République Algérienne Démocratique et Populaire

Ministère de l'enseignement supérieur et de la recherche scientifique

Université 8Mai 1945 – Guelma

Faculté des sciences et de la Technologie

Département d'Electronique et Télécommunications

Mémoire de fin d'étude

Pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**

Filière : **Electronique**

Spécialité : **Instrumentation**

Etude d'un Système Biométrique à Base d'un Descripteur De Motif à Double Croisement

---

Présenté par :

Redjimi Salim

Bouchmal Wahid

Sous la direction de Mr :

Dr. Bourouba hocine

Octobre 2020

Remerciement

Tout d'abord nous tenons à remercier ***« ALLAH »*** *pour nous avoir donné le courage, la force et la volonté pour réussir et de nous avoir éclairci le chemin tout au long de notre vie.*

La première personne que nous tenons à remercier est notre encadreur professeur Mr. BOUROUB.H, pour avoir accepté de nous encadrer, aussi pour son orientation, et sa patience qui ont constitué un apport considérable sans lequel ce travail n'aurait pas pu être mené au bon port. Qu'il trouve dans ce travail un hommage vivant à sa haute personnalité.

Nos remerciements s'étendent également au professeur Mr. DOGHMANE.H pour ses bonnes explications qui nous ont éclairé le chemin son collaboration avec nous dans l'accomplissement de ce modeste travail.

Nous tenons à exprimer nos sincères remerciements à tous les professeurs qui nous ont enseigné et qui par leurs compétences nous ont soutenu dans la poursuite de nos études.

Enfin, on remercie tous ceux qui, de près ou de loin, ont contribué à la réalisation de ce travail.

Merci

Introduction Générale

Savoir déterminer de manière à la fois efficace et exacte l'identité d'un individu est devenu un problème critique dans notre société. En effet, bien que nous ne nous en rendions pas toujours compte, 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. Il existe traditionnellement deux manières d'identifier un individu. La première méthode est basée sur une connaissance (knowledge-based). Cette connaissance correspond par exemple au mot de passe utilisé au démarrage d'une session Unix ou au code qui permet d'activer un téléphone portable. La seconde méthode est basée sur une possession (token-based). Il peut s'agir d'une pièce d'identité, une clef, un badge, etc. Ces deux modes d'identification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue comme pour la carte bleue. Cependant, elles ont leurs faiblesses respectives. Dans le premier cas, le mot de passe peut-être oublier par son utilisateur ou bien deviné par une autre personne. On estime ainsi qu'une personne sur quatre écrits directement sur sa carte bleue son code secret afin de ne pas l'oublier [1]. Dans le second cas, le badge (ou la pièce d'identité ou la clef) peut être perdu ou volé. 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, 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 : « No PIN to remembre, no PIN to Forget ») ou perdu. En général, ils sont très difficiles à deviner ou à voler ainsi qu'à dupliquer [27]. Nous décrivons maintenant les propriétés souhaitables d'une caractéristique biométrique [19]. Cette caractéristique doit être universelle, c'est-à-dire que toutes les personnes de la population à identifier doivent la posséder. Elle doit être à la fois facilement et quantitativement mesurable. Elle doit être unique, c'est-à-dire que deux personnes ne peuvent posséder exactement la même caractéristique. Elle doit être permanente, ce qui signifie qu'elle ne doit pas varier au cours du temps. Elle doit être performante, c'est-à-dire que l'identification doit être précise et rapide. Elle doit être bien acceptée par les utilisateurs du système. Enfin elle doit être impossible à dupliquer par un imposteur.

Le travail présenté dans cette thèse se compose de quatre chapitres :

Le Chapitre 1 présente la biométrie de manière générale ainsi que les différents types de modalités et leurs rôles dans notre vie quotidienne. Chapitre 2 présente les Systèmes biométriques et leurs structures ainsi que le mode de fonctionnement et les critères d'évaluation. Chapitre 3 est consacré à la description de l'empreinte palmaire, ses avantages, les différents types du système de reconnaissance biométrique de l'empreintes palmaires. Chapitre 4 est réservé à la partie expérimentale qui est basée sur le principe de la méthode de DCP (Dual Cross Pattern). Nous terminons notre travail par une conclusion générale.

Résumé

Depuis ces dernières années, l'authentification humaine joue un rôle important dans l'environnement temps réel. La principale raison de l'application de solutions biométriques est la sécurité. Entre autres, les empreintes palmaires sont de plus en plus utilisées comme une nouvelle modalité biométrique pour l'identification et la vérification humaines. Les images d'empreintes palmaires capturées dans le visible et l'infrarouge ne contiennent pas seulement les rides et la structure des crêtes de l'épiderme mais aussi le motif sous-jacent des veines, ce qui les rend un identifiant biométrique très discriminant.

Dans notre travail, nous essayons d'évaluer l'utilité de l'application de la méthode DCP dans un système biométrique d'empreintes palmaires pour améliorer le taux d'identification des personnes basés sur les empreintes palmaires. Pour ce faire, nous proposons un système d'identification d'empreintes palmaires basé sur le descripteur DCP qui s'applique sur chaque image de l'empreinte palmaire. L'idée est d'extraire les caractéristiques texturales de chaque image d'empreinte palmaire pour traiter les caractéristiques uniques inhérentes à l'empreinte palmaire. Ces caractéristiques sont ensuite encodées sous forme d'histogramme dont la dimension des caractéristiques est réduite à l'aide de l'analyse discriminante (LDA) avant d'effectuer la classification. Le système proposé est appliqué à la base de données IIT DELHI. Les résultats obtenus montrent que la méthode proposée donne des performances très encourageantes avec un taux de reconnaissance de 99%

Mots clés : Biométrie, Empreintes palmaires, Multi spectral, Identification, Système biométrie, Apprentissage, LDA, DCP

Abstract

In recent years, human authentication has played an important role in the real-time environment. The main reason for applying biometric solutions is security. Among other things, palm prints are increasingly used as a new biometric modality for human identification and verification. Multispectral palm print images captured in the visible and infrared contain not only the wrinkles and ridge structure of the epidermis, but also the underlying pattern of the veins, making it a highly discriminating biometric identifier.

In our work, we try to assess the utility of multispectral palm print images to improve a palm print based human identification system. To do this, we propose a system for identifying palm prints based on the DCP descriptor which is applied to each spectral image. The idea is to extract the textural characteristics of each palm print spectral image to process the unique characteristics inherent in the palm print. These characteristics are then encoded in the form of a histogram whose characteristic dimension is reduced using discriminant analysis (LDA) before performing the classification. The proposed system is applied to the IIT DELHI database. The results obtained show that the proposed strategy gives very encouraging performances with a recognition rate of 99%.

Key words: Biometrics, Palm Prints, Multispectral, Identification, Biometric system, Apprenticeship, LDA, DCP

الملخـص

في السنوات الأخيرة، لعب التحقق من الهوية البشرية دورًا مهمًا في حدود الوقت الفعلي. السبب الرئيسي لتطبيق حلول القياسات الحيوية هو الأمان. من بين أمور أخرى، يتم استخدام بصمات اليد بشكل متزايد كطريقة بيومترية جديدة لتحديد هوية الإنسان والتحقق منه. لا تحتوي صور بصمة الكف متعددة الأطياف التي تم التقاطها في الأشعة المرئية والأشعة تحت الحمراء على التجاعيد وبنية التلال للبشرة فحسب، بل تحتوي أيضًا على النمط الأساسي للأوردة، مما يجعلها معرفًا بيولوجيًا مميزًا للغاية.

في عملنا هذا، نحاول تقييم فائدة صور بصمات اليد متعددة الأطياف لتحسين نظام التعريف البشري القائم على بصمة الكف. للقيام بذلك، نقترح نظامًا لتحديد بصمات اليد بناءً على واصف DCP الذي يتم تطبيقه على كل صورة طيفية. الفكرة هي استخراج الخصائص التركيبية لكل صورة طيفية لطباعة الكف لمعالجة الخصائص الفريدة الكامنة في بصمة الكف. ثم يتم ترميز هذه الخصائص في شكل مدرج تكراري يتم تقليل أبعاده المميزة باستخدام التحليل المميز (LDA) قبل إجراء التصنيف. يتم تطبيق النظام المقترح على قاعدة بياناتIIT DELHI ، تظهر النتائج التي تم الحصول عليها أن الاستراتيجية المقترحة تعطي أداء مشجعا للغاية بمعدل اعتراف 99٪.

الكلمات المفتاحية :البيومترية، بصمة اليد، متعددة الأطياف، تحديد نظام القياسات الحيوية، التعلم، خصائص الصورة الإحصائية الثنائية، التحليل الخطي للتمييز.

Chapitre 1

La biométrie

Sommaire

Liste de figure :

1. Définition :

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique.

La biométrie est la reconnaissance automatique des personnes qui ont leurs caractéristiques comportementales privées telles que la voix, la signature ou physiologique comme le visage, l'empreinte digitale. Ces caractéristiques sont appelées modalités biométriques [1]. Les modalités biométriques ne peuvent pas être facilement oubliées, perdus, échangés ou volés. Ils sont également permanents, ce qui signifie qu'ils ne changent pas, ou peu, au fil du temps. Grâce à ces propriétés La reconnaissance biométrique a été l'une des solutions les plus sécurisées dans les dernières années qui convient aux applications qui exigent une sécurité élevée, comme l'accès à l'aéroports, centrales nucléaires, contrôle des frontières, banques, etc. [2]

1.2. Les modalités biométriques :

Il existe plusieurs modalités biométriques utilisées dans divers secteurs, On peut distinguer trois catégories :

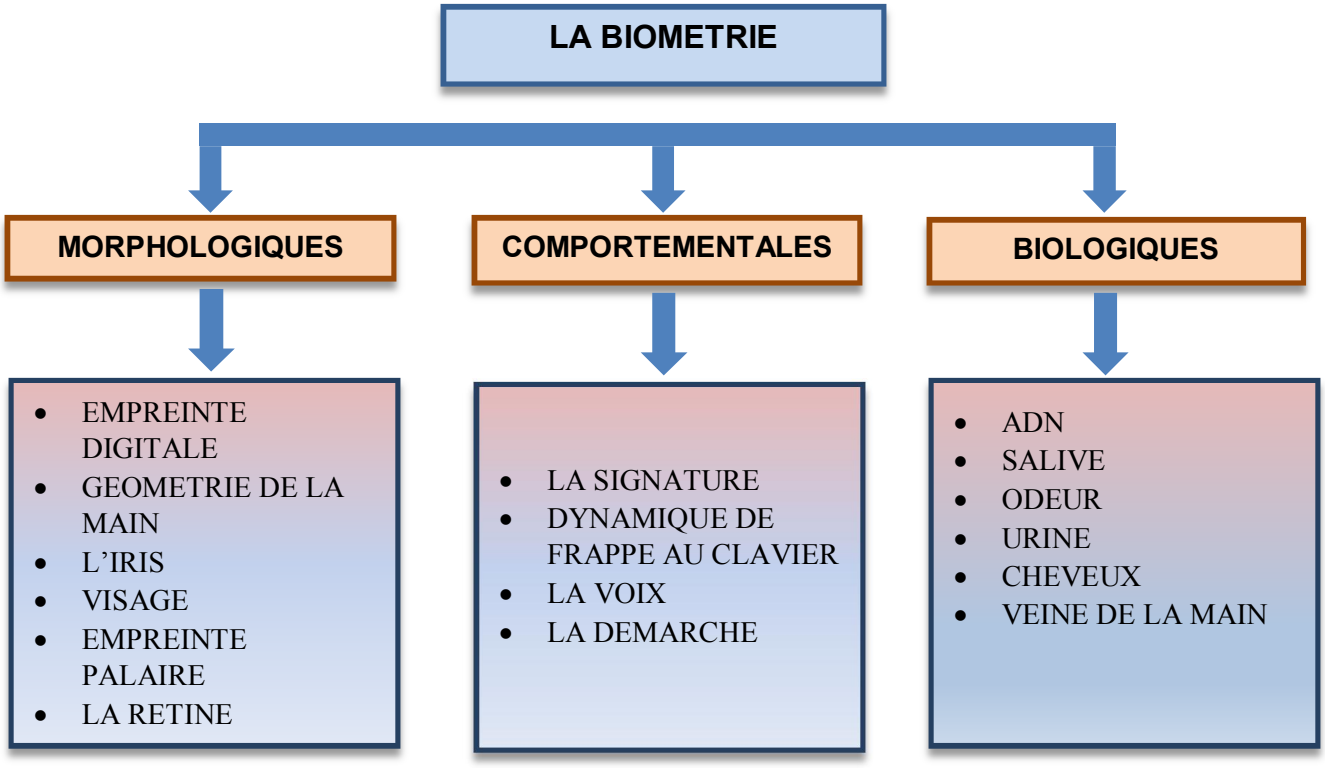


Figure 1.1: Classification d'un certain nombre de modalités biométriques.

1.2.1. Les modalités morphologiques :

Ce sont des modalités basées sur l'identification des traits physiologiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe l'iris de l'œil, la forme de la main, les empreintes digitales, les traits du visage, etc.

1.2.1.1 L'empreinte palmaire : Cette technique utilise la surface intérieure de la paume pour l'identification et/ou la vérification des personnes. Elle est bien adaptée pour les systèmes de moyenne sécurité telle que le contrôle d'accès physique ou logique.

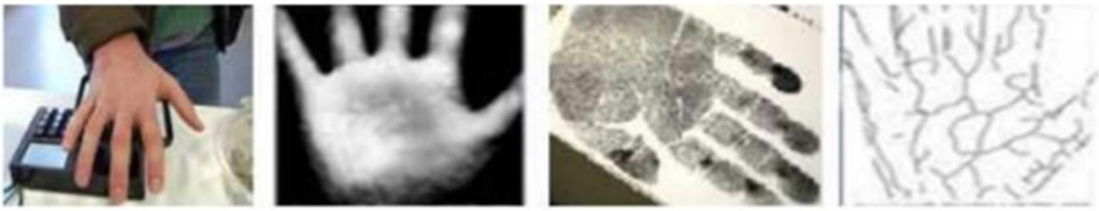


Figure 1.2: Empreinte palmaire

1.2.1.2 Les Empreintes digitales : Il s'agit d'une des premières biométries utilisées dans des machines d'authentification, La formation des empreintes dépend des conditions initiales développement embryogénique, ce qui les rend uniques à chaque personne et même à chaque doigt.

Figure 1.3: Images de l'empreinte digitale

1.2.1.3 Géométrie de la main : Il consiste à mesurer plusieurs caractéristiques de la main (jusqu'à 90) telle que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter articulations, &etc. La technologie associée à cela est principalement de l'imagerie infrarouge.

Figure 1.4: Géométrie de la main

1.2.1.4 L'iris : est la membrane colorée de l'Sil. Une caméra proche des infrarouges photographie une tranche de l'iris, elle relève les caractéristiques particulières du relief.

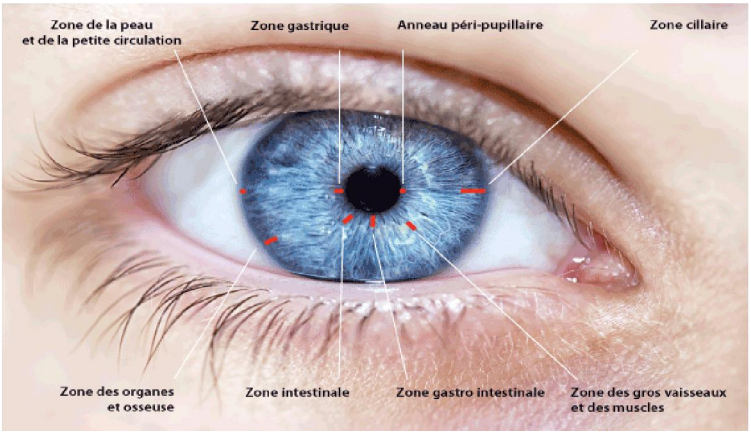


Figure 1.5: L'iris

1.2.1.5 La rétine : Il a été montré que chaque S'il possède en sa rétine un vaisseau sanguin. La technique basée sur la rétine utilise la texture de ces vaisseaux. L'identification consiste à éclairer le fond de l'Sil par un faisceau lumineux de faible intensité.

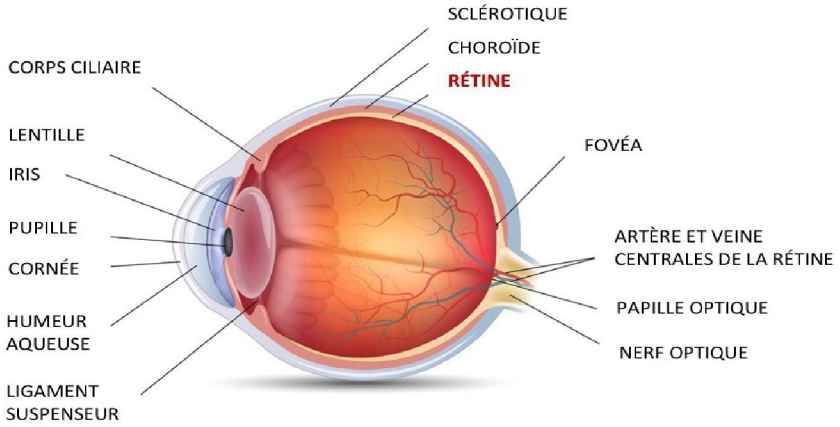


Figure 1.6: La rétine

1.2.1.7 Le visage : Il s'agit de capter la forme du visage d'un individu et d'en extraire certaines informations jugées évidentes pour l'authentification.

Selon le système utilisé, l'individu doit être positionné devant l'appareil où peut-être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence. Au début des années 1970, la reconnaissance par le visage était principalement basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme, & etc. Depuis les années 1990, les différentes technologies utilisées exploitent toutes les découvertes effectuées dans le domaine du traitement d'image et de l'analyse de données.

Figure 1.7 : Visage

1.2.2. Les modalités comportementales :

Ce sont des modalités basées sur l'analyse de certains comportements d'une personne comme.

1.2.2.1 L'écriture (la signature) :

Les systèmes de reconnaissance de l'écriture consistent à analyser les caractéristiques spécifiques d'une signature comme la vitesse, la pression sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé. Elle se base généralement sur le fait que l'utilisateur signe avec un stylo électronique sur une palette graphique et au même temps elle examine l'ensemble de dynamique comme la vitesse, la direction, et la pression de l'écriture, le temps pendant lequel le stylo est en contact avec le papier, le temps pris pour faire la signature et les positions où le stylo est relevé et abaissé sur le papier.

Figure 1.8 : Système de reconnaissance de signature.

1.2.2.2 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. Elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à « imiter » Lors de la mise en place de cette technique, il est demandé à l'utilisateur de saisir son mot de passe une dizaine de fois de suite. A l'aide d'un algorithme qui exploite le temps d'appui sur chaque touche et le temps entre chaque touche, la dizaine de saisie est « moyennée » pour bâtir un Profil de frappe » de l'utilisateur qui servira de référence. Aux accès suivants, en suivant la même approche, la saisie du mot de passe donnera sera couplée à un profil de frappe qui sera comparé au profil de référence.

Figure 1.9 : Système de reconnaissance de frappe au clavier.

1.2.2.3 La voix (Reconnaissance vocale) :

La reconnaissance par voix utilise les caractéristiques vocales pour identifier les personnes en utilisant des phrases mot de passe. L'identification de la voix est considérée par les utilisateurs comme une des formes les plus normales de la technologie biométrique, car elle n'est pas intrusive et n'exige aucun contact physique avec le lecteur du système. [3].

Figure 1.10: Image de la Reconnaissance vocale

1.2.2.4 La démarche **:** On peut aussi modéliser la démarche d'une personne à travers plusieurs techniques, mais le problème c'est qu'on peut tromper ce système facilement. La biométrie de la marche est une biométrie basée sur la marche de la personne. Ça devrait être Mentionné que la marche n'est pas affectée par la vitesse de la marche de la personne. Certains scientifiques distinguent la démarche de la reconnaissance de la démarche, soulignant que la démarche peut être Considérée comme une combinaison cyclique de mouvements qui entraîne la locomotion humaine et la reconnaissance de la démarche est la reconnaissance de certain style de propriété de la marche, la pathologie, etc. Les paramètres communs de l'analyse de la marche sont [4] :

- Paramètres cinématiques tels que le genou, les mouvements de la cheville et les angles.

- Paramètres spatiotemporels tels que la longueur et la largeur des marches, la vitesse de marche.

1.3. Les avantages de la biométrie :

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique.

L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce. - Suppression des mots de passe, Suppressions des clés :

Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur. - Utilisation d'une signature biométrique : Grande sécurité, intransmissible à une autre personne. Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données). Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr. La biométrie constitue le chaînon manquant dans la triade des problèmes de sécurité :

- Diminution de la fraude.

- Rehaussement de l'intégrité des informations et la sécurité.

- Réduction des attaques à l'égard des programmes gouvernementaux.

- Croissance de la confiance envers les systèmes de sécurité.

- Diminution des frais administratifs.

- Accélération des services.

1.4 Domaines d'application :

Nous pouvons distinguer quatre applications biométriques principales : le contrôle d'accès, l'authentification des transactions, l'application de la loi et la personnalisation.

1.4 **Contrôle d'accès :** Le contrôle d'accès lui-même peut être divisé en deux sous-catégories : le contrôle d'accès physique et le contrôle d'accès virtuel. Nous parlons de contrôle d'accès physique lorsque les utilisateurs cherchent à accéder à des

emplacements sécurisés. Nous parlons de contrôle d'accès virtuel dans les situations où les utilisateurs essaient d'accéder à des ressources ou des services.

1.4.2 Le contrôle d'accès physique : utilise depuis longtemps des clés ou des badges pour accéder à des lieux sécurisés (tels que des bâtiments ou des chambres). Il y a une photo sur le badge, qui est vérifiée par un agent de sécurité. Grâce à la technologie biométrique, la même opération peut désormais être effectuée automatiquement. L'une des géométries en forme de main les plus couramment utilisées pour le contrôle d'accès se trouve dans plusieurs grands aéroports des États-Unis (New York, Washington, Los Angeles, San Francisco, etc.). L'application permet aux passagers répertoriés dans le système de sauter la ligne de contrôle des passeports. Ils ont une carte magnétique qui contient des informations sur la forme de la main. Lorsqu'ils montrent leur main au système, ils le comparent aux informations sur la carte. [4]

1.4.3 Contrôle d'accès virtuel : Le contrôle d'accès virtuel permet, par exemple, d'accéder à des réseaux informatiques ou de sécuriser l'accès à des sites Web. Le marché du contrôle d'accès virtuel est dominé par les systèmes basés sur la connaissance (généralement des mots de passe). À mesure que le prix des systèmes de collecte baisse, les applications biométriques devraient devenir de plus en plus populaires. Un exemple d'application est l'intégration par Apple du module de reconnaissance du locuteur dans son système d'exploitation MAC OS 9 afin de protéger les fichiers de l'utilisateur, notamment lors de l'utilisation d'un ordinateur. Situation croissante par quelques personnes. [5]

1.4.5 Authentification des transactions : L'authentification des transactions représente un marché énorme car elle comprend les retraits aux guichets bancaires, les paiements par carte bancaire, les virements de fonds, les paiements effectués à distance via le téléphone ou Internet, etc. Mastercard estime que grâce à l'utilisation de la reconnaissance d'empreintes digitales intégrée La carte à puce peut réduire l'utilisation frauduleuse des cartes de crédit de 80%. Les 20% restants sont principalement dus au risque de paiement à distance. Pour les transactions à distance, des solutions ont été déployées, notamment les transactions téléphoniques. Par exemple, les clients d'un réseau de magasinage à domicile, une société de magasinage par téléphone et Charles Schwab utilisent tous la technologie de reconnaissance du locuteur de Nuance (Nuance Check TM). [6][7]

1.4.6 Répression : la criminologie est l'une des applications les plus directes de la biométrie dans l'application de la loi. L'exemple le plus célèbre est la reconnaissance d'empreintes

digitales. Elle a été acceptée au début du 20e siècle comme moyen d'identifier formellement les individus et leur utilisation. Il existe également des applications dans le domaine judiciaire. Par conséquent, T-Netix compagnie fournit une solution pour le suivi des périodes d'essai individuelles en combinant la technologie Internet et la reconnaissance du locuteur. [8]

1.4.7 Personnalisation : la biométrie peut également être utilisée pour personnaliser les appareils que nous utilisons au quotidien. Cette application de la technologie biométrique apporte une plus grande commodité d'utilisation. Afin de personnaliser les paramètres de la voiture, par exemple, Siemens a proposé l'utilisation de la reconnaissance d'empreintes digitales. Une fois l'identité de l'utilisateur expirée, tout comme les autres « nouvelles technologies » (biotechnologie, réalité virtuelle, etc.), son développement doit s'accompagner d'une réflexion approfondie sur le respect de la liberté personnelle. Après la fixation, la voiture ajustera automatiquement le siège, le rétroviseur, le climatiseur, etc.

Figure 1.11: Quelques applications de la biométrie

1.5. Conclusion :

Dans ce chapitre, nous avons présenté les différentes modalités biométriques pour l'identification des personnes, ainsi que l'utilité de son utilisation dans le domaine de la sécurité des biens et des êtres, et aussi coté disciplinaire (moyen fiable pour le contrôle de présence), Ce qui nous a rendu la vie plus facile qui se résume à ses nombreux avantages.

Chapitre 2

Système biométrique

Sommaire

Liste de figure

Listes de tableaux

2.1 Introduction :

Nous assistons aujourd'hui à une expansion de l'utilisation d'Internet dans diverses pratiques quotidiennes. La plupart de ces pratiques exigent l'authentification de l'utilisateur afin de sécuriser les communications. Comme exemples de telles applications, citons l'achat en ligne, les transactions bancaires, l'e-Gouvernement, etc. On distingue deux manières classiques d'authentification. La première est basée sur une connaissance comme un mot de passe, alors que la deuxième est basée sur une possession comme une carte à puce. Ces deux méthodes présentent quelques inconvénients. En effet, le mot de passe peut-être oublié où espionner et la carte à puce risque d'être volée ou perdue. En outre, ces deux méthodes ne permettent pas de différencier entre un client authentique et un imposteur. La biométrie s'impose de plus en plus comme alternative afin de remédier aux problèmes des méthodes précédentes. La biométrie est basée sur des caractéristiques propres à l'individu, qui ne peuvent être ni perdues, ni volées. De plus, en pratique il n'est pas assez évident d'imiter une caractéristique biométrique.

2.2 Les Systèmes biométriques : Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. L'apparition de l'ordinateur et sa capacité à traiterait à stocker les données ont permis la création des systèmes biométriques informatisés.

2.3 La structure d'un système biométrique :

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

2.3.1 Module de capture : responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.).

2.3.2 Module d'extraction de caractéristiques : qui prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.

2.3.3 Module de correspondance :

Il compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux

2.3.4 Module de décision :

Vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

Ce système est très important dont leurs avantages peuvent être résumés :

- Facile à utiliser
- Elément de dissuasion
- Coûts abordables
- Technologie arrivée à maturité

2.4 Modes de fonctionnement :

Un système biométrique est essentiellement un système de reconnaissance de formes. Il existe toujours au moins deux modules dans un système biométrique : le module ***d'apprentissage*** et celui de ***reconnaissance***. Le troisième module (facultatif) est le module d'adaptation. Donc, Il consiste principalement en deux phases (figure 2.1):

- Apprentissage (entraînement, L'enrôlement)
- Comparaison (La vérification d'identité ou l'identification)
- Adaptation (Facultatif)

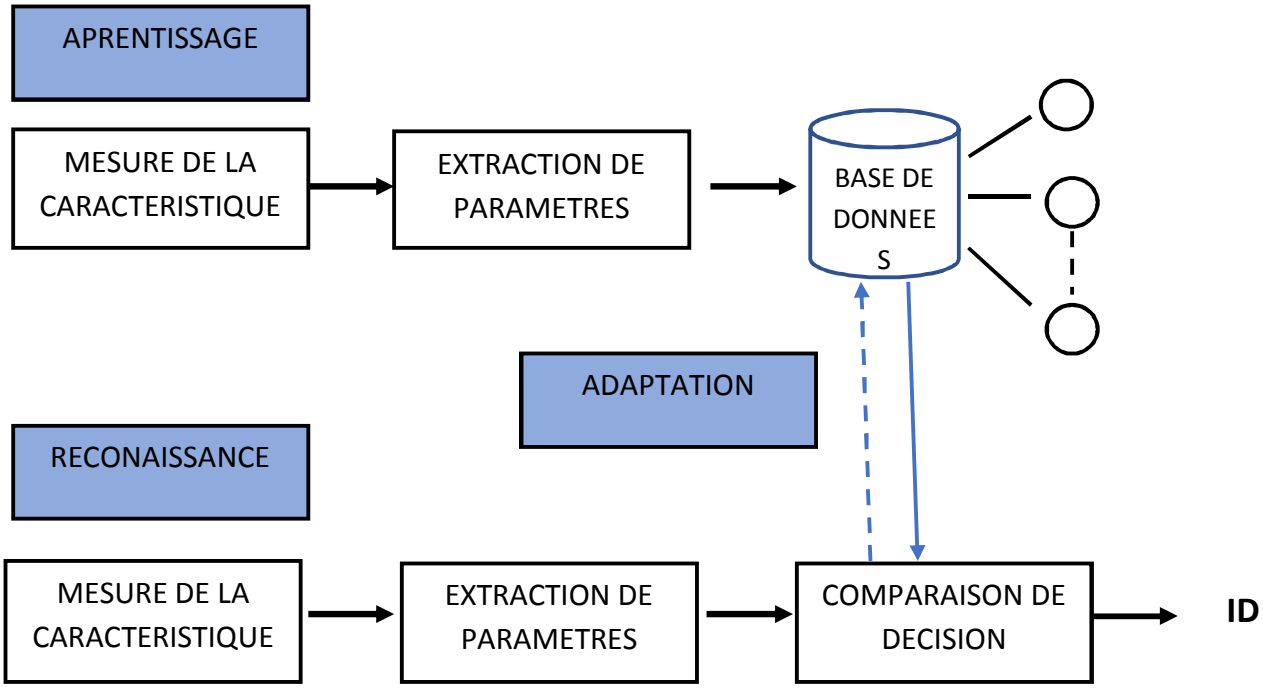


Figure 2.1 : *Architecture d'un système de reconnaissance biométrique.*

2.4.1 Apprentissage :

Dans la première phase, le système va acquérir par un dispositif dédié une ou plusieurs échantillons (généralement de 3 à 5) de la modalité biométrique d'une personne qui serviront à construire un modèle de l'individu. Ce modèle de référence servira de point de comparaison lors de la reconnaissance. Afin d'améliorer la qualité de la modalité, des prétraitements sont généralement appliqués sur les données acquises. Ensuite, des paramètres sont extraits de chaque échantillon capturé et sont stockés dans une base de données.

Il s'agit d'une étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Elle est commune à la vérification et l'identification. Pendant l'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien d´fini, afin de réduire la quantité de données à stocker pour ainsi faciliter la vérification et l'identification. Dépendant de l'application et du niveau de sécurité souhaité, le modèle biométrique retenu, est stocke soit dans une base de données centrale soit sur un élément personnel propre à chaque personne. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation.

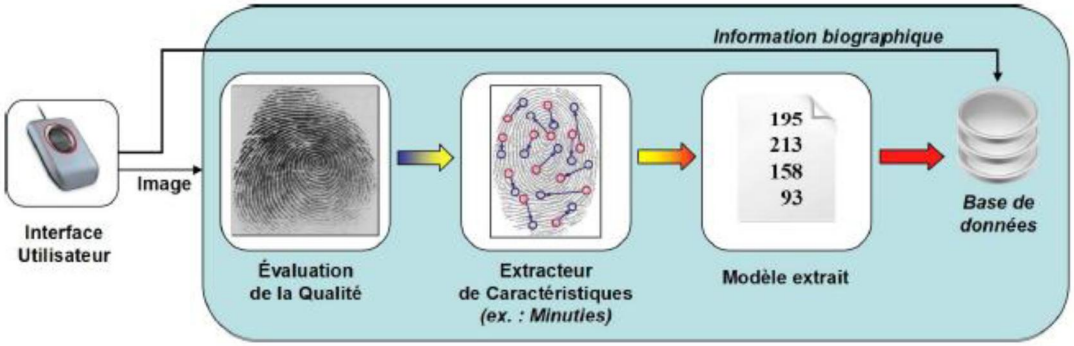


Figure 2.2 : *Enrôlement d'une personne dans un système biométrique.*

2.4.2 Comparaison

Au cours de l'étape de comparaison (reconnaissance), la même modalité biométrique de la personne, que l'on veut soit ***authentifier*** (vérifier), soit ***identifier***, est capturée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances. La suite de la reconnaissance sera différente suivant le mode opératoire du système

2.4.2.1 Vérification:

C'est la comparaison 1-à-1, entre les données biométriques capturées (model test) et les données stockée dans sa propre base (les modèles d'apprentissage). Dans un tel système, un individu qui désire être identifié réclame une identité, habituellement par l'intermédiaire d'un PIN (numéro d'identification personnelle), d'un nom d'utilisateur, d'une carte d'identité, etc.

Le système doit alors répondre à la question suivante "Suis-je réellement la personne que suis-je entrain de proclamer ?" [9].

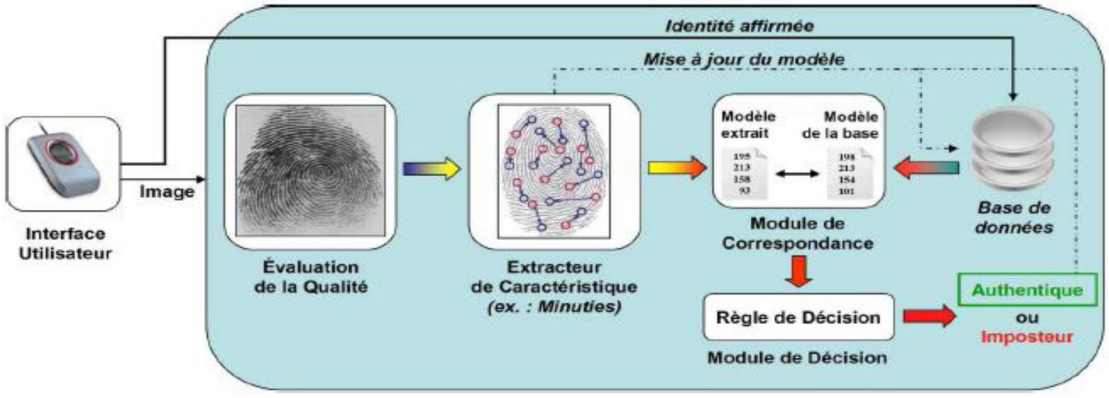


Figure 2.3: *Authentification d'un individu dans un système biométrique.*

2.4.2.2 Identification :

Le système identifie un individu en cherchant les signatures (Template) de tous les utilisateurs dans la base de données. Par conséquent, le système conduit plusieurs comparaisons 1-à-N pour établir l'identité d'un individu [10]. En résumé, un système biométrique opérant en mode identification répond à la question "Suis-je bien connu du système ?".

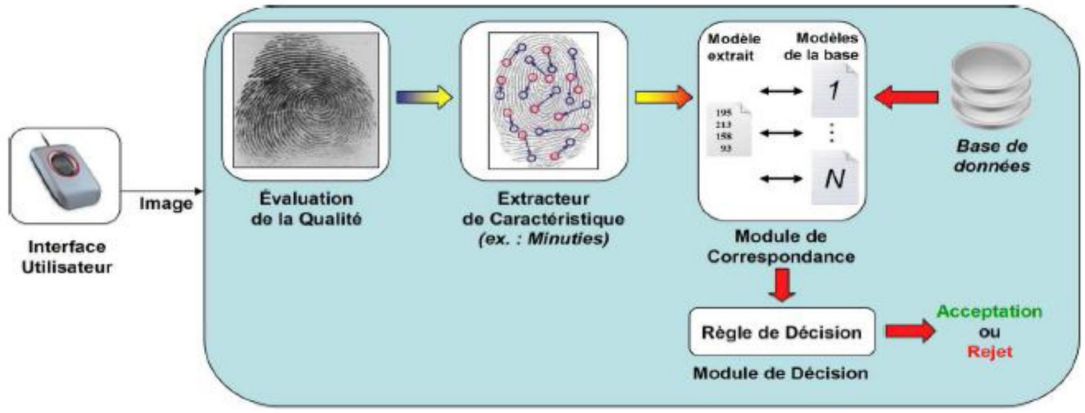


Figure 2.4 : *Identification d'un individu dans un système biométrique.*

2.4.2.3 Module d'adaptation

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire amélioré la performance d'un système utilisation après utilisation. L'adaptation peut se faire en mode supervisé ou non-supervisé mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à ré-estimer son modèle. En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur. Bien entendu, l'adaptation non-supervisée peut poser problème en cas d'erreurs du module de reconnaissance. L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix [11][12].

2.5 Critères d'évaluation des systèmes biométriques :

L'évaluation des systèmes biométriques est un enjeu majeur en biométrie pour plusieurs raisons.

Premièrement, elle donne accès aux chercheurs pour mieux tester et évaluer leurs systèmes avec ceux qui existent dans la littérature. En conséquence, elle permet de prendre en considération le comportement des utilisateurs durant le processus d'évaluation.

De plus, elle permet d'identifier, pour chaque système, les applications industrielles en se basant sur ces performances.

Ces derniers dépendent de plusieurs circonstances de test incluant

- Le capteur utilisé
- Le protocole d'acquisition
- La disposition de la personne
- Le nombre d'utilisateurs
- Le nombre d'échantillons par utilisateur
- Le profil démographique des utilisateurs
- L'habitude des utilisateurs
- Les laps de temps séparant l'acquisition, etc.

L'évaluation des systèmes biométriques a pour objectif d'en diminuer les limitations vues dans la section. L'évaluation de ces systèmes est généralement réalisée selon trois aspects d'évaluation comme le montre la figure 2.5 :

- **La performance** : qui mesure l'efficacité d'un système biométrique en termes d'erreur tel que le taux d'échec à l'acquisition (FTA) [13].
- **L'usage** : qui mesure l'acceptabilité et la satisfaction des utilisateurs lors de l'utilisation de systèmes biométriques [14].
- **La sécurité :** qui mesure la robustesse d'un système biométrique (capteur et algorithmes) contre la fraude. L'évaluation des systèmes biométriques est un enjeu majeur en biométrie pour plusieurs raisons. Premièrement, elle permet d'offrir aux chercheurs et aux développeurs un outil pour mieux tester et évaluer leurs systèmes avec ceux qui existent dans l'état de l'art. Deuxièmement, elle permet de prendre en

considération le comportement des utilisateurs durant le processus d'évaluation, ce qui permet de mieux comprendre leur besoin et mieux déployer cette technologie dans notre vie quotidienne. Enfin, elle permet d'identifier, pour chaque système, les applications industrielles en se basant sur divers critères que sont la performance, l'usage, la sécurité et le cout de déploiement de la technologie [15].

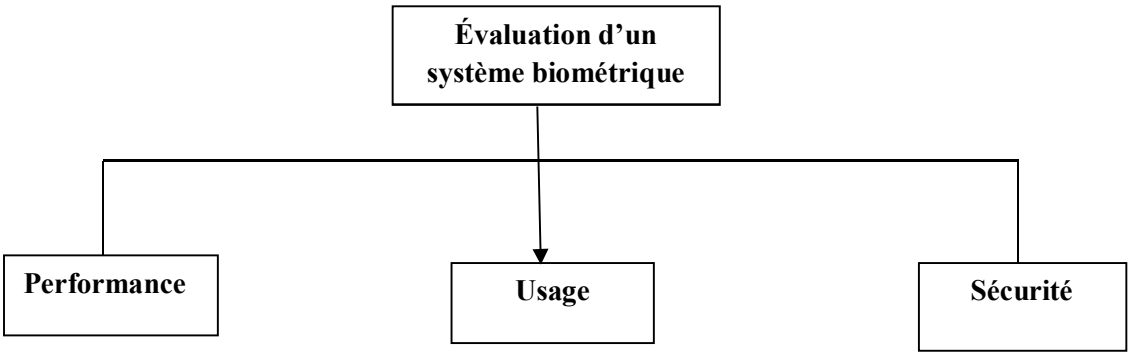


Figure 2.5 : *évaluation d'un système biométrique*

2.5.1 Les critères d'évaluation des systèmes de vérification biométriques :

Lorsque le système fonctionne en mode de vérification, il peut effectuer deux types erreurs :

- Il peut rejeter les utilisateurs légitimes, c'est le « faux rejet » (False rejection).
- Le deuxième cas, il peut aussi accepter des imposteurs, c'est la « fausse acceptation » (acceptation d'erreur) [16] [17].

Par conséquent, les performances du système sont mesurées par trois critères principaux

Premier critère s'appelle le taux de faux rejet ("False Reject Rate" ou FRR). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par système,

FRR = nombre de client rejeté **FRR** / nombre total d'accès clients

a) Deuxième critère est le taux de fausse acceptation ("False Accepte Rate" ou FAR). Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système :

FAR = nombre imposteur acceptés **FA** / nombre total d'accès imposteurs

b) Troisième critère est connu sous le nom de taux d'égale erreur ("Equal Error Rate" ou EER). Ce taux est calculé à partir des deux premiers critères et constitue un point de

mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations [18].

ERR = nombre de fausses acceptations (FA) + nombre de faux rejets (Fr) / nombre totale d'accès

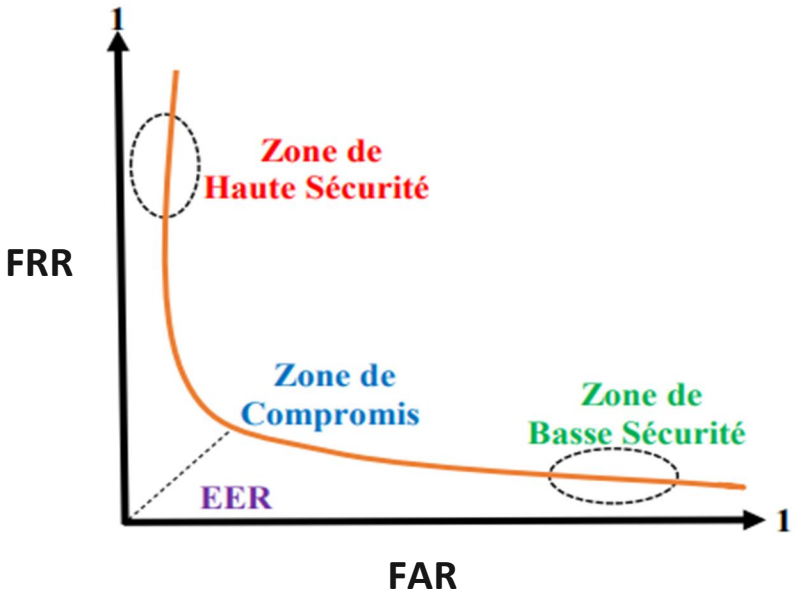


Figure 2.6 *: Distributions des taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système biométrique.*

La figure.2.6 présente, la distribution hypothétique des taux de vraisemblance qu'obtiendraient les utilisateurs légitimes et les imposteurs d'un système de vérification donné. Les FAR et FRR sont représentés en hachuré. Idéalement, le système devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Plus le seuil de décision Θ est bas, plus le système acceptera d'utilisateurs légitimes mais plus il acceptera aussi d'imposteurs. Inversement, plus le seuil de décision Θ est élevé, plus le système rejettera d'imposteurs mais plus il rejettera aussi d'utilisateurs légitimes. Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps.

La figure suivante illustre le FRR et le FAR à partir de distributions des scores authentiques et imposteurs.

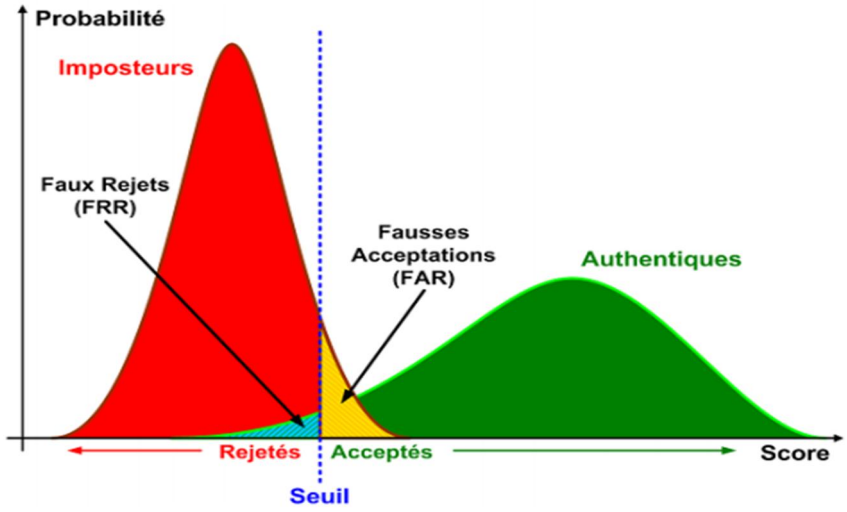


Figure2.7 *: lustration du FRR et du FAR.*

A partir de ces critères, plusieurs types de courbes de performances peuvent être dessinés :

- **La courbe ROC (Receiver Operating Characteristics) :** Cette courbe représente en ordonnée la proportion de tests positifs parmi les utilisateurs authentique (la sensibilité) en fonction de la proportion de tests positifs parmi les imposteurs (complément de la spécificité ou 1 – spécificité, en abscisse) pour toutes les valeurs des seuils de test envisageables. Pour pouvoir déterminer la validité d'un test à travers cette courbe, il est nécessaire de calculer la surface située sous la courbe ROC appelée AUC (Area Under the Curve). Plusieurs méthodes ont été proposées dans pour estimer l'AUC. Ainsi, quand le test est parfaitement discriminant, la surface sous la courbe (AUC) vaut 1 mais cela n'est jamais réalisable. En réalité, plus l'AUC est grande, plus l'algorithme est performant. La Figure 2.8 illustre un exemple de la courbe ROC [19] :

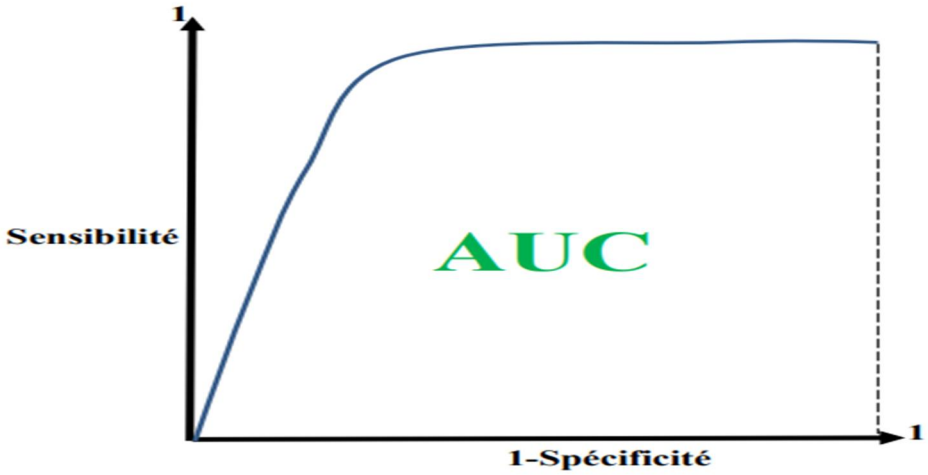


Figure 2.8 *: Exemple d'une courbe ROC.*

- **La courbe DET (Détection error tradeoff) :** Cette courbe illustre la relation entre le FRR et le FAR. Elle est obtenue en faisant varier le seuil de décision et en calculant à chaque fois les deux valeurs FRR et FAR. La Figure (2.9) illustre un exemple de la courbe DET [20].

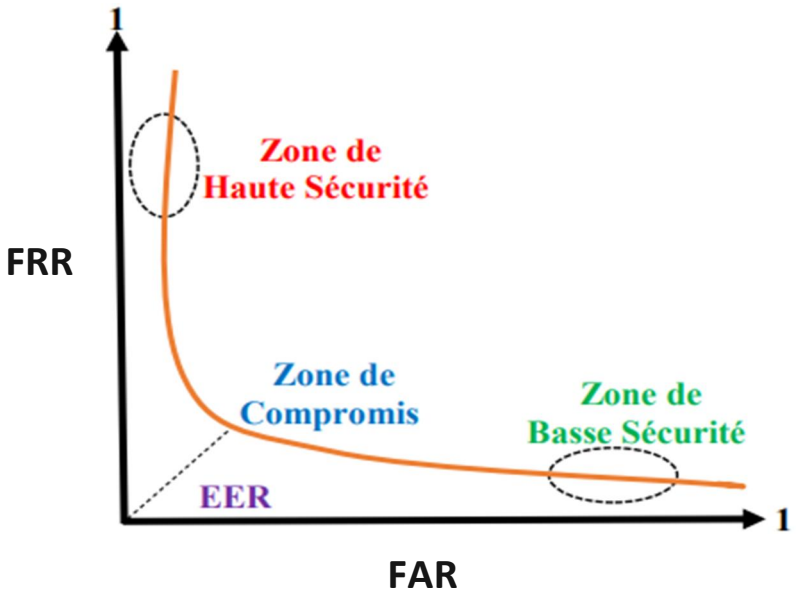


Figure 2.9 *: Exemple d'une courbe DET.*

2.5.2 Les critères d'évaluation des systèmes d'identification biométriques :

Le taux d'identification est la mesure la plus couramment utilisée, mais elle n'est pas toujours suffisante. En effet, si une erreur survient, il est utile de savoir si le bon choix est parmi les N. Ensuite, nous traçons le score d'appariement cumulatif (cumulative match score), qui

représente la probabilité du bon choix parmi les N premiers. Dans le cas il existe plusieurs modèles pour chaque individu dans la base de données (database retrieval system), vous pouvez utiliser la base de données pour récupérer ces mesures. La précision est le rapport entre le nombre de modèles correctement trouvés par le système dans la base de données et le nombre total de modèles trouvés. Le taux de rappel est le rapport entre le nombre de modèles correctement trouvés dans la base de données et le nombre total de modèles à trouver.

2.6 Les type des systèmes biométrique :

2.6.1 Systèmes biométrique uni-modal :

La biométrie monomodale est une technologie d'authentification de personnes se basant sur une seule modalité biométrique. Avant de procéder à proposer un système biométrique, il est nécessaire de choisir la modalité la plus appropriée l'application.

2.6.2 Systèmes biométrique multimodaux :

Elle peut se définir comme l'association de différentes technologies biométriques en vue d'améliorer la précision ou les résultats du système (elle est également appelée « biométrie multi niveaux »). Les systèmes biométriques utilisent au moins deux traits/modalités biométriques de la même personne lors du processus d'établissement de correspondances. Ces systèmes peuvent travailler de différentes manières, soit en collectant différentes données biométriques avec différents capteurs soit en collectant plusieurs unités des mêmes données biométriques. Certaines études englobent également dans cette catégorie les systèmes qui procèdent à plusieurs lectures des mêmes données biométriques et les systèmes qui utilisent plusieurs algorithmes pour l'extraction de traits du même échantillon biométrique. Parmi les systèmes biométriques multimodaux, on retrouve le passeport électronique au niveau de l'UE ainsi que le système d'identification biométrique US-VISIT aux États-Unis.

Le système multimodal peut correspondre à de nombreux systèmes différents :

a) **Systèmes multi algorithmes :** C'est le type de système le plus classique implicitement utilisé par de nombreuses approches. Les caractéristiques sont extraites via différents algorithmes puis fusionnées. La fusion de caractéristiques extraites via un algorithme analysant les textures et un autre la forme d'un caractère biométrique entre dans ce cadre.

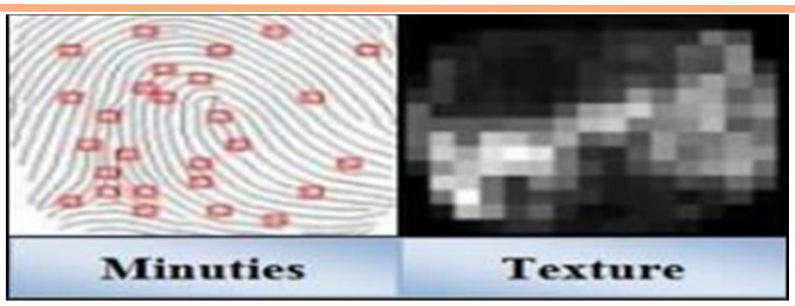


Figure 2.10 : Systèmes multi algorithmes

b) **Systèmes multi échantillons :** Un capteur unique peut capturer plusieurs instances du même caractère biométrique dans le but de rendre plus robuste l'extraction des caractéristiques ou d'enrichir le modèle biométrique d'une personne. C'est le cas, par exemple, de plusieurs captures de visage d'une personne sous différents angles. L'utilisation de vidéos entre également dans ce cadre.

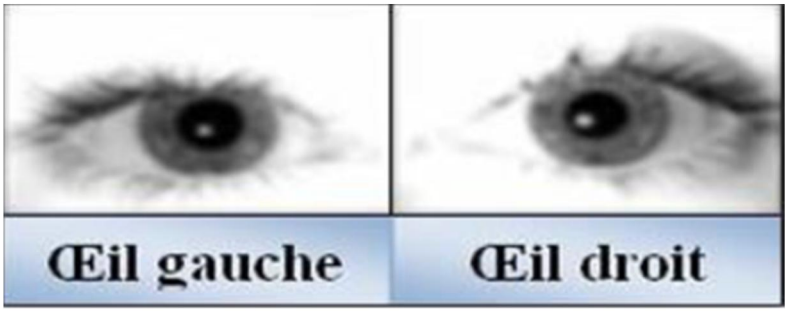


Figure 2.11 : Systèmes multi échantillons

c) **Systèmes multi capteurs :** Plusieurs capteurs permettent de capturer le même caractère biométrique sous différents angles. Ainsi la capture d'un visage à l'aide d'une caméra classique et d'une caméra infrarouge entre dans ce scénario. Ce type de système permet notamment la fusion au niveau capteur, ce que ne permettent pas d'autres systèmes comme les systèmes multi caractères.

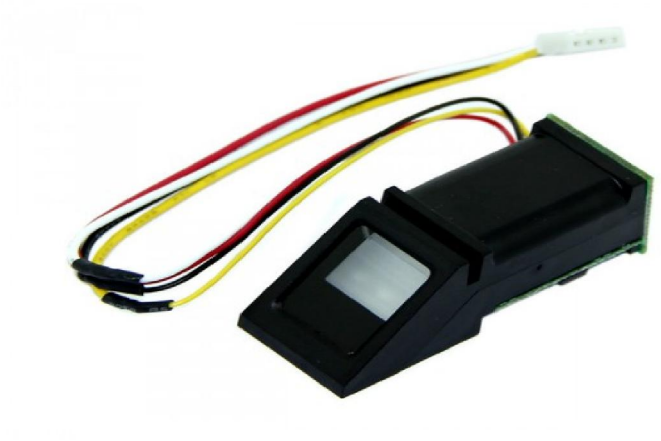


Figure 2.12 : Systèmes multi capteurs

d) **Systèmes multi instances :** Ce type de système permet de capturer plusieurs instances du même caractère biométrique. L'acquisition de plusieurs empreintes digitales via le même capteur est l'exemple typique de ce type de système. Ces systèmes n'entraînent pas de surcoût de capteurs, ni le développement de nouveaux algorithmes. À ne pas confondre avec les systèmes multi échantillons.

Figure 2.13 : Systèmes multi instances

e) **Systèmes multi caractères :** Ce type de système combine différents traits biométriques d'un individu. Les fusions visage iris, ou visage empreinte digitale font partie de ce type d'approche. Ces systèmes nécessitent différents capteurs ainsi que des algorithmes dédiés à chaque caractère biométrique. Ce type de système a comme principale caractéristique que les caractères biométriques considérés peuvent être plus décarrelés que pour les systèmes multi capteurs.

Figure 2.14 : Systèmes multi caractères

La fusion de données issues de visages capturés via une caméra en lumière visible et une autre en lumière infrarouge entre dans le cadre des systèmes multi capteurs, où il est considéré que les deux captures sont issues de modalités différentes. Même si les deux captures sont sensiblement décarrelées (la chaleur émise par un visage n'est pas visible en lumière visible), la fermeture des yeux d'un individu est visible sur les deux modalités. À noter la présence des systèmes hybrides combinant plusieurs scénarios. Une revue de nombreux systèmes biométriques multimodaux développés peut être trouvée dans [21].

2.7 Bases de données biométriques :

Afin de permettre aux chercheurs d'évaluer leurs systèmes biométriques ainsi que la comparaison entre les différents systèmes, la communauté scientifique a mis à disposition plusieurs bases de données des différentes modalités biométriques. Certaines de ces bases de données contiennent une seule modalité alors que d'autres sont multimodales.

Le tableau résume les caractéristiques de certaines bases multimodales.

Base de données	Année	Utilisateurs	Sessions	Modalités	2Fa	3Fa	Fp	Ha	Hw	Ir	Ks	Sg	Sp
BioSecure	2008	971 (DS1, scénario Internet)	2	2	X								X
		971 (DS2, scénario bureau)	2	6	X		X	X		X		X	X
		971(DS3, scénario mobile)	2	4	X		X					X	X
BiosecureID	2007	400	4	8	X		X	X	X	X	X	X	X
BioSec	2007	250	4	4	X		X			X			X
MyIDEA	2005	104	3	6	X		X	X	X			X	X
BIOMET	2003	91	3	6	X	X	X	X				X	X
MBioID	2007	120	2	6	X	X	X			X		X	X
M3	2006	32	3	3	X		X						X
FRGC	2006	741	variable	2	X	X							
MCYT	2003	330	1	2			X					X	
BANCA	2003	208	12	2	X								X
Smartkom	2002	96	variable	4			X	X				X	X
XM2VTS	1999	295	4	2	X								X
M2VTS	1998	37	5	2	X								X
BT-DAVID	1999	124	5	2	X								X

2Fa : visage 2D, 3Fa : visage 3D, Fp : empreinte, Ha : la main, Hw : manuscrite, Ir : iris, Ks : frappe au clavier, Sg : signature et Sp : voix.

Tableau 2.1 : Quelques bases de données biométriques multimodales et leurs caractéristiques

2.8 Conclusion :

Dans ce chapitre, nous avons présenté quelques structures d'un système biométrique avec Critères d'évaluation des systèmes biométriques. On a évoqué aussi les types d'un système biométrique avec leur application dans la vie réelle et enfin, on a discuté l'évaluation d'un système biométrique. Dans le chapitre suivant, on présente l'Empreinte Palmaire.

Chapitre 3

L’empreinte Palmaire

Chapitre 3 :

Liste de figure chapitre 3 :

Liste de tableau chapitre 3

3.1. Introduction

Comme il l'a présenté au chapitre 1, il existe plusieurs modalités biométriques utilisé dans le domaine de l'authentification d'identité. Parmi ces modalités on trouve que la reconnaissance des empreintes digitales de la paume (empreintes palmaires) est une technologie biométrique relativement nouvelle. Comme tous les systèmes biométriques, un système biométrique des empreintes palmaires se composent de trois étapes essentielles : prétraitement, extraction de caractéristiques et classification. Dans ce chapitre, on donne les différentes empreintes palmaires, avec contact et sans contact, Ensuite nous allons donner les types d'images, L'état de l'art sur empreinte palmaire multi spectrale, et enfin une conclusion.

3.2. Les avantages de l'empreinte palmaire :

Les empreintes palmaires représentent un modèle de la paume d'une personne et illustrent les caractéristiques physiques de son motif de peau, telles que les lignes (principales et rides), les points, les détails et les textures. En d'autres termes, du poignet à la base des doigts, lorsque la main est fermée, l'intérieur de la main n'est pas visible, comme le montre la figure ci-dessous

Figure 3.1 : paume de la main

Le tableau ci-dessous nous montre une comparaison entre les différentes modalités biométriques

biométrie	Universalité	Unicité	Permanence	Mesurabilité	Performance	Acceptabilité	Circonvention
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	Haute	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	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

Tableau 3.1 : Comparaison entre les techniques biométriques

L'empreinte palmaire présente plusieurs avantages par rapport aux autres données biométriques, notamment :

a) L'image de palmaire est d'une basse résolution (traitement plus rapide).

b) Généralement elle ne nécessite pas un grand coût de calcul.

c) Elle atteint une exactitude élevée.

d) Peu de risques d'intrusion.

e) Bonne acceptation des usagés.

f) Très simple à utiliser.

g) Le résultat est indépendant de l'humidité et de l'état de propreté des doigts

h) Fichier "gabarit" de petite taille.

D'autre part l'empreinte palmaire à peu d'inconvénients comme :

a) Problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système.

b) Il suffit de se couper pour présenter une anomalie dans le dessin de ses empreintes.

c) Trop encombrant pour un usage sur le bureau, dans une voiture ou un téléphone

d) Le risque de fausse acceptation de jumeaux ou de membres d'une même famille.

3.3 Les différents types de captures d'empreintes palmaires

L'acquisition de données est la première étape de tout système biométrique" et les empreintes palmaires ne font pas exception. Dans ce chapitre, nous abordons tout d'abord deux méthodes d'acquisition des données d'empreintes palmaires : hors ligne et en ligne. Avant que le dispositif d'acquisition d'empreintes palmaires en ligne ne soit développé, toutes les empreintes palmaires sont obtenues hors ligne. Les empreintes palmaires hors ligne sont obtenues en pressant une paume encrée sur du papier" et en utilisant ensuite un scanner pour numériser le signal. L'acquisition en ligne des empreintes palmaires est le moyen le plus direct de numériser les données des empreintes palmaires.

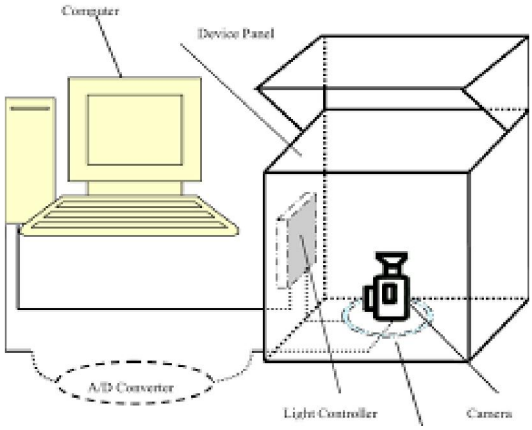


Figure 3.2: Capture d'empreinte palmaire Hors ligne

Figure 3.3 : Capture d'empreinte palmaire En ligne

3.3.1 Système de reconnaissance en ligne

Le premier dispositif de capture d'empreinte palmaire en ligne au monde est conçu en décembre 1999" à l'Université polytechnique de Hong Kong [21]. C'était la première tentative de créer un dispositif en ligne pour la recherche sur les empreintes palmaires. Le dispositif a été fabriqué à l'aide d'une boîte en plastique, d'une source de lumière, d'un miroir, d'une plaque de verre et d'une caméra CCD, comme le montre la figure 3.4. Des essais répétés ont montré que l'image formée par le miroir n'était pas aussi bonne qu'une réflexion directe car le second miroir à la surface crée une image fantôme. La plaque de verre utilisée pour tenir la paume a déformé la surface de la peau de la paume de sorte que les lignes de la paume n'étaient pas assez bonnes pour l'extraction des caractéristiques. Un meilleur dispositif était nécessaire pour obtenir une meilleure qualité d'image pour le traitement ultérieur

Dans ce type de systèmes, les images de modalités sont capturées par un appareil de capture spécifique et ces images numériques acquises sont traitées en temps réel [22].

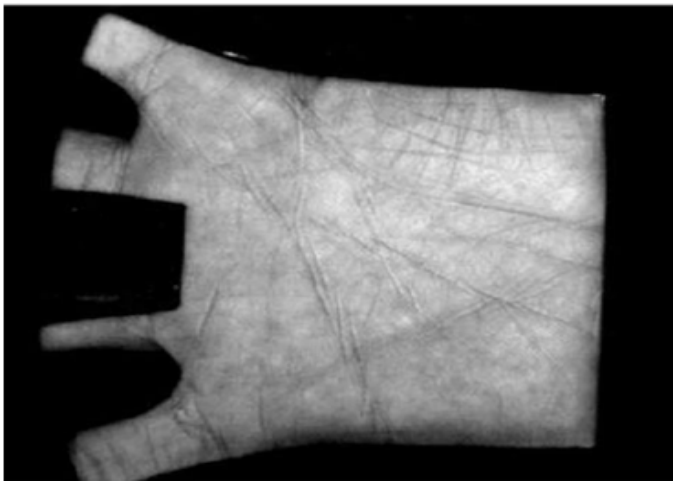


Figure 3.4 : capture d'empreinte palmaire en ligne

3.3.2 Système de reconnaissance Hors Ligne :

Les recherches sur l'empreinte palmaire ont commencé en 1996 en utilisant des "images encrées", comme le montre là [figure 3,1]. La méthode hors ligne consiste à collecter des échantillons en encrant la paume de l'utilisateur et en la pressant sur une feuille de papier blanc. Après que l'encre a séché, l'image de la paume sur le papier est numérisée par un scanner et stockée dans l'ordinateur personnel. Il est clair que cette méthode n'est pas adaptée à une application en temps réel, comme le contrôle d'accès physique. Outre le nombre d'étapes nécessaires, la qualité de l'image de l'empreinte palmaire n'est pas satisfaisante car

elle peut être affectée par la quantité d'encre utilisée. Trop d'encre et pas assez d'encre produisent des empreintes de palme insatisfaisantes.

Ce type de système traite les images de chaque modalité précédemment capturée par un scanner numérique. Ces méthodes fournissent des images à haute résolution, mais ne conviennent pas aux systèmes de sécurité en temps réel.

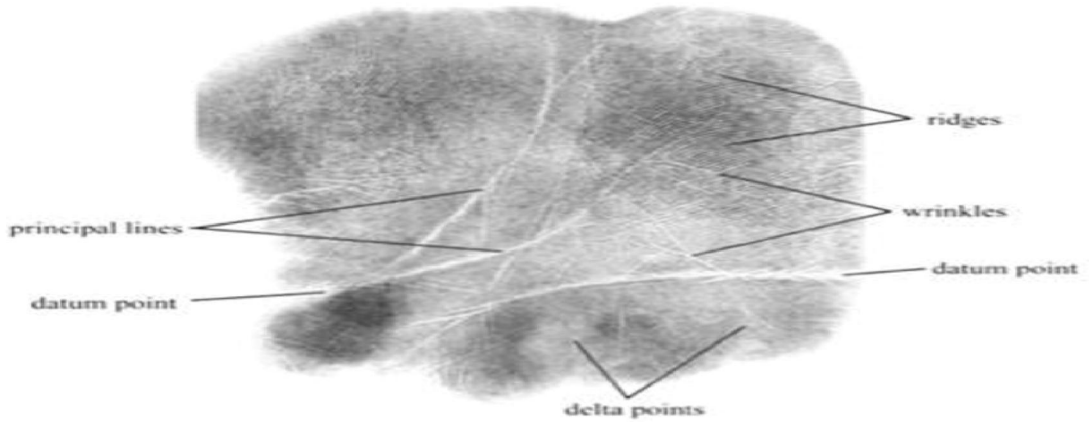


Figure 3.5 : empreinte de paume encrée

3.3.3 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 le montre la figure (3.6), qui est indiquée pour les applications médico-légales et légitimes. Il existe deux méthodes principales pour reconnaissance des empreintes palmaires à haute résolution : es méthodes basées sur les détails et les méthodes basées sur la fusion régionale.

La reconnaissance d'images d'empreintes palmaires haute résolution prend beaucoup de temps en raison de la grande capacité d'image et du prétraitement complexe.

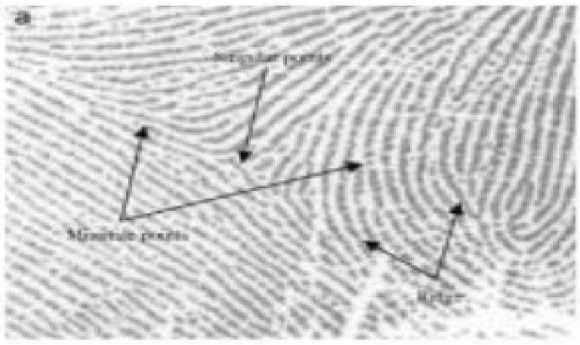


Figure 3.6 : image empreinte palmaire haute résolution

3.3.4 La reconnaissance d'empreintes palmaires à basse résolution :

La reconnaissance d'empreintes palmaires à basse résolution présente beaucoup d'avantages Ce qui l'a fait utiliser dans de nombreux domaines civiles et commerciales. Par exemple, l'utilisation des appareils photo ordinaires pour capturer facilement les images des empreintes palmaires à basse résolution.

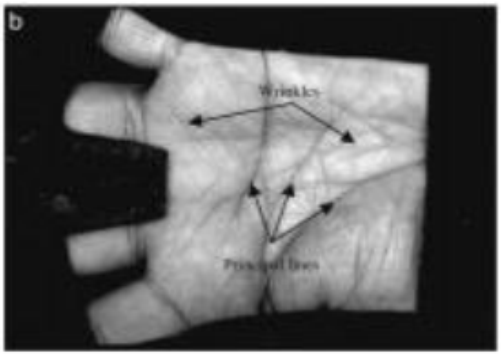


Figure 3.7 : image empreinte palmaire basse résolution

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

La reconnaissance 3D de l'empreinte palmaire a également subit à un progrès essentiel. Les travaux existants montrent que les informations 3D sur la carte palmaire peuvent être transformées en image 2D basé sur la texture pour la reconnaissance. Par conséquent, la méthode de reconnaissance traditionnelle des empreintes digitales 2D ont été adopté pour être utilisées avec succès pour identifier les empreintes 3D.

L'empreinte palmaire 3D utilise les informations structurelles 3D de la surface de la paume en particulier, la technologie d'imagerie par lumière structurée est utilisée pour obtenir des données 3D à partir des impressions de paume. L'empreinte palmaire 3D n'est pas comme

L'empreinte de paume 2D, elle n'est pas facile à falsifier. Plus les informations de profondeur 3D ne seront pas perdues pendant le traitement. De plus, l'éclairement de l'image 2D de l'empreinte de la paume varie considérablement qui cause des problèmes de reconnaissance de l'empreintes 2D. Par conséquent, il y a donc un intéressé par l'exploration d'une nouvelle technologie de reconnaissance de l'empreinte de la main pour surmontez les difficultés. Intuitivement, la reconnaissance de l'empreinte 3D est Bonne solution.

De plus, la projection du laser sur la surface de la paume à l'acceptation de l'utilisateur est supérieure à celle du visage.

3.3.6 La reconnaissance d'empreintes palmaires multi spectrale :

Quant aux méthodes multi spectrales, elles utilisent des caractéristiques extraites sous des longueurs d'onde spectrales distinctes pour la reconnaissance pour le but d'améliorer la Précision et capacité anti-déception. [Guo et al] ont analysé les données d'empreintes palmaires hyper-spectrales pour déterminer le nombre optimal de bandes spectrales et avoir Déterminer la bande de fréquences la plus caractéristique pour établir son système d'identification.

3.4 Structure des systèmes de reconnaissance d'empreintes palmaires :

La reconnaissance biométrique est constituée des procédures utilisées par les systèmes biométriques pour comparer les caractéristiques biométriques des individus, calculer leur similarité et déterminer qu'ils appartiennent ou non à la même personne. Le processus de reconnaissance peut être divisé en cinq modules :

3.4.1 Acquisition :

Il est basé sur les caractéristiques biométriques utilisés, un capteur spécifique est utilisé pour capturer ces caractéristiques appartenant à l'utilisateur. Les caractéristiques capturées peuvent être une image, un son ou une séquence d'images. Les caractéristiques capturées par le capteur sont appelées "échantillons".

3.4.2 Segmentation :

La région de l'échantillon contenant les informations biométriques est isolée. Par exemple, dans le cas d'une image provenant d'une acquisition de l'iris, le les cils et les paupières sont éliminés, de sorte que seule la région de l'iris est prise en compte

3.4.3 Extraction :

Les caractéristiques distinctives sont extraites de l'échantillon segmenté, et une représentation abstraite de la caractéristique biométrique est calculée. Ce modèle est mieux adapté au stockage dans une base de données et à l'analyse par un système de traitement automatisé de l'information. Les modèles peuvent être des chaînes de bits, des coordonnées de points particuliers dans l'image, des images, des signaux ou des fonctions algébriques.

3.4.4 Correspondance (comparaison) d'identité :

Le modèle est comparé avec un ou plusieurs modèles présents dans la base de données. La base de données peut être centralisée ou stockée sur un appareil possédé par l'utilisateur. Le résultat de l'étape de vérification de l'identité est un "score de correspondance", qui est une mesure de la similarité entre les deux modèles comparés.

3.4.5 Décision :

Le score de correspondance est utilisé pour produire la décision finale du système. Dans la plupart des cas, un seuil pour la valeur du score de correspondance est utilisé pour transformer le résultat de la comparaison en une décision booléenne, qui détermine si le les modèles appartiennent à la même personne ou pas, c.-à-d. accepté ou refusé.

3.5 État de l'art des méthodes d'extraction automatique de paramètre caractéristique :

Généralement, la méthode de reconnaissance de l'empreinte palmaire peut être à peu près divisé en deux catégories, méthodes globales (ou statistiques) et méthodes locales (ou géométriques).

Les méthodes globales de reconnaissance d'empreinte palmaire peuvent être divisées en quatre catégories :

- Les méthodes sous-espaces
- Les méthodes structurelles
- Les méthodes de codage de texture
- Statistique des caractéristiques.

3.5.1 Les méthodes sous-espace :

La méthode du sous-espace couramment utilisée considère les images de l'empreinte palmaire comme des matrices ou des vecteurs de grande taille, puis les convertit en images de petite taille par projection ou transformation mathématique. En général, différents ensembles d'apprentissage de différents types d'empreintes de paume doivent être établis, et la meilleure matrice ou vecteur de projection a été sélectionné pour représenter l'image d'empreinte de paume en tant que vecteur de caractéristiques. Lors de la création de l'ensemble d'apprentissage, des informations figurent sur l'étiquette de chaque catégorie. Les méthodes traditionnelles (telles que l'ACP et l'analyse des composants indépendants (ICA)) n'utilisent pas ces informations, tandis que l'analyse discriminante linéaire (LDA) utilise ces

informations. Par la suite, les chercheurs ont combiné l'ACP et l'ADL pour examiner à la fois la discrimination et la représentation de l'empreinte palmaire.

3.5.2 Les méthodes structurelles

Les méthodes basées sur la structure sont des techniques de reconnaissance traditionnelles, qui ont été adaptées à partir de la reconnaissance des empreintes digitales. La clé principale de ces méthodes est l'utilisation d'un algorithme de détection des contours pour extraire l'information sur l'orientation et l'emplacement :

- Des crêtes
- Des lignes
- Des points caractéristiques

Concernant la méthode d'extraction centrée sur les crêtes, Huang et al. [86] ont proposé une nouvelle méthode d'extraction des caractéristiques des crêtes basée sur leur orientation et leur fréquence. Ils utilisent une banque de filtres de Gabor pour capturer les détails locaux et globaux afin de représenter les crêtes comme différents ensembles de points.

Cependant, ils ont de nombreux inconvénients. Par exemple, elles remplacent les lignes réelles de la paume de la main par les lignes ou les points extraits, ce qui entraîne une perte d'information considérable. Ainsi, au cours de la dernière décennie, moins de chercheurs s'y sont intéressés.

3.5.3 Codage de texture :

Le codage permet de transformer les images en informations codées. Il est facile et rapide à traiter dans les processeurs. La forme de la dérivation de la matrice peut réduire la complexité de l'espace en même temps. Le codage générique signifie qu'une image d'empreinte palmaire est d'abord filtrée à l'aide d'un filtre prédéfini, puis codée selon un certain principe. Ensuite, le degré de similarité peut être obtenu en utilisant une opération arithmétique binaire.

Depuis l'émergence de l'Iris Code, les techniques de codage se sont développées rapidement. Le *code Palm*, *le code compétitif*, *le code de fusion* et le *code ordinal* ont été proposés. *Code Ordinal* ont été proposés successivement. Au cours de la dernière décennie, une plus grande attention a été accordée à l'information d'orientation d'une empreinte palmaire plutôt qu'au contenu de la phase. En outre, de plus en plus de chercheurs s'intéressent à la robustesse et à la modification de la conception des filtres, schéma de codage et l'algorithme de classification

3.5.4 Méthodes statistiques :

Utilise la fonction de texture de l'image de la paume en représentant la ligne de la paume comme un champ directionnel dans la géométrie. Ensuite, une transformée complexe en ondelettes à double arbre est utilisée pour améliorer la structure locale de l'image, et l'histogramme LBP est extrait et utilisé comme caractéristique distinctive. Il est proposé de combiner des caractéristiques géométriques avec des caractéristiques de texture. En particulier, les moments Zernike sont utilisés comme descripteur de la texture de l'empreinte de la paume. Une méthode d'intelligence artificielle (IA) combinant un graphe adaptatif autonome (soms) et un réseau neuronal à rétroaction (BPNN) est utilisée pour classer les caractéristiques.

3.6. Conclusion

La reconnaissance de l'empreinte palmaire est une méthode promise pour l'authentification de l'identité avec la plus grande sécurité et stabilité. Dans ce chapitre, on a présenté les l'état de l'art en matière d’extraction des empreintes palmaires.

Chapitre 4

Descripteur de Motif à Double Croisements

Sommaire

.

Liste de figure :

List de tableau :

4.1 Introduction :

La classification des textures est l'un des sujets de recherche actifs en raison de défis scientifiques et d'une utilisation potentielle dans une large gamme d'applications pratiques telles que l'analyse d'images médicales, télédétection, inspection de tissu, segmentation, recherche d'images basée sur le contenu [22] et reconnaissance biométrique basée sur l'iris [23]. Dans le passé, des performances satisfaisantes ont été obtenu par diverses techniques uniquement dans un environnement contrôlé. Cependant, la classification d'une image de texture sans contrainte est un problème crucial en raison de la grande variation des points de vue, des changements d'éclairage et de la qualité dégradée de l'image de texture. Par conséquent, la conception d'un descripteur efficace est un problème fondamental dans la classification des images de texture. Fondamentalement, la représentation de texture peut être classée en fonction des approches employées

4.2 L'architecture du système proposé :

Pour pouvoir reconnaitre une personne après avoir capturé son empreinte palmaire il faut passer par quatre étapes essentielles :

- Capture d'images d'empreintes palmaires,
- Extraction du ROI,
- Extraction des histogrammes BSIF vectoriel,
- Appariement des caractéristiques.

4.2.1 Détection de la main :

La détection de contour est une clé majeure dans le domaine de la reconnaissance d'objets. En fait, un contour représente, en gros, une frontière entre des zones adjacentes dans une image, ayant une luminosité distinctive (ou des textures ou des couleurs). En effet, les techniques de détection de bord, Analysent l'image globale sans tenir compte des caractéristiques de ses différentes régions. Ainsi, les contours de la même image peuvent être bien détectés dans certaines zones et mal détectées dans d'autres. Pour surmonter ce problème, il est nécessaire d'étudier certaines approches de détection de contour et d'analyser leurs performances.

En ce qui concerne la détection d'objets de la main, plusieurs méthodes ont été proposées dans la littérature et classés en méthodes basées sur la couleur de la peau et méthodes basées sur la forme.

Cependant, la couleur de la peau peut être exposée à certaines variations en raison de l'éclairage et les changements de fond lors de l'acquisition. Par conséquent, nous nous concentrons sur la détection des mains approches fondées sur la forme, à savoir méthodes actives basées sur les contours, forme active méthodes basées sur un modèle et méthode basée sur le contexte de forme.

4.3 Principe du motif à double croisement (DCP) :

Le modèle DCP (Dual Cross pattern), que nous présentons dans ce mémoire, est une méthode basée sur des descripteurs, qui traite du même concept de LBP dans la mise en forme d'un motif et dans l'encodage de l'image pixels. Cependant, alors que ce dernier utilise une méthode d'encodage basée sur le pixel le plus proche du voisinage, l'approche DCP utilise plus d'un niveau de voisinage. Il compare à la fois le pixel central à ses voisins les plus proches et aux pixels voisins entre eux, pour calculer le code pixel central. Donc, comme le montre la Figure (4.1), échantillonner les points DCP à partir des positions et selon plusieurs orientations informatives, sur les deux les cercles concentriques, qui définissent le motif considéré, aident l'opérateur pour capturer toutes les variations d'intensité potentielles du pixel, car, comme on le sait, les défauts de l'empreinte palmaire survenus peuvent être, non seulement de tailles différentes, mais de directions aléatoires aussi.

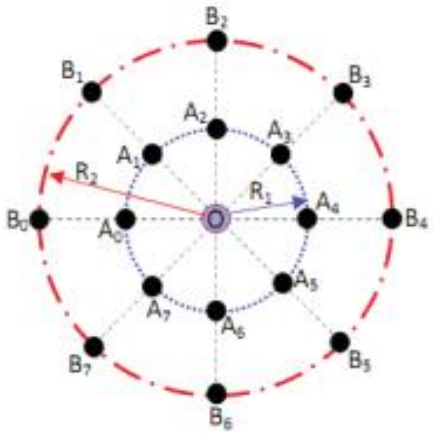


Figure 4.1 : Pixel central et points d'échantillonnage spatial

4.4 Le descripteur DCP :

Les points A_i référencés $\{A_0, \ldots A_7\}$ sont situés à angles égaux sur le cercle intérieur (R_1), alors que le $B_i = \{B_0, \ldots B_7\}$ sont positionnés de la même manière, mais sur le cercle externe (R_2). En gros, pour obtenir un nouveau code d'un point donné avec le DCP méthode, les informations texturales dans chacun des huit échantillons directions de la figure 4.1, est quantifiée par l'équation 1, pour attribuer un nombre décimal DCP_i correspondant à la ième direction.

$$DCPi = S(IAi - I_o).2 + S(I_{Bi} - I_{Ai}),\ 0 \leq i \leq 7 \qquad \textbf{(1)}$$

Avec S(x), la fonction signe donner par :

$$S(x) = \begin{cases} 1, & si \quad x \geq 0 \\ 0, & autre \end{cases} \qquad \textbf{(2)}$$

Et où Io, I_{Ai} et I_{Bi} représentent respectivement le pixel intensités des points O, A_i et B_i. Puisque la statistique du second ordre de l'équation 1, implique un grand nombre de 4^8 valeurs DCP pour encoder toutes les informations texturales possibles dans les huit directions, la méthode de calcul consiste à créer les codes pixels à partir de deux sous-ensembles, constitué par les deux groupes à quatre points {Ai} et {Bi}, à la place de traiter l'ensemble complet des points échantillonnés ; c'est-à-dire : toutes les orientations.

Les quatre points de chaque sous-ensemble créé sont choisis clairsemés et uniformément répartis sur les cercles, mais avec un décalage de $\pi/4$ pour les positions des points du deuxième sous-ensemble. Celles-ci deux groupes sont :

DCP_0 = $\{DCP_0, DCP_2, DCP_4, DCP_6\}$ pour le premier, et DCP_π/4 = $\{DCP_1, DCP_3, DCP_5, DCP_7\}$ pour le deuxième, avec le x, dans DCP_x, se rapporte à une position de point. Le nombre total de motifs locaux (local pattern) obtenus à partir d'une telle méthode de regroupement est, alors, $2x4^4 = 512$. Ci-dessous, l'illustration de la méthode de regroupement dans l'application DCP.

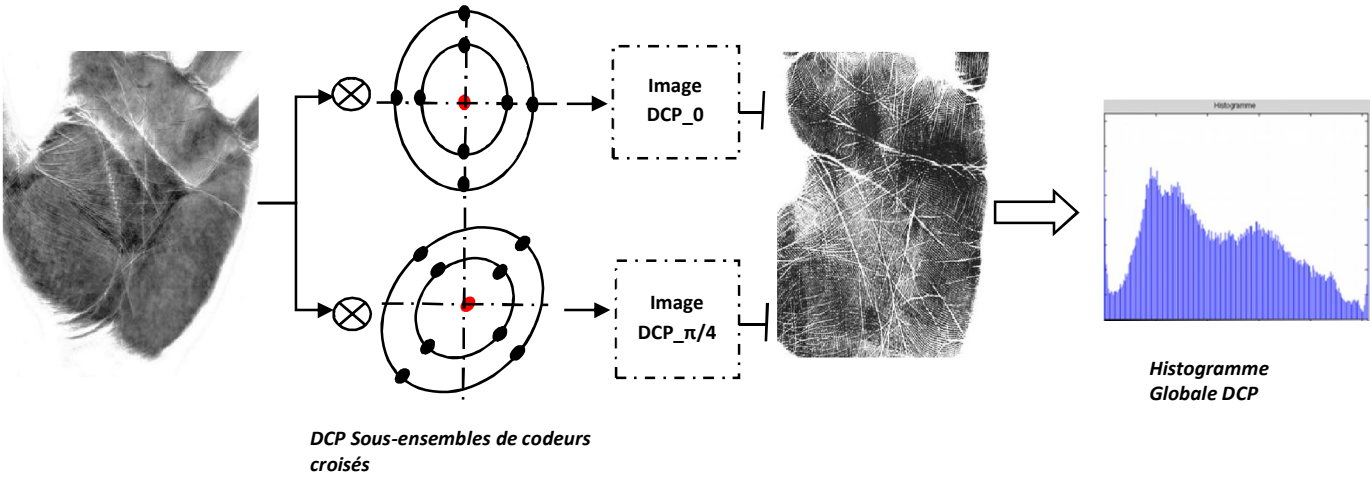


Figure 4.2 : Le descripteur de motif à double croisements (DCP)

Les deux codes pixels obtenus par le DCP_0 et le DCP_π / 4, les codeurs croisés sont formulés comme suit

$$\begin{cases} DCP\_0 = \sum_{i=0}^{3} DCP_{(2i)}.4^i \\ DCP\_\pi/4 = \sum_{i=0}^{3} DCP_{(2i+1)}.4^i \end{cases} \quad (3)$$

Le descripteur DCP final de chaque image considérée est obtenu par la concaténation des histogrammes calculés à partir des images de sortie DCP_0 et DCP_π / 4.

4.5 Système proposé :

Une nouvelle représentation supervisée est proposée dans cette section, pour surmonter les défis rencontrés lorsque des empreintes de paume sans contact sont utilisées pour l'identification humaine. Il explore les modèles de texture spatialement invariants entre différentes échelles. Ainsi, cet article présente une nouvelle tentative d'intégrer le codeur Cross Pattern avec la méthode de fractionnement spatial sans chevauchement. Un résumé de la représentation proposée est présenté à la Figure 4.3.

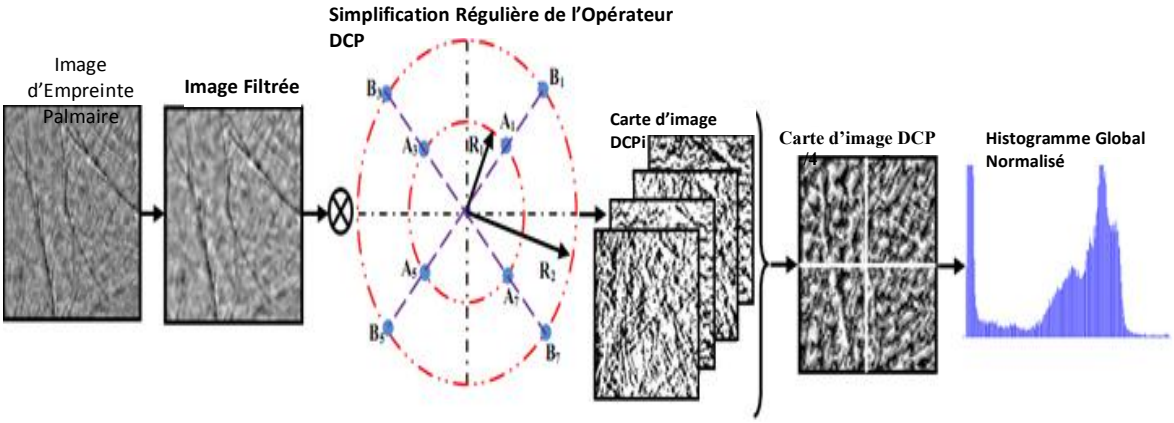


Figure 4.3 : Représentation de l'empreinte palmaire Patch Cross Pattern (PCP).

Le tableau (4.1) montre un exemple de mappage d'images et de valeurs d'entropie utilisant $[R_{in}\ R_{ex}] = [1\ 2]$ pour les encodeurs CP_0 pair et $CP_{\pi/4}$ impair, où CP_0 capture les motifs de texture dans les directions horizontale et verticale tandis que $CP_{\pi/4}$ capture la texture modèles dans le sens diagonal.

Pour évaluer notre système, il existe deux critères pour choisir entre les codeurs CP_0 et $CP_{\pi/4}$: (i) des critères subjectifs (visuels) et (ii) des critères objectifs (entropie). Selon les premiers critères, les résultats montrent que les images cartographiques de $CP_{\pi/4}$ contiennent plus de primitives visibles (lignes principales, rides, etc.) de l'empreinte de la paume que celles de CP_0 (voir tableau 4.1)

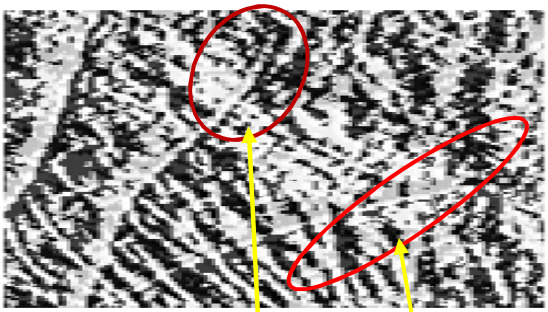
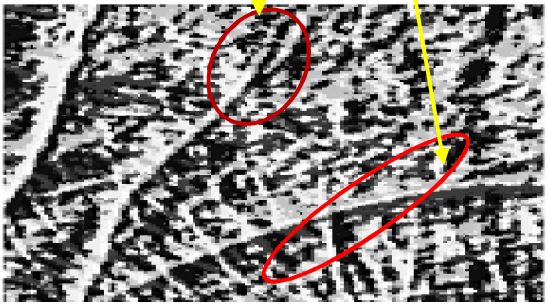
	Delhi
ROI image	
CP_0 image map	
$CP_{\pi/4}$ image map	
Entropies (CP_0)	0.0310
Entropies ($CP_{\pi/4}$)	**0.2008**

Tableau 4.1: Valeurs d'entropie des images empreinte palmaire encodées

Pour être plus objectif, un second critère, basé sur l'entropie de l'image, est utilisé. Conçu pour deux types d'images d'empreinte palmaire, il affiche des valeurs plus élevées lors de l'utilisation de l'encodeur $CP_{\pi/4}$. Cela confirme que cet encodeur permet d'obtenir des images cartographiques avec plus d'informations. Par conséquent, seul le sous-ensemble impair défini par les codeurs croisés $CP_{\pi/4}$ est utilisé dans ce travail pour évaluer l'approche proposée.

4.6 Résultats expérimentaux et discussions :

La performance de la méthode proposée est démontrée en conduisant plusieurs expériences sur des bases de données de l'empreinte palmaire sans contact. Ces performances dépendent de trois paramètres qui sont : le niveau de décomposition L, le rayon R_{in} et R_{ex} du codeur $CP_{\pi/4}$. Ensuite, pour connaître les rayons optimaux [R_{in}, R_{ex}], pour les bases de données IIT Delhi, les taux d'erreur sont calculés avec une paire de rayons changeante comme sur les figures 4 et 6 pour un niveau L variant de 1 à 6. En utilisant le résultat obtenu valeurs optimales, la méthode proposée est comparée, dans les dernières expériences, à celles existantes par son application aux deux bases de données mentionnées.

Les informations de la base de données, la configuration expérimentale et les résultats sont présentés dans les sous-sections ci-dessous. Il est à noter que dans tous les tableaux, les taux d'identification (IR) les plus élevés apparaissent en caractères gras. [24]

4.7. Base de données IIT Delhi :

Dans la base de données de l'empreintes palmaires sans contact de l'IIT Delhi, des images ont été collectées à partir de 230 sujets à l'aide des deux mains (soit 460 paumes distinctes). Chaque personne a au moins cinq images de paume pour chaque main. Ces images sont acquises dans des variations sévères de distorsion, de rotation et de translation. La région d'intérêt (ROI) des images de paume est disponible publiquement. Par conséquent, il y a 460 classes de palmiers dans la base de données IIT Delhi, chacune avec environ cinq images d'empreinte palmaire.

La figure (4.4) montre quelques exemples d'images d'une empreinte palmaire de la base de données IIT-Delhi de deux sujets différents. Les trois images de la première rangée (Figure. a) ont été capturées à partir du premier sujet, tandis que les images de la deuxième rangée (Figure. b) ont été capturées à partir du deuxième sujet.

Au cours de toutes les expériences, les trois premiers échantillons sont sélectionnés comme ensemble d'apprentissage et les échantillons restants comme ensemble de test. Ainsi, nous avons 1380 (460x3) échantillons d'apprentissage et 920 (460x2) échantillons de test.

Figure. a

Figure. b

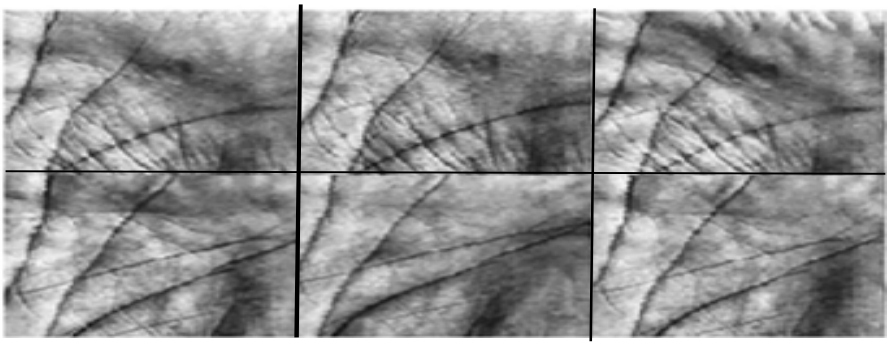


Figure 4.4: Quelques images d'une empreinte palmaire de la base de données IIT-Delhi.

4.7.1 Expérience 1 :

Dans cette partie, nous examinons les paramètres les plus appropriés de la méthode proposée. Nous étudions l'effet du niveau de décomposition L sans chevauchement, du rayon intérieur R_{in} et du rayon extérieur R_{ex}. Tous ces paramètres ont une influence sur la performance de la méthode proposée. Afin de trouver les valeurs optimales de ces paramètres pour les représentations PCP et R-PCP, nous avons mené des expériences en utilisant différentes valeurs de [R_{in} R_{ex}] pour L variant de 1 à 6.

Comme le montre la Fig. 4.a, la représentation PCP permet une bonne performance (EIR = 1,74%) pour une paire de rayons [R_{in} R_{ex}] égale à [2 5] ou [4 6] et un paramètre L de 5. De plus, avec une valeur fixe de R_{in}, l'EIR semble changer inversement au rayon R_{ex}. Il diminue lorsque cette valeur de rayon augmente. Pourtant, les deux paramètres augmentent pour un R_{in} passant à une valeur plus élevée. Quant à l'opération de décomposition sans chevauchement, elle fait diminuer l'EIR lorsque son niveau (L) augmente. Des valeurs d'EIR plus élevées sont ainsi obtenues sans décomposition, et le taux d'erreur le plus élevé de 35,65% est atteint avec une paire de rayons de [R_{in} R_{ex}] = [1 2] et un niveau de décomposition L = 1.

D'autre part, montre les performances obtenues en utilisant la représentation R-PCP. Les performances du système deviennent plus efficaces (EIR = 0,22%) par rapport à la représentation PCP. Cela est dû à l'utilisation de la méthode WLDA, qui rend les fonctionnalités plus discriminantes en maximisant entre les classes et en minimisant les variations intra-classes. De plus, cette amélioration est obtenue avec deux niveaux de décomposition au lieu de cinq niveaux dans le cas de la représentation PCP.

4.7.2 Expérience 2 :

Pour mieux démontrer l'efficacité de l'approche proposée, elle a été comparée à certains travaux antérieurs. Comme mentionné dans le tableau 2, il atteint un taux d'identification le plus élevé, prouvant que la méthode de représentation R-PCP est beaucoup plus efficace que celles comparées.

Méthodes	Nbre Classes	Protocol		Descripteurs	IR(%)
		Train Test			
[21]	460	03 premières images	Échantillons restants	RPBSIFD	99.57
[22]	460			DGLSPH	99.57
[23]	460	Trois images Sélectionné aléatoirement		Motif de texture + forme des lignes principales	97.98
				Fractal (FDBC)	95.80
Proposé	460	03 premières images		PCP	98.48
				R-PCP	**99.78**

Tableau 4.2 : Résultats comparatifs montrant le taux de reconnaissance des schémas proposés et des méthodes récemment proposées sur la base de données IIT Delhi.

4.8 Conclusion :

En raison de la dégradation de la qualité de l'image de paume et des grandes variations de l'éclairage, de la pose et de l'expression, la reconnaissance d'images de paume sans contrainte est une tâche difficile. La résolution de ce problème exige un travail avec un descripteur d'image de paume efficace et un schéma de représentation de la paume complet. Pour atteindre cet objectif, nous apportons la contribution d'un descripteur d'image de paume nommé Dual-Cross Patterns. DCP encode les statistiques de second ordre dans les directions les plus informatives avec une image de paume.

Les tests de ces systèmes sont effectués sur les bases IIT Delhi d'empreinte palmaire, les résultats obtenus sont encourageants

Conclusion Générale :

La biométrie est la mesure d'éléments biologiques, comportementaux ou physiologiques, uniques et propres à chaque individu. Chaque année, plus de 210.000 personnes sont victimes d'une usurpation d'identité ce qui a conduit à faire de nombreuses études afin de trouver les voies et moyens d'assurer une meilleure protection des biens et des êtres.

Cette étude nous a permis de valider la faisabilité d'un système biométrique par l'identification des personnes dans l'utilisation de ses caractéristiques physiques ou comportementales ou biologies. Parmi les modalités les plus utilisées dans la reconnaissance de système biométrique est l'empreinte palmaire.

Nous pouvons noter que le descripteur à base de motif à double croisement (DCP, Dual Cross Pattern) aide à mieux différencier et identifier les personnes. Des efforts supplémentaires ont été déployés pour améliorer les taux de reconnaissance, comme la recherche des paramètres optimaux du descripteur DCP, en ce qui concerne le rayon du pixel voisin.
Le système proposé est appliquée à la base de données IIT DELHI. Les résultats obtenus montrent que la stratégie proposée donne des performances très encourageantes avec un taux de reconnaissance assez élevé.

Bibliographique :

[1]-H.Fraga, M.Fedias, mémoire master "Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages", Université Mohamed Khi der – Biskra. 2019

[2]-DANG Hoang Vu., "Biométrie pour l'identification", Rapport final, Institut de la Francophonie pour l'Informatique, Hanoï, Vietnam, 07 – 2005.

[3]-C. Fredouille, J. Mariethoz, C. Jaboulet, J. Hennebert, J.-F. Bonastre, C. Mokbel, F. Bimbot, « Comportement d'une méthode d'adaptation bayésienne pour Inscription incrémentielle à la vérification des locuteurs », Conférence internationale sur l'acoustique, la parole et le traitement du signal, p. 1197-1200, Istanbul, Turquie, 5-9 Juin 2000.

[4] L. Heck, N. Mirghafori, « Adaptation non supervisée en ligne de la vérification du locuteur », Conférence internationale sur le traitement du langage parlé, Vol. 2, p. 454-457, Peking, Chine, 16-20 October 2000.

[5] A. K. Jain, A. Ross, Introduction à la biométrie, dans le manuel de la biométrie, Springer, 2008.

[6] J. Bhatnagar et A. Kumar. Sur l'estimation des indices de performance pour la biométrie identification. La reconnaissance de formes, Vol. 42, pp.1803-1815, 2009.

[7] Salah Zoubida, Bedad Fatima, , «Méthode d'extraction des caractéristiques des images biométriques», Universite Abdelhamid Ibn Badis – Mostagane. 2017

[8] P. Phillips, H. Hyeonjoon, S. Rizvi, P. Rauss, «La méthodologie d'évaluation FERET pour les algorithmes de reconnaissance faciale», IEEE Transactions sur l'analyse de modèles et l'intelligence artificielle, Vol. 22, n ° 10, octobre 2000.

[9] S. Prabhakar, A. Jain, « Fusion au niveau de la décision dans la vérification biométrique », La reconnaissance de formes, Vol. 35, n ° 4, p. 861-874, 2002.

[10] INSPASS, http://www.ins.usdoj.gov/graphics/howdoi/inspass.htm.

[11] J. Bellegarda, D. Naik, M. Neeracher, K. Silverman, « Vérification vocale indépendante de la langue, inscription courte sur un microphone à champ lointain», ICASSP, Vo l. 1, p. 445-448, Salt Lake City, Utah, 7-11 mai 2001. 1.5.5.2.

[12] La biométrie prend vie », Banking Journal, janvier 1997 http://www.banking.com/aba/cover_0197.htm.

[13] Nuance, http://www.nuance.com

[14] T-NETIX Inc., http://www.t-netix.com.

[15] revues.univ-biskra.dz/index.php/cds/article/vue/455/422

[16] M. Theofanos, B. Stanton et C. A. Wolfson. Utilisabilité et biométrie : assurer

Systèmes biométriques réussis. Institut national des normes et de la technologie (NIST),

2008. [citer p. 23]

[17] ISO / CEI FCD 19792. Technologies de l'information - techniques de sécurité - sécurité

Évaluation de la biométrie, 2008. [cite p. 20, 21, 23, 58, 104, 109]

[18] ISO / CEI 19795-1. Technologies de l'information - tests et Rapports de performances biométriques - partie 1 : Principes et cadre, 2006. [Cite p. 3, 14, 20, 21, 22, 23, 26, 27, 33, 154]

[19]. Svoboda J., Masci J. et Bronstein M. M.: "Reconnaissance de l'empreinte palmaire via un apprentissage d'index discriminatif", dans Proc. 2016 23e Int. Conf. sur la reconnaissance de formes (ICPR), décembre 2016, pp. 4232–4237 (2016).

[20]. Krizhevsky A., Sutskever I. et Hinton G.E. : " Classification Image Net avec Réseaux profonds de neurones convolutionnels ", dans Proc. 25e Int. Conf. sur les informations neuronales Systèmes de traitement (NIPS), pp. 1097-1105 (2012).

[21]. Bendjoudi S., Bourouba H., Doghmane H. et al.,: " Amélioration des performances d'identification de l'empreinte palmaire grâce à des fonctionnalités d'image statistique binarisées basées sur des patchs ", J. Electron. Imag. 28 (5) 053009, (2019).

[22]. Doghman H., Bourouba H., Messaoudi K. et al.,: " Reconnaissance de l'empreinte palmaire basée sur la représentation multi-échelles discriminante ", J. Electron. Imag. 27 (5) 053032 (2018).

[23]. Mokni R., Drira H. et Kherallah M.:" " Combinant l'analyse de forme et le motif de texture pour l'identification de l'empreinte palmaire ", Multimed. Application d'outils. 76, 23981–24008 (2017).

[24]. Ding C., Choi J., Tao D. et Davis L. S.: " Double croix multidirectionnelle à plusieurs niveaux modèles pour une reconnaissance faciale robuste & quot;, transactions IEEE sur l'analyse de modèles et la machine intelligence, 38 (3): 518-531 (2016).