doctoral dissertation, Université de Caen).

[6] J. Daugman. Recognizing Persons by Their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in a Networked Society*, pp. 103- 121, Kluwer Academic Publishers, 1999.

[7] Zitouni Sif Eddine, Saci Abde Imoumen. Authentification et Identification biométrique des personnes par les empreintes palmaires. Mémoire Master Académique. Université Kasdi- Merbah.Ouargla. Algérie. 01/06/2016.

[8] Boussafeur Yousra, Yeddiou Idriss. La biométrie multimodale basée sur la fusion de la reconnaissance de visage et l’empreinte palmaire. Mémoire Master Académique. Université Larbi Ben M'hidi Oum El Bouaghi. Algérie. 2016/ 2017.

[9] Bouzidi adel, Système de reconnaissance des empreintes palmaires. Mémoire Master Académique. Université Mohamed Khider de Biskra. Algérie. 2017/2018.

[10] Yang, B., Wang, X., Yao, J., Yang, X., & Zhu, W. (2013). Efficient local representations for three-dimensional palmprint recognition. *Journal of Electronic Imaging*, 22(4), 043040-043040.

[11] A.N. Akansu, W.A. Serdij, I.W. Selesnick, *Wavelet Transforms in Signal Processing: A Review of Emerging Applications*, Physical Communication, Elsevier, vol. 3, issue 1, pp. 1-18, March 2010

Chapitre II

[1] Zhou, K., Zhou, X., Yu, L., Shen, L., & Yu, S. (2019). Double biologically inspired transform network for robustz palm print recognition. *Neurocomputing*, 337, 24-45.

[2] Chaa, M. (2018). *Système De Reconnaissance De Personne Par Des Techniques Biométriques* (Doctoral dissertation).

[3] Fei, L., Zhang, B., Zhang, W., &Teng, S. (2019). Local apparent and latent direction extraction for palm print recognition. *Information Sciences*, 473, 59-72.

[4] W. Boukharri et M. Benyetou, ‘Identification Biométrique des Individus par leurs Empreintes Palmaires : Classification par la Méthode des Séparateurs à Vaste Marge (SVM)’, Mémoire de Magister, UST Oran, Octobre 2007.

[5] K. Barka Et Y. Boukhris, ‘ Système d’identification biométrique à base d’un modèle flou’, Mémoire de Master, Ouargla, 2016.

[6] Tamije Selvy, A. Anjugam Et P. Arifa, ‘Authentiquassions Using Palm Print Recognition System’, *International Journal of Engineering Développement and Research*, Vol.5, No.1, 2017.

[7] A. Kong, D. Zhang, Et K. Kamel,” Palm print identification using feature-level fusion”, *Journal of pattern recognition*, Vol 39, pp. 478-487; Aout 2005.

[8] D. Santos Martine, ‘Biometric recognition based on the texture along Palmprint principal lines’, Thèse de masters, university de Porto, 2011.

[9] Aykut, M., &Ekinci, M. (2015). Developing a contactless palmprint authentication system by introducing a novel ROI extraction method. *Image and Vision Computing*, 40, 65-74.

[10] Genovese, A., Piuri, V., &Scotti, F. (2014). *Touchless palmprint recognition systems* (Vol. 60). Switzerland: Springer.

[11] Zhong, D., Du, X., &Zhong, K. (2019). Decade progress of palmprint recognition: A brief survey. *Neurocomputing*, 328, 16-28.

[12] Towards contactless palm print recognition: A novel device, a new benchmark, and a collaborative representation based identification approach.

[13] Hong, D., Liu, W., Su, J., Pan, Z., & Wang, G. (2015). A novel hierarchical approach for multispectral palm print recognition. *Neurocomputing*, 151, 511-521.

[14] Han, D., Guo, Z., & Zhang, D. (2008, Octobre). Multispectral palm print recognition using wavelet-based image fusion. In *Signal Processing, 2008. ICSP 2008. 9th International Conference on* (pp. 2074-2077). IEEE.

Chapitre III

[1] Jain A, Bolle R, Pankanti S (1999) *Biometrics: personal identification in network society*. Kluwer, Boston

[2] Zhang D (2000) *Automated biometrics—technologies and systems*. Kluwer, Boston

[3] Wu X, Zhang D, Wang K (2003) Fisherpalm based palmprint recognition. *Pattern Recogn Lett* 24 (15):2829–2838

[4] Schukers SAC (2002) Spoofing and anti-spoofing measures. *Inf Secur Tech Rep* 7(4):56–62

[5] Rowe RK, Nixon KA, Corcoran SP (2005) Multispectral fingerprint biometrics. In: *Proceedings of information assurance workshop*, pp 14–20

[6] Singh R, Vatsa M, Noore A (2008) Hierarchical fusion of multispectral face images for improved recognition performance. *Inf Fusion* 9(2):200–210

[7] Park JH, Kang MG (2007) Multispectral iris authentication system against counterfeit attack using gradient-based image fusion. *Opt Eng* 46(11):117003-1–117003-14

[8] Hao Y, Sun Z, Tan T (2007) Comparative studies on multispectral palm image fusion for biometrics. In: *Asian conference on computer vision*, pp 12–21

-
- [9] Hao Y, Sun Z, Tan T, Ren C (2008) Multispectral palm image fusion for accurate contact-free palmprint recognition. In: International conference on image processing, pp 281–284
- [10] Rowe RK, Uludag U, Demirkus M, Parthasaradhi S, Jain AK (2007) A multispectral whole-hand biometric authentication system. In: Proceedings of biometric symposium. biometric consortium conference. Baltimore, September
- [11] Likforman-Sulem L, Salicetti S, Dittmann J, Ortega-Garcia J, Pavesic N, Gluhchev G, Ribaric S, Sankur B (2007) Final report on the jointly executed research carried out on signature, hand and other modalities. http://www.cilab.upf.edu/biosecure1/public_docs_deli/BioSecure_Deliverable_D07-4-4_b2.pdf.pdf
- [12] Wang J-G, Yau W-Y, Suwandy A, Sung E (2008) Person recognition by fusing palmprint and palm vein images based on “Laplacianpalm” representation. *Pattern Recogn* 41(5):1514–1527
- [13] Ross AA, Nadakumar K, Jain AK (2006) *Handbook of multibiometrics*. Springer, Berlin
- [14] Gawkrödger DJ (2002) *Dermatology: an illustrated color text*, 3rd ed. Elsevier, Amsterdam
- [15] Zharov VP, Ferguson S, Eidt JF, Howard PC, Fink LM, Waner M (2004) Infrared imaging of subcutaneous veins. *Lasers Surg Med* 34(1):56–61
- [16] Zhang D, Kong W, You J, Wong M (2003) Online palmprint identification. *IEEE Trans Pattern Anal Mach Intell* 25(9):1041–1050
- [17] A.N. Akansu, W.A. Serdij, I.W. Selesnick, *Wavelet Transforms in Signal Processing: A Review of Emerging Applications*, Physical Communication, Elsevier, vol. 3, issue 1, pp. 1-18, March 2010.
- [18] A. Uhl and P. Wild, Personal recognition using single-sensor multimodal hand biometrics, *International Conference on Image and Signal Processing*, pp. 396-404, 2008.
- [19] J. Wu, Z. Qiu, and D. Sun, A hierarchical identification method based on improved hand geometry and regional content feature for low- resolution hand images, *Signal Processing*, 88, pp. 1447-1460, 2008.
- [20] Shivsubramani Krishnamoorthy, K P Soman, “Implementation and Comparative Study of Image Fusion Algorithms”, *International*
- [21] Connie T, Andrew T, Goh K (2005) An automated palmprint recognition system. *Image Vis*
-

-
- [22] Hu D, Feng G, Zhou Z (2007) Two-dimensional locality preserving projections (2DLPP) with its application to palmprint recognition. *Pattern Recogn* 40(1):339–342
- [23] Han C, Cheng H, Lin C, Fan K (2003) Personal authentication using palm-print features. *Pattern Recogn* 36(2):371–381
- [24] Wu X, Zhang D, Wang K (2006) Palm line extraction and matching for personal authentication. *IEEE Trans Syst Man Cybern Part A* 36(5):978–987
- [25] Kong A, Zhang D, Kamel M (2006) Palmprint identification using feature-level fusion. *Pattern Recogn* 39(3):478–487
- [26] Kong A, Zhang D (2004) Competitive coding scheme for palmprint verification. *Int Conf Pattern Recogn* 1:520–523
- [27] Jia W, Huang D-S, Zhang D (2008) Palmprint verification based on robust line orientation code. *Pattern Recogn* 41(5):1504–1513.
-