REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE 8 MAI 1945 – GUELMA
FACULTE DES SCIENCES ET DE LA TECHNOLOGIE
DEPARTEMENT ELECTRONIQUE ET TELECOMMUNICATIONS

LABORATOIRE PROBLEMES INVERSES, MODELISATION,
INFORMATION ET SYSTEMES (PI:MIS)

THÈSE

Présentée en vue de l'obtention du diplôme en Electronique :

Doctorat 3ème Cycle en LMD

Intitulée :

Identification de personnes par signature manuscrite

Présentée par : **Hedjaz HEZIL**

Filière : Electronique

Spécialité : Signaux et Images Biométriques

THÈSE dirigée par :

Rafik DJEMILI Professeur des Universités, Univ. Skikda

Devant le jury composé de :

Abdelhani BOUKROUCHE	Professeur des Universités	Univ. Guelma	Président du jury
Layachi BENNACER	Professeur des Universités	Univ. Guelma	Examinateur
Abdelkrim MOUSSAOUI	Professeur des Universités	Univ. Guelma	Examinateur
Salim OUCHTATI	Maître de conférences 'A'	Univ. Skikda	Examinateur
Aissa BELMEGUENAI	Maître de conférences 'A'	Univ. Skikda	Examinateur
Houcine BOUROUBA	Maître de conférences 'A'	Univ. Guelma	Invité

Soutenue le : / /2018


بسم الله الرحمن الرحيم

Dédicaces

Je dédie ce travail :

***À** ceux ; qui m'ont tant donné sans rien demander, qui m'ont toujours offert leur soutient m'ont épargné aucun effort pour m'aider, qui m'ont appris mes principes, à qui tous les mots ne suffisent pas pour les remercier :*

« Mes très chers parents »

***À** ma femme et ma petite belle fille 'Arine'*

***À** mes frères et à ma sœur avec mes souhaits de bonheur et de prospérité.*

***À** mon encadreur pour son aide précieuse*

***À** mes collègues*

A**ux membres du laboratoire **PI: MIS

***À** toute ma famille*

***À** tous mes amis*

***À** toute personne, qui m'a aidée à réaliser ce modeste travail, de proche ou de loin.*

Remerciements

Je remercie en premier lieu mon grand DIEU qui m'a donné à la fois le courage, la volonté, et la patience afin d'élaborer cette thèse de recherche scientifique.

Je tiens à remercier, mon directeur de thèse Monsieur : ***Rafik DJEMILI,*** Professeur à l'université 20 Aout 1955 à Skikda, pour l'encadrement de mon travail et pour son encouragement, ainsi que son soutien tout au long de la thèse. Je le remercie pour tout son aide. Son enthousiasme et sa patience ont beaucoup facilité et agrémenté mon travail. Il a été toujours disponible pour répondre aux questions que je lui posais. Ses remarques m'ont permis de faire progresser ce travail.

Un remerciement spécial est aussi adressé à Monsieur : ***Abdelhani BOUKROUCHE*** Professeur à l'université 08 Mai 1945 à Guelma et directeur de notre laboratoire PI:MIS. Je le remercie très sincèrement pour son extrême gentillesse, son aide et surtout ses encouragements durant toute la période de préparation de cette thèse.

Je tiens aussi à exprimer mes très sincères remerciements à Monsieur ***Hocine BOUROUBA***, Maître de conférences à l'université de Guelma, qui a accepté de donner des heures de leur temps libre pour me permettre de réaliser plusieurs expérimentations de cette thèse.

Nous tenons tout particulièrement à remercier Monsieur ***Abdelhakim DOGHEMAN***, qui nous a soutenus, conseiller et nous a offert leur temps précieux.

Je remercie également tous mes collègues de notre laboratoire **PI : MIS** avec lesquelles j'ai pu avoir de nombreux échanges, et évoluer mon esprit de débat scientifique, en leurs espérant une bonne continuation et une bonne chance.

Je tiens également à remercier les membres du jury qui m'ont fait l'honneur de bien vouloir évaluer mon travail, et plus précisément :

Monsieur ***Layachi BENNACER,*** Professeur à l'Université de Guelma, Monsieur ***abdelkrim MOUSSAOUI***, Professeur à l'Université de Guelma, Monsieur ***Salim OUCHTATI,*** Maître de conférences à l'Université de Skikda, Monsieur ***Aissa BELMEGUENAI,*** Maître de conférences à l'Université de Skikda, d'avoir accepté de juger le présent document.

J'adresse un grand MERCI à toute l'équipe du ***Système National de Documentation en Ligne (SNDL)*** qui a mis à la disposition de tous les chercheurs Algériens une immense base de documentation Multidisciplinaires gratuite (ouvrages, thèses, rapports, communications, revues et bases de données scientifiques, etc.).

RESUME

Ce mémoire propose l'utilisation des caractéristiques binaires dans les systèmes de reconnaissance de signature hors ligne. En effet, la reconnaissance de la signature hors ligne trouve principalement son importance pour l'authentification des documents administratifs et officiels dans lesquels une précision plus élevée est nécessaire. Dans l'approche proposée, les fonctionnalités sont extraites en utilisant deux descripteurs: les caractéristiques statistiques d'image binaire (BSIF) et les modèles binaires locaux (LBP). Pour évaluer la fiabilité de la méthode, des expériences ont été réalisées à l'aide de deux bases de données publiques, MCYT-75 et GPDS-100. En utilisant la méthode de k-plus-proches voisins comme classifieur, les performances de reconnaissance atteignent respectivement des valeurs de 97,3% et 96,1% pour les bases de données MCYT-75 et GPDS-100.

Concernant le système de vérification de signatures manuscrites, la précision de la reconnaissance mesurée avec un taux d'égal erreur ou Equal Error Rate (EER) en anglais, a atteint respectivement 4,2% et 4,8% sur GPDS-100 et GPDS-160. De plus, l'EER pour la base de données MCYT-75 a atteint 7,78%.

Toutes ces précisions ont surpassé les différents résultats de performance rapportés dans la littérature.

Mots-clés: Biométrie ; reconnaissance signature manuscrite ; identification par signature ; vérification par signature manuscrite ; les modèles binaires locaux (LBP) ; les caractéristiques statistiques d'image binaire (BSIF) ; k-plus proches voisins (KNN).

ABSTRACT

This paper proposes the use of binary features in offline signature recognition systems. Indeed, offline signature recognition finds mainly its importance for the authentication of administrative and official documents in which a higher accuracy is needed. In the proposed approach, features are extracted by using two descriptors: binary statistical image features (BSIF) and local binary patterns (LBP). To assess the reliability of the method, experiments were carried out using two publicly available datasets, MCYT-75 and GPDS-100 databases. Using a k-nearest neighbour classifier, recognition performances reach values high as 97.3% and 96.1% for MCYT-75 and GPDS-100 databases respectively.

In signature verification, the classification accuracy measured with equal error rate (EER) achieved 4.2% and 4.8% respectively on GPDS-100 and GPDS-160. In addition, the EER for theMCYT-75 database has attained 7.78%. All those accuracies outperformed various performance results reported in literature.

Keywords: offline signature recognition; feature extraction; biometrics; local binary patterns (LBP); binary statistical image features (BSIF); k-nearest neighbour classifier (KNN).

ملخص

يقترح هذا العمل مبدا استعمال الخصائص الثنائية في نضام *التعرف* البيو متري للتوقيع دون اتصال، مع العلم ان هذا النظام يجد أهميته كبيرة في مجال التعرف على الوثائق الادارية و الرسمية التي تحتاج دقة كبيرة للمعاينة.

في العمل المطروح، تم استخراج الخصائص و المميزات عن طريق خاصيتين :LBP وBSIF

ولتقييم واقعية العمل ، اجريت التجارب على قاعدتي بيانات متاحتين اللتين هما : GPDS-100 و MCYT-75 .

وباستخدام المصنف KNN بلغت نسبة التحقق الى قيمة عالية 97.3 % و 96.1 % لقواعد البيانات MCYT-75 و GPDS-100 على التوالي.

اما فيما يخص *التحقق* من التوقيع كمرحلة ثانية ، فقد حققت دقة التصنيف المقاسة بمعدل خطأ مكافئ (EER) 4.2 % و 4.8 % على التوالي في GPDS-100 و GPDS-160. بالإضافة إلى ذلك، حققت EER لقاعدة بيانات MCYT-75 نسبة 7.78٪. كل هذه النتائج فاقت النسب المذكورة

Table de matières

Liste des tableaux

Liste des figures

INTRODUCTION GENERALE

La biométrie est la science qui détermine l'identité d'un individu; elle est basé sur des mesures physiologiques, chimiques ou comportementales d'un ou de plusieurs de ses attributs biologiques, tels que la signature manuscrite, l'iris, la géométrie de la main ou de la paume, les caractéristiques faciales, la voix, l'odeur, les frappes, l'ADN .

L'importance de la biométrie dans les sociétés modernes a été augmentée en raison du grand besoin de sécurité et des systèmes de gestion des identités à grande échelle, fonctionnellement basées sur la détermination précise de l'identité d'un individu dans un contexte d'applications largement interconnectées. Exemples de telles applications: contrôle d'accès sécurisé, frontières internationales et applications juridiques, partage de ressources informatiques dans un réseau public, accès à haute sécurité aux zones nucléaires, banques en ligne, cartes de crédit.

Les systèmes biométriques fonctionnent selon le principe selon lequel la plupart des caractéristiques biologiques humaines sont particulières pour chaque individu et peuvent être acquises en utilisant des capteurs appropriés et peuvent être représentés sous forme numérique. Ainsi, ces systèmes peuvent être considérés comme un moteur de reconnaissance de formes et peuvent être intégrés sur différents marchés.

Plusieurs caractéristiques humaines ont été étudiées et testées. Ces modalités peuvent être encore subdivisées en différentes sous-catégories selon leur position respective dans le corps humain, telles que : Caractéristiques de la région de la main (ex., empreinte digitale, géométrie de la main,…), Caractéristiques de la région faciale (ex., visage et oreille), Caractéristiques de la région oculaire (ex., iris et rétine), Caractéristiques comportementaux (ex., façon de marcher, signature électronique,…) et Caractéristiques médicaux-chimiques (ex., os, odeur, ADN,…). Bien que l'ADN, l'iris et l'empreinte digitale soient considérés parmi les modalités extrêmement fiables, elles reposent, malheureusement, sur la coopération du participant-capteur.

Dans le cadre de cette thèse, nous nous sommes concentrés sur les caractéristiques comportementales, à savoir la signature manuscrite, cette dernière est l'une des caractéristiques biométriques les plus anciennes utilisées pour l'authentification d'un individu ou d'un document.

Jusqu'à présent, la signature reste l'un des moyens les plus populaires pour l'authentification de documents officiels tels que les chèques bancaires, les transactions par carte de crédit, les certificats, les contrats et les obligations. L'objectif principal d'un système automatique de vérification de signature est de vérifier l'identité d'un individu sur la base de l'analyse de sa signature. Selon la méthode d'acquisition de la signature, un système peut être classé en ligne ou hors ligne. Les signatures manuscrites peuvent

être utilisées avec des taux de réussite élevés pour l'identification biométrique. De plus, l'importance de la vérification de la signature provient du fait que les signatures ont une acceptation élevée des utilisateurs et sont légalement acceptées comme méthode de vérification d'identité.

Comme indiqué ci-dessus, il existe deux méthodes principales de vérification de signature, de méthodes en ligne et hors ligne. Le premier mesure des données séquentielles telles que la pression de vitesse et / ou de stylo ... etc., avec un dispositif spécial. Ce dernier utilise un scanner optique pour obtenir des données écrites sur papier.

Dans cette étude, nous proposons un système de reconnaissance de signature hors ligne basé sur l'utilisation des méthodes de l'image statistique binaire (BSIF) et des formes binaires locaux (LBP) pour extraire des fonctionnalités. Nos tests ont été établis en utilisant des images fournies par les bases de données MCYT et GPDS, L'approche est appliquée sur deux sujets principaux de reconnaissance de signature, principalement l'identification et la vérification de signature.

Ce manuscrit est composé de quatre chapitres. Il est structuré comme suit :

Dans le premier chapitre « *Introduction à la biométrie et aux systèmes biométriques* » nous présentons des notions et des définitions de base liées à la biométrie et au principe de fonctionnement des systèmes biométriques ainsi que les outils, généralement utilisés pour évaluer leurs performances. Après on a présenté et on a comparé quelques modalités biométriques les plus utilisées à nos jours. Dans ce premier chapitre nous accordons une attention particulière à la reconnaissance biométrique par signature manuscrite parmi les autres modalités biométriques, puisqu'elles constituent l'objectif de cette thèse.

Nous présentons à travers le deuxième chapitre intitulé «*Reconnaissance par signature* », les éléments essentiels pour la reconnaissance et le traitement de signature hors ligne. On y expose les modes de fonctionnement d'un système biométrique (enroulement, vérification et identification) par l'intermédiaire de schéma synoptiques, nous évoquons ensuite le processus de vérification de signature hors ligne, les avantages de l'utilisation de signature manuscrite comme une modalité biométrique et la déférence entre les deux systèmes hors ligne et en ligne.

Après avoir introduit au deuxième chapitre, les principales méthodes d'extraction des caractéristiques en lien avec la signature, nous présentons dans ce troisième chapitre, intitulé «*Extraction des caractéristiques*», les techniques que nous avons utilisées et testées dans le but d'extraire des informations biométriques texturées. Nous étudions l'utilisation de deux descripteurs de texture locaux très récents: LBP et BSIF.

Dans le quatrième chapitre «*Résultats expérimentaux et discussions*», nous testons et nous comparons les performances des descripteurs de texture locaux (LBP, BSIF) appliquées sur des données biométrique, en utilisant les bases d'images de signature : MCYT-75, GPDS-100 et GPDS-160.

Nous achevons notre manuscrit par une « Conclusion et perspectives », dans laquelle nous concluons notre travail de recherche et d'autre part, nous établissons de manière étendue des perspectives, notamment en considérant l'implémentation d'un système biométrique multimodal en plus de la signature manuscrite prise comme modalité de base.

Chapitre 1

Introduction à la Biométrie et aux Systèmes Biométriques

1.1. Introduction

La biométrie est la science qui permet de reconnaître l'identité d'une personne sur la base de ses caractéristiques physiologiques, chimiques ou comportementales, telles que: le visage, l'iris, l'odeur, la façon de marcher ou la signature électronique…etc. Avec la nécessité de techniques solides de reconnaissance humaine dans les applications critiques, telles que: le contrôle d'accès sécurisé, le passage des frontières internationales et les applications légales, la biométrie se positionne comme une technologie viable qui peut être intégrée dans les systèmes de management d'identité à grande échelle. Les systèmes biométriques fonctionnent en vertu du principe que la plupart des caractéristiques biologiques de l'être humain soient distinctives pour chaque individu, puissent être acquises d'une manière fiable à l'aide des capteurs convenables et peuvent être représentées dans un format numérique. Ainsi, ces systèmes peuvent être considérés comme des moteurs de reconnaissance des formes et peuvent être incorporés dans divers marchés.

Dans ce chapitre, nous introduisons tout d'abord quelques notions et définitions de bases liées à la biométrie, nous décrivons le principe de fonctionnement d'un système biométrique ainsi que les outils d'évaluations utilisés pour mesurer leurs performances, nous donnons un bref aperçu des modalités biométriques les plus répandues, tout en accordant une attention particulière à la reconnaissance par signature parmi les autres modalités biométriques, puisqu'elles constituent l'objectif de cette thèse.

1.2. Généralités et notions de bases en biométrie

Les méthodes classiques d'authentification biométriques sont basées soit sur *une connaissance* à priori de la personne (ex., un mot de passe ou un code d'activation) ou sur *la possession* d'un objet (ex., une pièce d'identité, un badge ou une clef). Cependant, ce type de présentation d'identité peut être facilement perdu, partagé, oublié par son utilisateur ou deviné par d'autres personnes. Aujourd'hui, *la biométrie* est un domaine émergeant ou la technologie améliore notre capacité à identifier une personne. La protection des consommateurs contre la fraude ou le vol est un des buts de la biométrie. L'avantage de l'identification biométrique est que chaque individu a ses propres caractéristiques physiques qui ne peuvent être changé, perdues ou volées [1], [2].

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. ***La figure 1.1*** illustre un exemple de quelques modalités biométriques.

Fig.1.1. Exemples de modalités (physiologiques et comportementales)

1.3. les modalités biométriques

Il existe plusieurs modalités qui ont été utilisées dans plusieurs systèmes biométriques, Bien qu'il existe un très grand nombre de modalités biométriques, nous pouvons distinguer deux grandes catégories ***figure 1.2*** :

a) La biométrie physiologique ou morphologique : Utilisant les caractéristiques physiologiques de l'individu (visage, main, oreille, empreinte digitale, la rétine …)
b) La biométrie comportementale : qui se base sur l'analyse de comportements d'un individu (la signature, la démarche, la voix …) [3]

Nous allons aussi introduire quelques modalités cachées qui sont en cours d'expansion

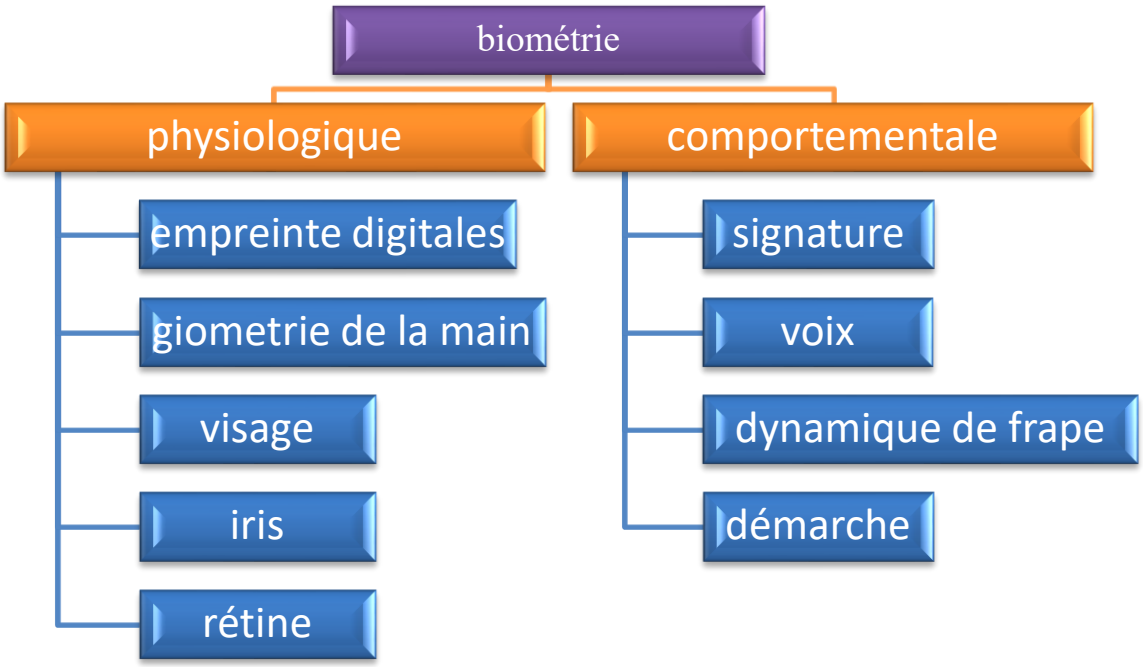


Fig.1.2. Catégories des méthodes d'identification biométriques

1.3.1. modalités comportementale :

Dans ces techniques de reconnaissance, on s'intéresse aux caractéristiques physiques en activité des individus qui peuvent être typiques et permettent de distinguer une personne d'une autre, Dans la suite, nous présenterons quelques modalités de ce type avec leurs modes d'utilisations :

i.la signature

L'identification par signature comme technique était parmi les premières utilisées dans le demain de la biométrie et le moyen le plus accepté et le plus utilisé pour authentifier des documents. Elle a été acceptée comme une méthode d'authentification légale par les gouvernements et dans les transactions commerciales .Les systèmes de vérification de signatures se base sur deux catégories selon le type d'acquisition des données : en ligne ou *online* [4], [1] hors-ligne ou *offline* [5], [1].

Les systèmes *online* traitent les signatures, qui sont produites à l'aide d'une tablette à digitaliser, comme étant un signal dynamique et font l'extraction de plusieurs caractéristique comme les points de pauses, la pression, la direction, la vitesse pendant la signature et l'angle d'inclinaison. Ces caractéristiques dynamiques sont spécifiques à chaque individu

D'autre part, les systèmes *offline* traitent la signature à partir d'une image provenant d'un scanner. Ces systèmes sont assez complexes dû à l'absence de caractéristiques dynamiques stables. Dans notre travail on a travaillé sur deux bases offlines MCYT-75 et GPDS.

ii.la dynamique de frappe au clavier :

Cette modalité est une caractéristique comportementale n'est pas unique pour chaque individu, Les paramètres suivants sont généralement pris en compte par les systèmes de reconnaissance de cette modalité : la position de l'utilisateur par rapport au clavier et le type du clavier utilisé, la vitesse de frappe, la suite de lettres, la mesure des temps de frappe, la pause entre chaque mot et la reconnaissance de mot(s) précis [6], [1].

La différence avec ces systèmes se situe plus au niveau de l'analyse, qui peut être soit statique et basée sur des réseaux neuronaux [7], soit dynamique et statistique (comparaison continuelle entre l'échantillon et la référence). Ces techniques sont assez satisfaisantes, mais restent néanmoins statistiques.

iii.La démarche

Elle se réfère à la manière dont une personne marche et c'est l'une des rares modalités biométriques qui peuvent être utilisées pour reconnaître des personnes à distance. On cherche ici à identifier un individu par sa façon de marcher et de bouger tout en analysant des images vidéo de la promenade du candidat [1], [8]. Les gens montrent de différents traits tout en marchant comme le maintien du corps, la distance entre les deux pieds, la position des joints tels que les genoux et les chevilles et les angles de balancement [9] ce qui aide de manière significative à les identifier.

Cette modalité est notamment appropriée pour les applications de vidéosurveillance. Les performances des systèmes à base de la démarche ne sont pas assez acceptables, car elles sont affectées par le changement de l'environnement.

iv.La voix

La voix est considérée comme une combinaison entre les caractéristiques biométriques physiques et comportementales. [10], [1]. Les caractéristiques physiques de la voix d'un individu sont basées sur la forme et la taille des appendices (ex., les tractus vocaux, la bouche, les cavités nasales et les lèvres) qui sont utilisées dans la synthèse du son. Ces caractéristiques physiques de la parole humaine sont invariantes pour chaque individu, par contre, l'aspect comportemental de la parole se change au cours du temps en raison de l'âge, des conditions médicales (ex., rhume) et de l'état émotionnel. La voix n'a pas été connue comme une modalité très distinctive et n'est pas appropriée pour une identification à grande échelle.

Un système de reconnaissance vocale de type texte-dépendant est basé sur l'expression d'une phrase fixe et prédéterminée. Par contre, un système de reconnaissance vocale de type texte-indépendant identifie un individu à la base de ce qu'il parle. L'implémentation des systèmes de type texte-indépendant est plus difficile par rapport aux systèmes de type texte-dépendant, mais elle offre plus de sécurité et protection contre les attaques malveillantes. L'inconvénient des systèmes de reconnaissance vocale est que les caractéristiques de la parole sont sensibles à certains facteurs comme le bruit [10]. La reconnaissance vocale est plus appropriée dans les applications qui se basent sur le téléphone malgré la dégradation de la qualité de la voix, typiquement, à travers le canal de transmission.

1.3.2. Modalité physiologique (morphologique)

Ces types de reconnaissance mesurent une caractéristique spécifique de la structure ou de la forme d'une partie du corps humain. Nous pouvons citer les exemples les plus connus :

i. L'empreinte digitale

L'être humain a utilisé les empreintes digitales, depuis plusieurs décennies, en criminalistique et en identification biométrique. Le taux d'identification à l'aide d'empreintes digitales a été montré d'être très élevé [11]. Une empreinte digitale est le motif de crête et de vallées sur la surface au bout d'un doigt. L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. En fait, les corps policiers utilisent cette technique depuis plus de 100 ans. Aujourd'hui, les empreintes digitales sont recueillies sur une scène de crime et sont ensuite comparées à celles contenues aux base de donné [12].

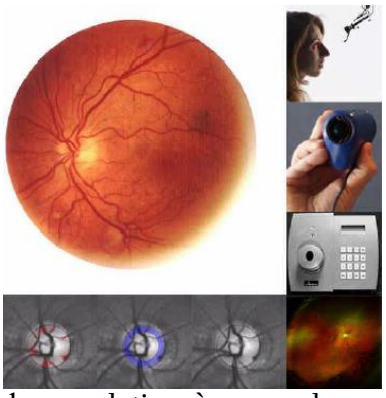
L'empreinte digitale est une impression produite par la transpiration, la graisse, l'huile ou l'encre présente dans les lignes de crêtes non uniformes contenues dans la partie supérieure de chaque doigt de main d'un être humain. Ces empreintes sont uniques pour chaque individu. Même des jumeaux parfaits n'ont jamais des empreintes digitales identiques.

ii. La géométrie de la main

La biométrie par cette modalité extrait près d'une centaine de paramètres comme les épaisseurs, les longueurs, les surfaces et les largeurs des doigts de la main [13]. La géométrie de la main n'est pas connue comme une modalité très distinctive, ainsi les systèmes de reconnaissances basés sur cette modalité ne peuvent pas être utilisés pour identifier un individu à partir d'une grande population. En outre, les informations de la géométrie de la main sont variantes durant la période de croissance des enfants.

L'acquisition de cette modalité ne nécessite aucune lecture d'empreintes et la mesure des épaisseurs des doigts s'effectue à l'aide de miroirs ce qui veut dire que l'acquisition s'effectue en trois dimensions. La taille du capteur est le major inconvénient de cette modalité. De plus, ce capteur coute très cher par rapport aux autres modalités. Tous ces inconvénients réduisent l'utilisation de cette technique biométrique. Il existe aussi des systèmes d'authentification qui se basent uniquement sur la mesure de quelques doigts au lieu de la main entière; ces appareils sont plus petits que ceux utilisés pour la géométrie de la main.

iii. La rétine



Cette technologie est bien adaptée aux applications de haute sécurité (sites militaires, salles de coffres forts, etc). Lors de l'acquisition, l'utilisateur place son œil à proximité du capteur où un rayon lumineux illumine le fond de l'oeil pour extraire des points repères. La détermination des caractéristiques de la rétine consiste à l'extraction de la distribution géographique des vaisseaux sanguins [14]. Cette mesure est richesse de caractéristique plus de 400 [15]. Cependant, la rétine n'est pas appropriée pour une grande population à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques centimètres). En outre, des risques liés à la santé sont signalés, ce qui réduit l'utilisation de cette modalité.

iv. Le visage

La reconnaissance par cette modalité s'effectue de façon spontanée dans la vie quotidienne des êtres humains. L'authentification par le visage est la technique la plus commune et la plus populaire puisqu'elle correspond à ce que nous utilisons naturellement pour reconnaître une personne [16]. Les caractéristiques qui servent à la reconnaissance du visage sont : les yeux, la bouche, la forme du visage (contour), etc [17], [1].
Dans un système de reconnaissance faciale, la photo d'une personne est prise volontairement ou involontairement à l'aide d'une caméra. Puis, un ensemble de caractéristiques propres à chaque individu est extrait (le tour du visage, la position des oreilles, les coins de la bouche, l'écartement des yeux et la taille de la bouche) à partir de la photo. Ces systèmes sont capables de faire face aux techniques de *spoofing* [18] comme le port de lunettes, la barbe, le maquillage, etc.

v. L'iris

L'iris est la région annulaire de l'oeil délimitée par la pupille et la sclérotique. La texture complexe de l'iris comporte des informations très distinctives et utiles pour différencier et reconnaître les individus [19], donc elle est considérée comme la modalité la plus précise pour l'identification et l'authentification [20]. Son seul inconvénient est son coût assez élevé, ce qui ne la rend pas autant répondu pour des applications quotidiennes. Alors, son utilisation s'est limitée dans des endroits où la sécurité est primordiale et même critique comme dans les bases nucléaires par exemple. La reconnaissance par l'iris [22] est utilisée aussi dans le secteur financier pour les employés et les clients, dans les hôpitaux et dans les grands aéroports. Une personne voulant s'identifier place son œil à quelques centimètres du capteur et l'image de l'iris est prise par une caméra. Ensuite, les caractéristiques sont extraites de l'image de l'iris et comparées à celles enregistrées dans la base de données [1], [21].

vi. L'oreille

Au cours de plusieurs années, l'oreille humaine a été utilisée comme un moyen d'identification en médecine légale. L'oreille humaine possède une richesse d'information qui se situe sur une surface 3D incurvée, cette richesse d'information a attiré l'attention des scientifiques légaux [22], [1].

Les images d'oreilles peuvent être acquises simultanément avec les images du visage et employées ensemble pour améliorer d'une manière significative la précision de la reconnaissance. Il est possible aussi d'employer l'oreille et le visage comme une pièce complémentaire d'information.

Les recherches ont légèrement évolué pour développer des technologies automatisées d'identification par oreille. Cependant, des efforts significatifs sont encore exigés pour améliorer la détection d'oreille, la segmentation et la possibilité d'identification dans le but de faire un déploiement dans la surveillance et dans les autres applications commerciales [1].

1.4. Comparaison entre les modalités biométriques

D'après la description précédente des différentes modalités biométriques, on a pu constater que chacune d'entre elles présente des avantages et des inconvénients et que certaines applications nécessitent de choisir une modalité à l'égard d'une autre. Ce choix s'effectue essentiellement en tenant compte d'un nombre de paramètres comme l'origine de l'application, son coût, les performances espérées du système et l'acceptation de la modalité par l'utilisateur.

Dans la ***figure 1.3***, on a effectué un classement des différentes modalités biométriques selon deux axes : la performance et le coût. Les systèmes à base de la voix ou du visage ne sont pas couteux, mais leurs performances restent limites. Les modalités de la biométrie cachée sont incontestablement les modalités les plus performantes. En revanche, les systèmes à base de ces modalités sont très coûteux à cause du prix élevé des dispositifs d'acquisition.

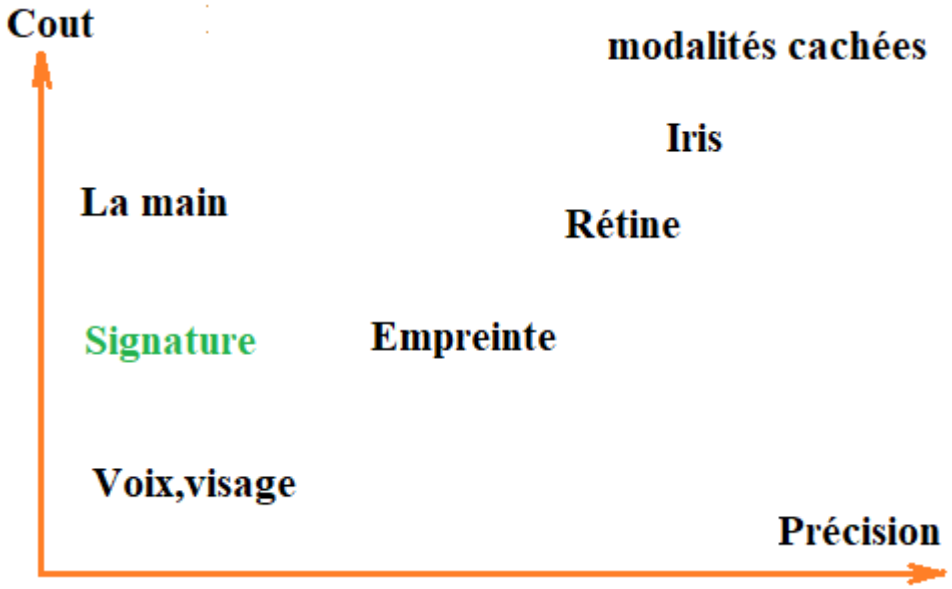


Fig.1.3. Classement des modalités biométriques selon le cout et la précision

1.5. Architecture fonctionnelle d'un système biométrique

Un système biométrique est généralement composé de deux principaux modes (***voir la Figure 1.4***) qui sont le mode d'*apprentissage* appelé également mode d'enregistrement ou d'enrôlement et le mode de *reconnaissance* (vérification ou identification). Le premier mode consiste à enregistrer dans une base de données les caractéristiques physiques ou comportementales d'un individu sous forme d'un "*Modèle*" biométrique appelé aussi "*Template*" ou "*Signature*". Le deuxième mode consiste à tester les mêmes caractéristiques et à les comparer avec les modèles biométriques stockés dans la base de données. Si les données testées correspondent à un modèle biométrique enrôlé, l'individu est donc considéré comme reconnu [23].

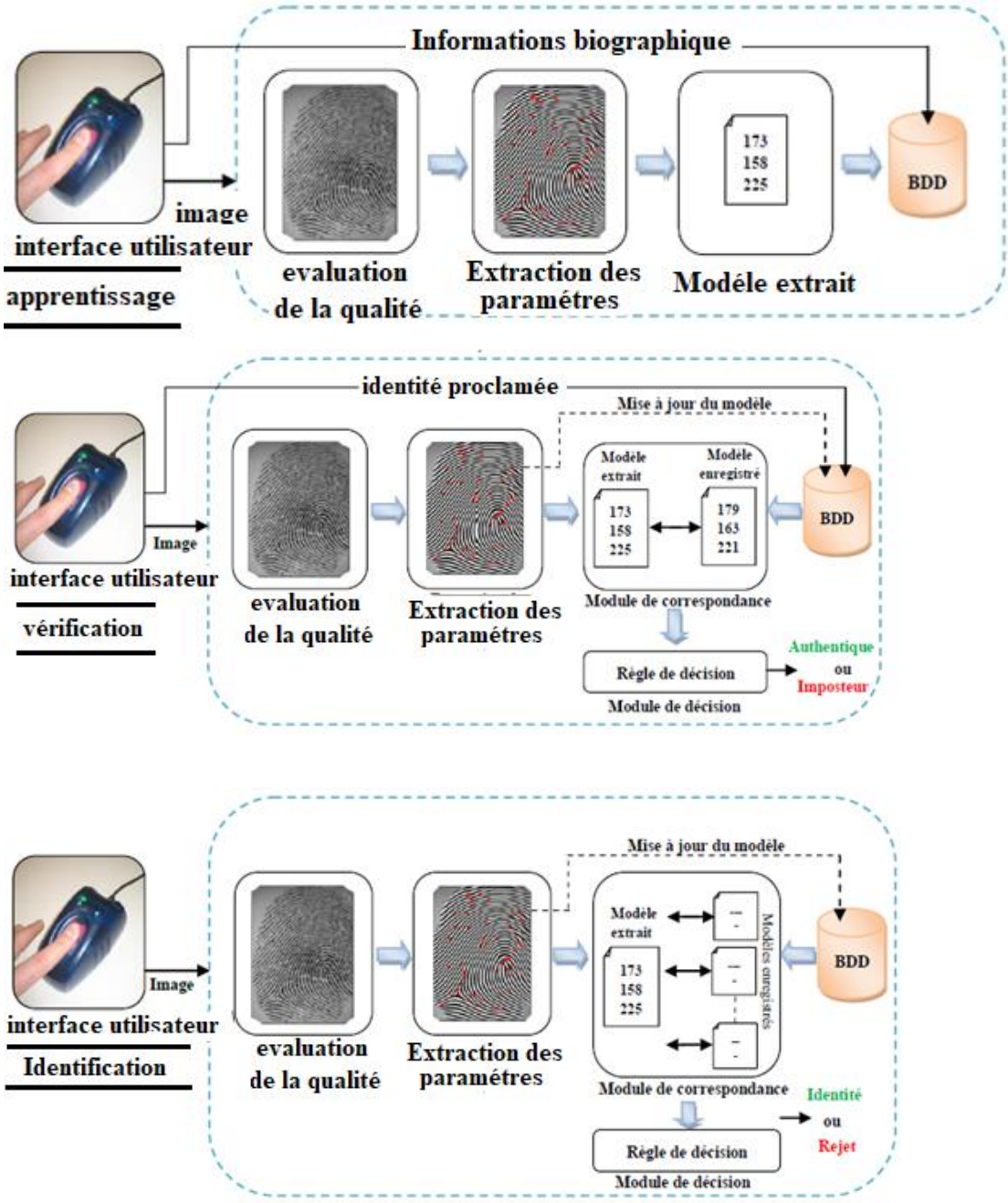


Fig.1.4. Architecture fonctionnelle d'un système biométrique. Diagramme des processus d'apprentissage, vérification et identification [1]

1.6. Caractéristiques de la biométrie

Comme nous l'avons dit précédemment, les modalités biométriques doivent être déterminées par quelques caractéristiques en but d'assurer leurs fiabilités, Chaque modalité possède ses propres avantages et inconvénients, le choix d'une modalité biométrique pour une application donnée dépend d'une variété de paramètres liés à la nature et les exigences de l'application et aux propriétés de la modalité [24], ont identifié quelques paramètres généralement employés dans une application biométrique, qui sont:

a. Universalité: tout individu, qui accède à une application, doit posséder le trait, donc la modalité doit exister chez tous les individus.

b. Unicité: Le trait biométrique doit être suffisamment différent d'une personne aux autres.

c. Stabilité: Le trait biométrique d'un individu doit être suffisamment stable et invariant au cours du temps.

d. Mesurabilité: il devrait être possible de numériser les données biométriques à l'aide d'un dispositif d'acquisition.

e. Performance: Signifie que l'authentification doit être précise et rapide.

f. Acceptabilité: Indique que la modalité biométrique utilisée doit être bien accepté par les utilisateurs du système.

Il n'existe aucun trait biométrique exceptionnel qui satisfait et répond efficacement à toutes les exigences mais à des degrés différents.

Tableau 1.1extrait de [1], [25] et [26], montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières.

Le choix de la modalité est ainsi effectué selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. A noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale des individus.

Type	modalité	précision	Simplicité d'utilisation	Acceptation par l'utilisateur
morphologique	empreinte	Haute	Moyenne	Basse
	Iris	Haute	Moyenne	Moyenne
	Rétine	Haute	Basse	Basse
	Visage	Basse	Haute	Haute
	Voix	Moyenne	Haute	Haute
	Géométrie de la main	Moyenne	Haute	Moyenne
comportementale	Frappe au clavier	Basse	Haute	Moyenne
	Démarche	Basse	Moyenne	Moyenne
	Signature	Moyenne	Moyenne	Haute
cachée	ECG, EMG	Haute	Moyenne	Moyenne
	Cerveau	Haute	Basse	Basse
	Imagerie par rayon x	Haute	Basse	Basse

Tableau 1.1. Comparaison entre les modalités biométriques [1], [25], [26]

1.7. les systèmes biométriques et leurs modes de fonctionnements

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

Après l'extraction de ces caractères, le système biométrique compare ces derniers par rapport aux modèles stockés dans la base de données et exécute une action basée sur le résultat de la comparaison. Par conséquent, un système biométrique générique peut être vu comme un processus à quatre modules principaux : un module de capture, un module de prétraitement et d'extraction des caractéristiques, un module de correspondance et un module de décision ***figure 1.5***.
Le fonctionnement de chaque module est détaillé ci-dessous [27].

1.7.1. Le module de capture *:* est responsable de l'acquisition des données biométriques d'un individu (cela peut être un : un lecteur, un scanner biométrique, une caméra ou un module de balayage approprié est requis pour la détection des donnée biométrique d'un individu)

1.7.2. Le module prétraitement d'extraction de caractéristiques *:* les donnée biométrique obtenue lors de la première phase doit être évaluée par ce module et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Généralement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classes.

1.7.3. Le module de correspondance : Le vecteur des caractéristiques, extrait, est comparé avec les modèles stockés dans la base de données pour générer des scores de correspondances. Le résultat de cette comparaison va être utilisé pour prendre une décision sur le taux de correspondance de la signature biométrique, inscrites dans la base de données (MCYT, GPDS) pour la validation ou le rejet de l'identité de l'individu à reconnaitre. Donc 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.

1.7.4. Le module de décision *:* vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés (bases de données).

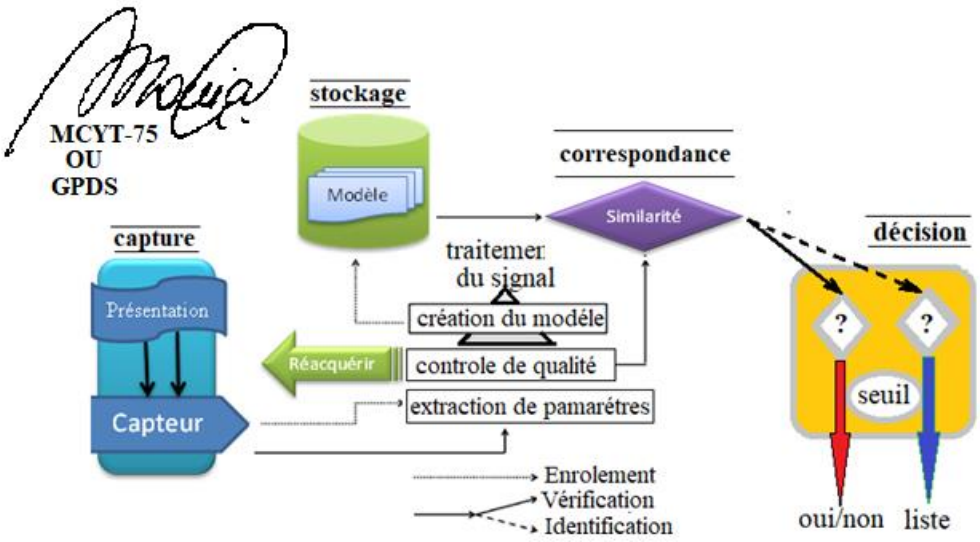


Fig.1.5. les modules principaux d'un système biométrique [30].

1.8. Performances d'un système biométrique

Dans les systèmes basés sur les mots de passe, une correspondance parfaite est nécessaire entre les deux chaînes de caractères pour valider l'identité d'un individu. Par contre, les systèmes biométriques rencontrent rarement deux modèles biométriques d'un même utilisateur présentant exactement les mêmes vecteurs de caractéristiques, en raison de: mauvaises conditions (ex., une empreinte digitale qui contient un bruit lié à un défaut du capteur), changements des caractéristiques biométriques de l'utilisateur (ex., une maladie respiratoire effectuant la reconnaissance du speaker), changements des conditions ambiantes (ex., le changement du niveau d'illumination en reconnaissance par visage) et variations en interaction utilisateur-capteur (ex., iris occlue ou empreinte digitale partielle). Il est donc rare d'avoir deux modèles biométriques exactement similaires provenant du même utilisateur. En effet, une correspondance parfaite entre deux vecteurs de caractéristiques peut indiquer la possibilité qu'il y ait une attaque malveillante lancée contre le système.

1.9. vérification et identification

Un système biométrique peut fonctionner en mode vérification ou en mode identification (voir Figure1.2).

- ✓ Dans la phase de vérification [2], le système évalue l'identité d'une personne en comparant les données biométriques capturées avec son (ses) propre(s) modèle(s) enregistré(s) dans la base de données du système. Dans ce type d'application, un individu qui veut être reconnu par le système doit proclamer son identité, habituellement, par son numéro d'identification personnelle (PIN), par son nom d'utilisateur ou par sa carte magnétique, le système effectuera une comparaison de type *un-contre-un* pour déterminer si cette proclamation est vraie ou fausse. La vérification est typiquement utilisée pour une reconnaissance positive afin d'empêcher l'utilisation d'une même identité par plusieurs personnes.

✓ En mode identification [2], le système identifie un individu en recherchant le modèle enrôlé qui représente la meilleure correspondance parmi tous les modèles d'utilisateurs stockés dans la base de données. Par conséquent, le système effectue une comparaison de type *un-contre-tous* afin d'établir l'identité de cet individu. L'identification est une composante essentielle pour les applications de reconnaissances négatives; l'objectif de ce type de reconnaissance est d'empêcher l'utilisation de plusieurs identités par un seul individu. Comme les méthodes traditionnelles de reconnaissances d'individus telles que les mots de passe et les possessions peuvent fonctionner en mode positif, le mode négatif peut être uniquement établi à l'aide de la biométrie.

Dans les systèmes biométriques, la correspondance n'est pas absolue. Ceci est dû à :

- Des conditions imparfaites lors de l'acquisition des échantillons biométriques (ex. : empreinte digital bruitée).
- Des variations de la caractéristique biométrique de l'utilisateur.
- Des changements des conditions ambiantes.
- La différence dans l'interaction de l'utilisation avec les dispositifs d'acquisition (ex. : iris occlus).

Cependant, il est très rare d'obtenir un ensemble de caractéristiques exactement similaires lors de deux acquisitions d'échantillons biométriques d'un individu. En effet, une correspondance parfaite de deux échantillons déclenche une mise garde du systèmecontre une tentative de fraude par reproduction.

Le degré de similitude entre deux ensembles de caractéristiques est appelé : le taux de similarité (simlarity score). Le taux de similarité d'une comparaison entre deux échantillons d'un trait biométrique du même individu est appelé : taux d'authenticité (genuine score ou authentic score). Le taux de similarité entre deux échantillons de deux individus différents est appelé : taux d'imposture (impostor score).

Comme montré sur ***la figure 1.6 (a)***, il est question d'un compromis, défini par un seuil, entre le taux de fausses acceptations et le taux des faux rejets. C'est –à-dire qu'un taux d'authenticité en dessous du seuil généré un faux rejet, tandis qu'un taux d'imposture qui dépasse le seuil résulte une fausse acceptation.

La performance d'un système biométrique est quantifiée par le taux de deux erreurs fondamentales définies dans [28], [29] par :

- **Le Taux de Faux Rejets (*False-Rejection Rate*), noté FRR :** il exprime le pourcentage des utilisateurs authentiques faussement rejetés par un système biométrique. En d'autres termes, ce taux représente les données de test authentiques qui ont été incorrectement rejetées et considérées comme des imposteurs. FRR est aussi nommé: *False Non-Match Rate* (FNMR).
- **Le Taux de Fausses Acceptations (*False-Acceptance Rate*), noté FAR :** il exprime le pourcentage des utilisateurs imposteurs faussement acceptés par un système biométrique. En d'autres termes, il représente les données de test

imposteurs qui ont été incorrectement acceptées et considérées comme authentiques.

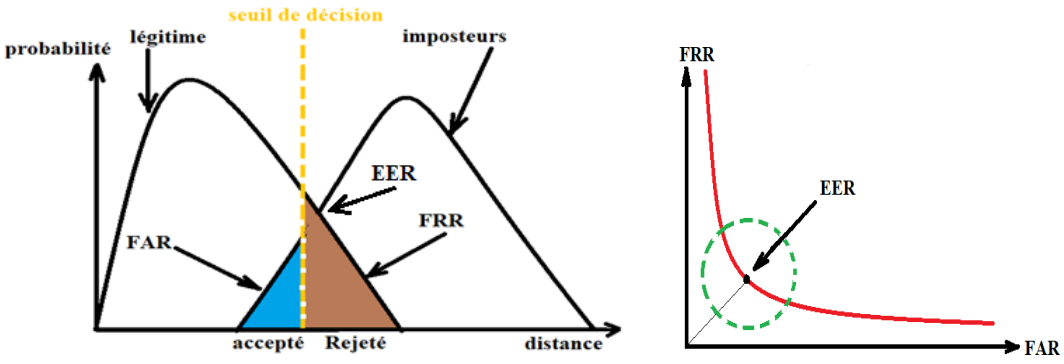
En pratique, la valeur du FAR est affectée par le nombre de fausses acceptations (FA) divisé par le nombre de tests imposteurs dans la base de données (N). Tandis que, la valeur du FRR est affectée par le nombre de faux rejets (FR) divisé par le nombre de tests authentiques (M). En plus, les deux taux FAR et FRR sont dépendants du seuil de décision θ fixé dans le module de décision. En effet, en faisant varier la valeur des deux taux d'erreurs d'une manière importante. Le calcul du FAR et FRR en fonction de θ est donné par :

$$FAR(\theta) = \frac{FA(\theta)}{N} \quad \textbf{(1.1)}$$

$$FRR(\theta) = \frac{FR(\theta)}{M} \quad \textbf{(1.2)}$$

Le choix optimal de la valeur du seuil de décision θ est très important puisqu'il influe directement sur la performance et la fiabilité du système biométrique. En effet, une valeur élevée du seuil θ entraîne l'apparition d'un grand nombre de faux rejets, par contre d'une faible valeur du seuil, résulte un nombre important de fausses acceptations [31]. La valeur la plus optimale du seuil θ pour faire un équilibre entre le FRR et le FAR correspond à l'endroit où le FAR = FRR est noté par le *point d'équivalence des erreurs (EqualError Rate (EER));* ce dernier est déterminé par le point d'intersection entre la courbe des taux de fausses acceptations et la courbe des taux des faux rejets. Un exemple de détermination du point EER est illustré dans ***la figure1.6 (a)***.

Les deux taux FRR et FAR en différentes valeurs du seuil θ peuvent être récapitulés en utilisant la courbe : *Receiver Operating Characteristic (ROC)* [32]. Cette courbe trace le taux de faux rejets en fonction du taux de fausses acceptations. Elle sera tracée d'une manière paramétrique en fonction des valeurs du seuil θ. Un exemple de détermination du point EER en utilisant la courbe ROC est illustré dans ***la figure 1.6 (b)*** Plus cette courbe tend à rapprocher la forme du repère, plus le système est performant, c'est-à-dire qu'il possède un taux de reconnaissance global élevé.



a) La courbe FRR et FAR ***b) la courbe ROC***

Fig.1.6. Courbes représentatives des taux de similarité FRR, FAR

1.10. Modalités cachées

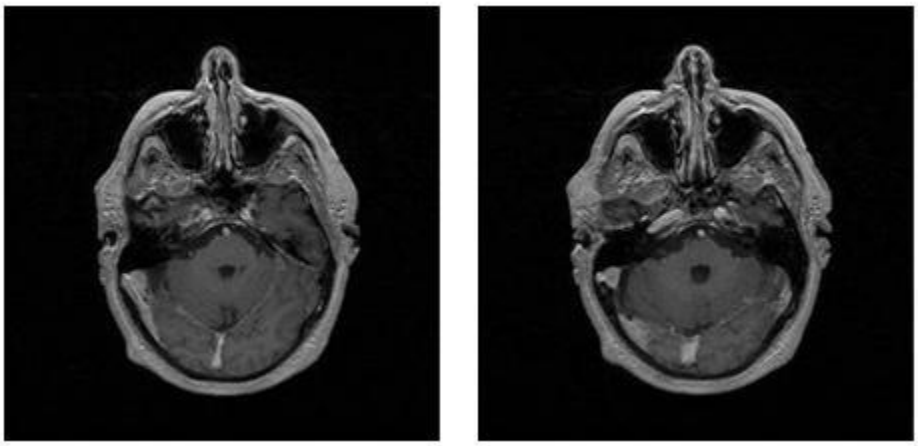
Dans cette partie, nous discutons une idée qui consiste à l'utilisation de la biométrie médicale dans le cadre d'authentification, donc au lieu de reconnaître un individu en utilisant ces modalités morphologiques ou physiologiques (signature, empreinte, visage … etc.) on utilise des traits inaccessibles tel que : les motifs du cerveau, la texture de l'os, ECG … Ce type est en cours d'exploration, s'appelle "la biométrie cachée", les modalités cachées considèrent plutôt les caractéristiques intrinsèques et non visibles du corps humain [1], [33] et [34] sois un *signal physiologique* ou bien un *organe humain* est considéré comme un candidat pour des applications biométriques. Dans la première catégorie Nous pouvons employer l'électrocardiogramme (ECG), l'électromyogramme (EMG). Ainsi, Dans la deuxième catégorie, nous pouvons considérer, comme exemple la morphologie ou la texture du cerveau humain. Nous présentons par la suite quelques idées et travaux réalisés dans ce domaine.

Ce type reste inconvenable, il est difficile d'employer ce type de biométrie pour sécuriser ou accéder à des ressources informatiques. La contrainte principale dans le système d'acquisition c'est la visualisation de la forme du cerveau nécessite l'utilisation des scanners *MRI* (Magnetic Resonance Imaging) et la visualisation du squelette du corps, contenant le crâne et les autres os, nécessite l'usage des scanners de *rayons X*.

1.10.1. Utilisation des images IRM en biométrie de cerveau.

Dans les applications médicales, l'IRM est une technique employée pour visualiser des organes du corps humain (cerveau, muscles, et cœur ...) avec une résolution relativement élevée. Ceci est rendu possible avec l'utilisation d'un champ électromagnétique puissant et constant, produit par un supraconducteur.

L'objectif de cette section est de présenter l'utilisation des images MRI du cerveau humain dans l'identification des individus ***figure 1.7 (a et b)*** et cherche à caractériser le cerveau humain à travers des images IRM 2D et 3D [35]



(a) **(b)**

Fig.1.7. Deux images MRI du cerveau humain qui montrent une différence visuelle entre deux individus : (a) individu 01, (b) individu 02.

Depuis les images IRM 2D ***(Figure 1.8.a)***, on peut faire la reconstruction en 3D ***(Figure 1.8.b)*** du cerveau pour avoir des informations sur la texture. Ainsi d'autres caractéristiques géométriques du cerveau peuvent être considérées comme le rapport isopérimètre et la courbure extérieure corticale.

En fait, la quantité de paramètres qui peuvent être extraits à partir d'une image du cerveau 3D est plus grande que ce que nous pouvons extraire à partir d'autres modalités classiques. On peut aussi définir ce qu'on appelle *brain code* ou code du cerveau à travers une segmentation de la zone d'intérêt du cerveau ***(Figure 1.8.c)*** [39].

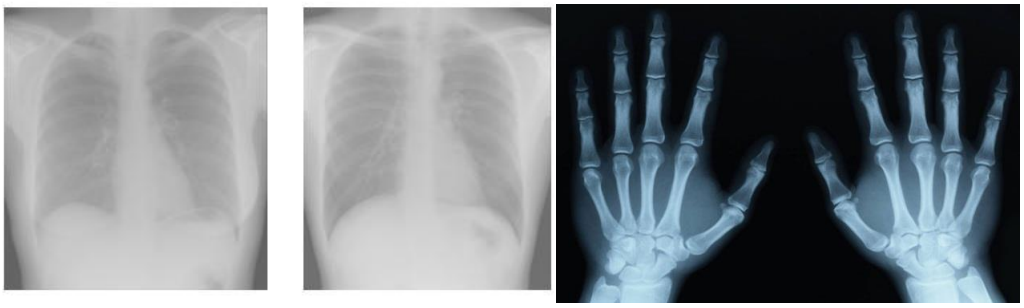
(a) **(b)** **(c)**

Fig.1.8. Biométrie du cerveau avec des images IRM : (a) Extraction des textures de cerveau par segmentation (b) reconstruction de 3D d'image de cerveau montrant les circonvolutions qui peuvent être employées pour identifier des individus (c) extraction du Brain Code [37]

L'avantage principal de ce type de modalité cachée est le fait que le cerveau est totalement protégé contre toutes sortes de changements. Cependant, l'inconvénient principal de cette modalité est la non-disponibilité de systèmes d'IRM robuste consacrés à la biométrie.

1.10.2. Biométrie avec des images de rayon X

La biométrie cachée a été aussi prolongée vers l'utilisation des images de rayons X. Elle permet d'obtenir un cliché dont le contraste dépend à la fois de l'épaisseur et du coefficient d'atténuation des structures traversées. Nous présentons, dans ***les figures 1.9 (a et b)***, deux images X-ray de poumons qui correspondent à deux individus différents. Les différences en termes de textures et en morphologies peuvent être remarquées facilement. Dans ce cas, l'extraction des caractéristiques par l'utilisation de quelques techniques appropriées de traitement d'images peut être facilement employée pour différencier entre les individus [33].



(a) (b) (c)

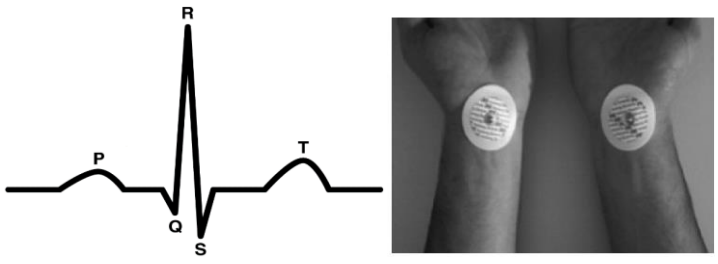
Fig.1.9. Biométrie cachée appliquée sur les images X-ray. (a) et (b) deux images X-ray des poumons de deux individus différents. (c) Biométrie de la main avec des images à rayon X.

Une autre application potentielle de la biométrie cachée qui utilise les images X-ray de la main est présentée dans ***la figure 1.9 (c)***. Cette méthode est plus efficace et robuste par rapport à la biométrie classique qui utilise les empreintes palmaires. Dans ce type d'application, les paramètres géométriques peuvent être facilement extraits et modélisés. Pour chaque individu.

1.10.3. Electrocardiogramme ECG

L'ECG est un signal représentant l'activité du cœur. Il est principalement employé dans des applications cliniques pour diagnostiquer les maladies cardio-vasculaires. Le signal d'ECG est caractérisé par la forme de ses battements composés de cinq vagues typiques, à savoir P, Q, R, S, et T ou parfois la vague U ***(figure 1.10(a et b)***.

La biométrie par ECG a fait l'objet d'un certain nombre de travaux [33], [38] et [39]. L'utilisation de l'ECG en biométrie est relativement nouvelle. En fait, il existe plusieurs méthodes biométriques basées sur l'ECG. Il y a des approches qui sont basées sur l'analyse de l'ECG [40]. D'autres basées sur l'intégration des caractéristiques analytiques et d'apparence extraite des signaux ECG [36], [41].



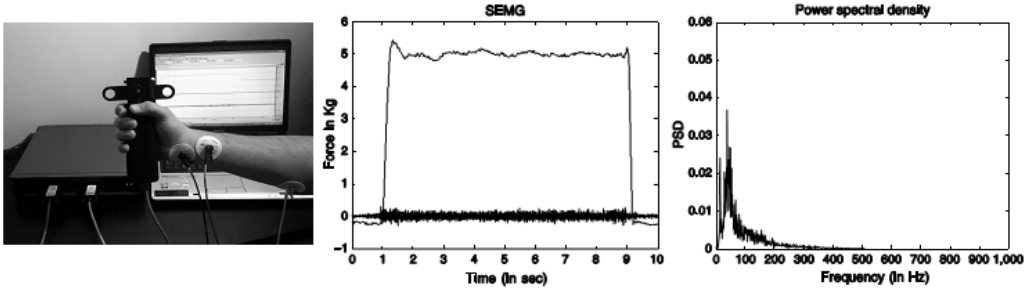
(a) (b)

Fig.1.10. Biométrie par ECG : (a) Signal d'ECG avec le rythme régulier (b) positionnement des électrodes sur les avant-bras pour la capture d'ECG [40]

1.10.4. Electromyogrammes EMG

Les signaux électromyogrammes (EMG) sont des signaux bioélectriques enregistrés fournissent des informations diverses sur l'état des nerfs et des muscles, dans ce contexte, quelques expériences récentes ont été réalisées [33], [41] et [42].

Lors de l'acquisition de ces signaux, les individus sont invités à appliquer une pression manuelle d'une intensité constante sur une sonde de force pendant plusieurs secondes (***Figure 1.11***). Le signal ainsi obtenu est analysé dans le domaine spectral. Puis, des paramètres sont extraits comme la puissance du signal, la fréquence moyenne, le coefficient d'aplatissement et le coefficient de dissymétrie. En effet, ces paramètres fournissent un vecteur de dispositif que nous pouvons employer pour caractériser des individus.



(a) (b) (c)

Fig.1.11. Biométrie par l'EMG : (a) Acquisition d'un signal EMG (b) L'intensité appliquée par l'utilisateur et l'EMG relatif (c) périodogramme d'EMG [10]

1.11. Applications de la biométrie

La nécessité des techniques d'authentification fiables est augmentée suite aux préoccupations croissantes qui concernent la sécurité et les progrès rapides en communication, réseau et mobilité. Ainsi, la biométrie est de plus en plus intégrée dans diverses applications ou bien pouvant être classées en trois groupes principaux qui sont:

a. Applications commerciales : telles que l'accès à un réseau d'ordinateurs, la sécurité des données électroniques, le e-commerce, l'accès d'internet, l'utilisation des cartes de crédit bancaire, le contrôle d'accès physique, mobile phone, la gestion des registres médicaux ou l'apprentissage à distance, etc.

b. applications gouvernementales : telles que les cartes d'identité (ID cards), la sécurité sociale, le contrôle des frontières, le contrôle des passeports, le déboursement en assistance sociale ou en permis de conduite, etc.

c. Applications légales : telles que l'identification des corps humains, les enquêtes criminalistiques ou la détermination parentèle, etc.

1.12. Conclusion

A travers ce premier chapitre, nous avons présenté un état de l'art sur la biométrie, ses propriétés, le principe de fonctionnement des systèmes biométriques, les différentes modalités ainsi que les critères d'évaluation des performances de ce type de systèmes. Ensuite, nous avons mis en évidence une comparaison entre ces modalités biométriques, tout en accordant une attention particulière à la reconnaissance par signature, puisqu'elles constituent un bon choix, en termes de praticabilité, robustesse, acceptabilité. Finalement, nous avons terminé le chapitre par une brève présentation de la biométrie cachée comme nouvel axe de recherche en criminalistique et en sécurité biométrique, qui constitue un défi très important que nous voulons exploiter dans un futur travail, par l'application et le développement des descripteurs de texture locaux proposés.

Chapitre 2

Reconnaissance par signature

2.1. Introduction

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu. Elle est aujourd'hui, et le demeurera sans doute dans le futur, le moyen biométrique d'authentification le plus utilisé et accepté.

La signature manuscrite d'un individu représente un bon compromis : tout en étant relativement fiable, elle est facile à acquérir, socialement acceptée comme un mode de reconnaissance. La signature est un moyen utilisé depuis longtemps, l'ancêtre étant le sceau, pour authentifier des documents, pour responsabiliser les individus face à des engagements (contrats, etc.). La signature est donc reconnue comme mode de validation associé à l'identité d'une personne.

La signature en ligne ou hors ligne peut être considérée comme une méthode biométrique comportementale. La principale difficulté concernant l'authentification est que la signature en entrée et la signature servant de référence ne sont pas exactement les mêmes. Pour que cette reconnaissance soit exacte, il faut que la variation existant entre les signatures d'une même personne soit inférieure à la distance entre les signatures de deux personnes différentes. Il faut donc essayer d'isoler les parties ou caractéristiques de la signature qui sont pratiquement constantes, de celles qui ne le sont pas.

Outre la variabilité habituelle, différentes raisons peuvent expliquer la variation de la signature :

- le support est le stylet utilisé
- l'importance du document sur lequel on appose la signature
- le lieu et les conditions d'écriture

Les fonctions assurées par la signature manuscrite sur papier sont l'identification, l'adhésion au contenu, la garantie de l'intégrité, la constitution d'un original.

Un système d'authentification biométrique basé sur la signature manuscrite doit assurer les mêmes fonctions :

- ✓ *Fonction d'identification* : Le système d'authentification doit être suffisamment fiable pour être reconnu comme moyen de non répudiation.
- ✓ *Fonction d'adhésion au contenu* : Culturellement le fait d'apposer sa signature manuscrite signifie que l'on adhère au contenu indépendamment du support.
- ✓ *Fonction de garantie de l'intégrité* : La garantie de l'intégrité du document peut être assurée par une fonction de hachage.
- ✓ *Fonction de constitution d'un original* : La signature manuscrite sur papier ou sur interface graphique reste toujours unique : on ne refait jamais exactement la même signature.

- ✓ *Fonction psychologique* : Le fait d'utiliser la signature manuscrite en amont de la signature électronique offre l'avantage de capter l'attention de l'individu sur l'importance de l'acte contrairement aux méthodes actuelles où l'on entre un code PIN.

2.2. Etat de l'art

La signature manuscrite est l'un des premier modalités qui à être utilisé avant même l'apparition des ordinateurs. La signature manuscrite a longtemps été utilisée dans le domaine financier pour la vérification de l'identité. Beaucoup des travaux a été fait dans le domaine de l'identification et la vérification de signature manuscrite.

En ce qui concerne l'identification des signatures, nous pouvons parler de l'identification des signatures manuscrites hors ligne et en ligne. Le premier ne nécessite qu'une image de signature qui doit être analysée d'une manière ou d'une autre. La personne n'a pas besoin d'être physiquement présente au moment de l'identification. De l'autre côté, l'identification de signature manuscrite en ligne nécessite la présence physique de la personne. Cela se fait généralement avec une tablette à numériser ou un stylo spécialisé qui envoie des «données en direct» au système biométrique.

Vargas et al. (2011) ont utilisé LBP avec 8 et 16 voisinages accompagnant des matrices de cooccurrence de niveau de gris (GLCM). Ils ont utilisé une technique efficace pour supprimer l'arrière-plan des signatures et une méthode de déplacement de l'histogramme pour réduire l'influence de différentes encres d'écriture, Ils ont présenté les résultats sur la base de données MCYT et GPDS-100.

Les EER de 12,06% et 9,02% ont été obtenus avec un classificateur LS-SVM (Suykens et al. 2002) pour 5 et 10 images respectivement dans la phase d'apprentissage.

Bharadi et Kekre (2010) ont utilisé la transformation de Walsh pour la distribution horizontale et verticale des pixels. Ils ont atteint un taux de fausses acceptations (FAR) de 2,5%, un taux d'erreur égal (EER) de 3,29% et un taux de reconnaissance de 95,08%.

La méthode de SVM est utilisée pour vérifier et classifier les signatures de différentes personnes avec un taux de classification de 95%. Trois types de caractéristiques sont utilisés pour décrire les signatures: les fonctions globales, directionnelles et de grille, avec 77 caractéristiques. Dubey et Agrawal, (2012).

Ferrer et Vargas (2012) ont mesuré la stabilité des caractéristiques du niveau de gris par rapport à la modification de la distribution des niveaux de gris des traits de signature. Ils ont mélangé un ensemble de vérifications et de factures différentes en modifiant la complexité de l'arrière-plan avec les bases de données de signatures MCYT et GPDS. Le modèle utilisé pour la fusion est basé sur la multiplication de l'image de contrôle par celle de la signature. En plus de l'utilisation de la matrice de

cooccurrence et de la LBP comme caractéristiques de texture statistique, ils ont utilisé d'autres méthodes telles que le modèle directionnel local (LDP) (Jabid et al., 2012) et le modèle dérivé local (LDeriveP) (Zhang et al., 2010) pour extraire des caractéristiques plus invariantes. Ils ont rapporté l'EER de 23,03%, 21,52% et 15,35% sur les simulations de faux de 300 utilisateurs de la base de données GPDS pour LBP, LDP, et LDeriveP, respectivement (Abdoli et Hajati, 2014).

Jabid et al. (2012) sont arrivés à la conclusion que le LDP est meilleur que la méthode LBP dans la vérification de signature. Dans Ferrer et al. (2010), LDP a été appliqué aux signatures binaires. L'EER de 19,99% et de 17,80% pour les simulations de faux sous 300 utilisateurs de la base de données GPDS (Vargas et al. 2007) a été réalisé pour des ensembles d'apprentissage de 5 et 10 échantillons, respectivement.

Ferrer et al. (2005) ont proposé des caractéristiques géométriques basées sur la description de l'enveloppe de signature et de la distribution des traits intérieurs dans les coordonnées cartésiennes et polaires. Les caractéristiques proposées sont calculées avec un microprocesseur à point fixe. Le faux taux de rejet (FRR) de 16,21% et le FAR de 15,66% ont été obtenus sur de simples falsifications avec un classificateur basé sur la distance euclidienne pour 12 échantillons (Abdoli et Hajati, 2014).

Karouni et al. (2011) ont utilisé les cinq caractéristiques géométriques globales (aire, centre de gravité, excentricité, aplatissement et asymétrie) en fonction de la forme et des dimensions d'une image de signature.

Sigari et Pourshahabi, ont proposé une méthode d'identification de signature basée sur la transformée d'ondes de Gabor (GWT) en tant qu'extracteur de caractéristiques et avec SVM en tant que classifieur. Dans leur étude après la normalisation de la taille et l'élimination du bruit, une grille virtuelle est placée sur l'image de la signature et les coefficients de Gabor sont calculés sur chaque point de la grille. Ensuite, tous les coefficients de Gabor sont introduits dans une couche de classificateurs SVM en tant que vecteur de caractéristiques. Le nombre de classificateurs SVM est égal au nombre de classes. Chaque classificateur SVM détermine si l'image d'entrée appartient à la classe correspondante ou non (une par rapport à la méthode). Dans leur étude, deux expériences sur deux ensembles de signatures ont été effectuées. Ils ont atteint un taux d'identification de 96% sur l'ensemble des signatures persanes et de plus de 93% sur l'ensemble des signatures turques.

Un grand nombre de méthodes ont été utilisées pour extraire des informations pertinentes sur les signatures. Les premières techniques ont été basées sur des caractéristiques statistiques comme des moments géométriques ainsi que des transformations globales d'image telles que la transformée en ondelettes, la transformée de Radon, la transformée Ridgelet, la transformée de Curvelet (Deng, Mark Liao, Ho, & Tyan, 1999; Rajae, & Pourreza, 2010, Radhika, Venkatesha et Sekhar, 2011, Hamadene, Chibani et Nemmour, 2012, Nemmour et Chibani, 2013 'b')

2.3. Enrôlement, vérification et identification.

Les systèmes biométriques fonctionnent selon trois modes que sont l'enrôlement, la vérification d'identité et l'identification :

- ✓ ***Enrôlement :***

L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'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 défini, 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 stocké soit dans une base de données centrale soit sur un élément personnel propre à chaque personne.

- ✓ ***Vérification :***

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

- ✓ ***Identification :***

En mode identification, le système biométrique détermine l'identité d'un individu inconnu à partir d'une base de données d'identités, on parle de test 1 : N. Dans ce cas, le système peut alors soit attribuer à l'individu inconnu l'identité correspondant au profil le plus proche retrouvé dans la base (ou une liste des profils proches), soit rejeter l'individu.

L'identification est un problème de recherche du plus proche voisin parmi un ensemble de possibilités alors que la vérification est un problème de discrimination à deux classes, acceptation ou rejet. Par conséquent, les approches utilisées ne sont pas les mêmes pour ces deux problèmes. Alors que tous les modèles sont disponibles pour un problème d'identification, la difficulté de la vérification est accrue car on ne dispose que du modèle d'une personne à chaque fois pour prendre la bonne décision. A aucun moment du processus nous n'avons la possibilité de stocker et de comparer les données biométriques des différentes personnes impliquées. On ne peut donc pas effectuer de classification supervisée, en associant une classe à chaque individu, afin de rechercher et d'adapter des critères qui séparent au maximum les classes, qui augmentent la variance interclasses. Par conséquent, il est plus difficile de connaître les caractéristiques représentatives et discriminantes des données biométriques et qui permettraient une vérification facile de la personne. Dans le cadre de l'identification, il faut maximiser la distance inter personnes alors qu'en vérification il faut minimiser la distance intra personne.

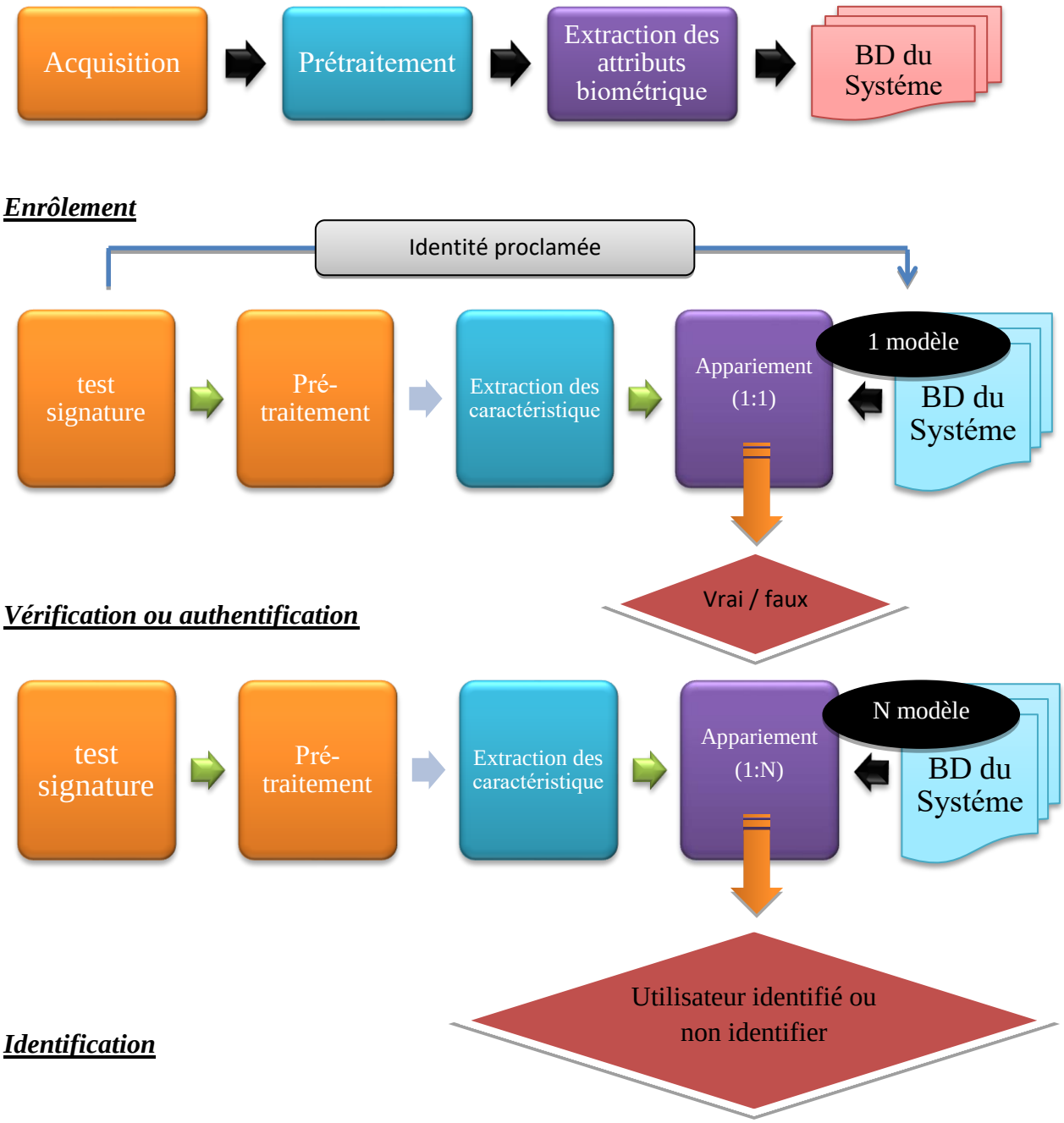


Fig. 2.1 schéma de fonctionnement d'un système biométrique. Diagrammes des processus d'enroulement, de vérification et d'identification.

Les schémas d'un système de vérification et d'un système d'identification sont illustrés dans ***la figure 2.1***; le processus d'enrôlement, qui est commun à ces deux tâches est également illustré. Le module d'enrôlement correspond à l'enregistrement biométrique des individus dans la base de données du système. Pendant la phase d'enrôlement, la caractéristique biométrique d'un individu est capturée par un lecteur biométrique. Un contrôle de qualité est généralement effectué pour s'assurer que la prise de l'échantillon est effectuée de manière fiable et pour garantir une bonne qualité de l'acquisition [43]. Afin de faciliter l'appariement, la représentation numérique

extraite par le capteur est généralement traitée par une fonction d'extraction pour générer une signature compacte et expressive, appelé aussi modèle. Selon l'application, le modèle peut être stocké dans la base de données centrale du système biométrique ou être enregistré sur une carte magnétique ou carte à puce délivrée à la personne.

2.4. Processus de vérification de signature hors ligne

Comme dans tout système de reconnaissance biométrique, la reconnaissance de signature manuscrite hors ligne passe principalement par quatre étapes : les prétraitements, l'extraction des caractéristiques, classification et l'appariement de caractéristiques. Dans ce qui suit nous détaillons chacune de ces étapes qu'on a appliquées aux bases de données MCYT et GPDS.

2.4.1. Prétraitements

La plus part des systèmes de reconnaissance comportent une étape de prétraitement après que l'acquisition est faite, son but est améliorer les résultats et les performances du module de reconnaissance. Généralement, ces prétraitements ne sont que des opérations classiques en traitement d'image, dans notre système en a passé par les opérations suivantes :

- **Réduction de bruit** : cette étape vise à nettoyer l'image de l'entrée, éliminer les points redondants car ces points-là vont causer les confusions pour le classificateur. Le bruit est une valeur découlant habillement de la reproduction de la numérisation et de la transmission de l'image originale. Le bruit ne peut pas toujours entièrement supprimé. On a utilisé *le filtre médian* comme technique pour réduire le bruit.
- **Normalisation** : les tailles des images de caractères sont variées. Ce phénomène peut perturber le système de reconnaissance des formes. On a besoin de normaliser les images obtenues l'hors de la lecture des base MCYT et GPDS on a choisi de normaliser tous les images a une taille de 255. Le classificateur va effectuer plus efficacement sur les images homogènes.
- **Squelettisation** : dans la plus part des cas, la forme à reconnaitre ne dépend pas géométriquement de l'épaisseur du tracé de l'objet, la squelettisation est une procédure qui a pour but de réduire l'épaisseur du tracé d'un caractère à un pixel seulement. L'amincissement jusqu'à ce que l'épaisseur reste un seul point peut constituer une procédure très utile.

2.4.2. Extraction des caractéristiques :

Cette étape représente le cœur du système de reconnaissance, on extrait de l'image les informations qui seront sauvegardées en mémoire pour être utilisées plus tard dans la phase de décision. Le choix de ces informations utiles revient à établir un modèle pour la signature, elles doivent être discriminantes et non redondantes.

L'analyse est appelée indexation, représentation, modélisation ou extraction de caractéristiques. L'efficacité de cette étape a une influence directe sur la performance du système de reconnaissance de signature.

2.4.3. Classification et décision

La classification est l'élaboration d'une réglé de décision qui transforme les attributs caractérisant les formes en appartenance à une classe (passage de l'espace de codage vers l'espace de décision). Comme tout système biométrique, avant qu'un modèle de décision ne soit intégré dans un système de reconnaissance de signature, il faut avoir procédé auparavant à deux étapes : *l'étape d'apprentissage et l'étape de test.*

- **Phase d'apprentissage :**
  L'étape d'apprentissage consiste à caractériser les classes de formes de maniéré à bien distinguer les familles homogènes de formes. Il existe deux types d'apprentissage supervisé et non supervisé.
  - ✓ ***L'apprentissage est dit supervisé*** si les différentes familles des formes sont connues a priori et la tâche d'apprentissage est guidée par un superviseur ou professeur, c'est-à-dire le concepteur indique pour chaque échantillon rentré, le nom de famille qui la contient.
  - ✓ ***L'apprentissage non supervisé,*** on l'appelle aussi apprentissage sans professeur, à partir d'échantillons de référence et de règles de regroupement ou de modélisation, de construire automatiquement les classes ou les modèles sans intervention de l'opérateur.
- **Phase de test :**

Le test est l'ultime étape de reconnaissance. Permet d'évaluer les performances du classificateur pour un apprentissage donné. Elle consiste à modéliser les paramètres extraits d'une signature ou d'un ensemble de signatures d'un individu en se basant sur leurs caractéristiques communes. Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités, ces derniers seront regroupés dans la même classe, et ces classes varient selon le type de décision. Selon les caractéristiques extraites précédemment, les algorithmes de comparaison diffèrent. On trouve dans la littérature plusieurs approches dont la plus simple est le calcul de distance (recherche de similarité). D'autres méthodes se basent sur la classification des caractéristiques par un seul classifieur (SVM, classifieur bayésien, réseau de neurones …etc.).

L'apprentissage consiste donc à mémoriser les représentations calculées dans la phase analyse pour les individus connus. Généralement les deux étapes d'analyse et d'apprentissage sont confondues et regroupées en une seule étape.

- **La décision** : C'est l'étape qui fait la différence entre un système d'identification d'individus et un système de vérification. Dans cette étape, un système d'identification consiste à trouver le modèle qui correspond le mieux à la signature prise en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. Par contre, dans un système de vérification il s'agit de décider si la signature en entrée est bien celui de l'individu (modèle) proclamé ou il s'agit d'un imposteur. Pour estimer la différence entre deux images, il faut introduire une mesure de similarité.

On définit ainsi plusieurs facteurs de performances du système tels que :

- **Le taux de reconnaissance :** qui présente le pourcentage des caractères reconnus parmi les caractères présentées.
- **Taux d'erreurs :** qui représente le pourcentage des caractères acceptés par le système mais classés de façon incorrecte.
- **Le taux de rejet :** qui représente le pourcentage des caractères rejetés parmi les caractères présentés.
- **Le taux d'ambiguïté :** qui représente le pourcentage des caractères ambigus parmi les caractères présentés.

2.5. Avantages de l'utilisation de la signature manuscrite

En dépit des difficultés que nous venons de relever, les avantages de l'utilisation de la signature manuscrite comme un moyen d'authentification forte sont nombreux.

Concernant la pertinence de son utilisation, en apposant sa signature manuscrite, chaque signataire exprime – dans le sens propre du terme – l'empreinte de sa personnalité. Les juristes sont unanimes sur le fait que la signature électronique (i.e. le mot de passe) ne peut remplacer entièrement la signature manuscrite. L'authentification certaine des utilisateurs de signatures électroniques ne peut être garantie qu'en y associant des caractéristiques biométriques. En effet, les cartes à puce, les codes confidentiels ainsi que les mots de passe ne représentent pas des références purement individuelles et en conséquence peuvent être sujets de manipulations ou de vols. De plus, contrairement aux mots de passe ou aux codes confidentiels, on n'oublie jamais sa signature. Par rapport aux autres technologies basées sur la biométrie physiologique, son utilisation ne nécessite pas généralement un coût supplémentaire élevé pour le capteur.

Concernant la fiabilité, chaque signature est unique, car elle reflète les propres habitudes, de nature autant physiologique que biomécanique, ainsi que le rodage individuel quotidien. Deux signatures ne peuvent jamais être exactement identiques sauf s'il s'agit d'une copie. Mais cela est automatiquement détectable.

Apposer sa signature sur un document est un acte bien accepté. En général, la signature a déjà fait l'objet de stockage au niveau, non seulement d'institutions financières, mais également au sein de diverses autres institutions.

De plus, à ce jour, un des signes les plus fréquemment acceptés pour permettre le non répudiation ou la preuve d'engagement de l'individu est sa signature manuscrite. Son utilisation pour l'authentification est autant habituelle qu'acceptée, aussi bien pour les clients que pour les prestataires. A contrario, les autres procédés, notamment la prise d'empreintes digitales et la forme et l'aspect de l'iris, sont jugés trop invasifs pour un usage grand public. En effet, les systèmes basés sur l'empreinte digitale ont une connotation d'investigation criminelle et ceux basés sur l'iris nécessitent un contact très proche de l'œil avec le système d'acquisition. Le dernier avantage que l'on peut citer est que l'authentification par signature manuscrite est très facile à expliquer par rapport aux autres techniques d'authentification biométrique.

Toutes les raisons citées ci-dessus expliquent pourquoi la signature manuscrite a été retenue pour cette étude. Suivant la méthode de capture de la signature, on distingue deux familles de signatures : *hors ligne et en ligne*. Le paragraphe suivant décrit les différences existant entre les deux familles.

2.6. Différences entre hors ligne et en ligne

Un système automatisé de vérification et d'authentification contournerait, a Priori, toutes ces difficultés. La vérification des signatures serait idéalement rapide, systématique et efficace, et réduirait de manière significative les risques de contrefaçon. Plusieurs systèmes ont été développés à ce jour afin d'automatiser la vérification des signatures et on peut diviser ces méthodes en deux classes suivant le mode d'acquisition de l'image des signatures:

Les systèmes «On-Line» : Dans le cas d'un système en ligne, la signature est effectuée sur une tablette graphique ou tout autre support muni d'un stylet électronique reliée à un ordinateur. La signature est donc représentée par une suite de points définis par au moins 3 valeurs : x, y, t.

Cette méthode permet d'utiliser des informations dynamiques telles que la vitesse, la pression et/ou l'inclinaison du stylo. Ces systèmes sont surtout utilisés pour contrôler l'accès à des zones protégées ou pour vérifier l'identité lors d'une transaction en-ligne (à condition d'avoir les périphériques d'entrée appropriés). Ces systèmes ne peuvent pas être utilisés pour vérifier des signatures déjà apposées sur des documents (chèques bancaires par exemple).

Les systèmes «Off-Line»: la signature est numérisée à partir d'un support physique tel un chèque ou tout autre document sur un scanner. La signature est donc assimilée à une image en niveaux de gris. C'est le cas notamment pour les systèmes de vérification de chèques. En hors ligne, on ne dispose pas de la dynamique de façon directe mais d'autres informations sont disponibles comme l'épaisseur du trait ou la variation d'intensité du niveau de gris constituant la signature. Cependant, ces systèmes permettent de vérifier les signatures à un temps différé. Mais la perte des informations dynamiques rend le processus de vérification plus difficile. [44][45][46].

Les problèmes liés à l'acquisition sont différents dans le cadre du en ligne et dans celui du hors ligne. En effet, en hors ligne, le papier utilisé pour signer peut être de différentes textures, le stylo a aussi une grande influence et enfin l'acquisition via le scanner peut donner des résultats différents suivant la résolution choisie. C'est aussi le cas pour les systèmes d'acquisition en ligne pour lesquels la résolution ou la fréquence d'acquisition ne sont pas fixées.

Dans le cadre de ce mémoire, nous aborderons le problème de la reconnaissance des signatures manuscrites à partir d'une saisie « Off-Line». On a travaillé sur les bases de données MCYT-75, GPDS-100 et GPDS-160.

2.7. Fausses signatures

Lorsqu'on évalue un système d'authentification par signature manuscrite, on doit prendre en compte trois types de faux : les faux aléatoires, les faux simples et les faux expérimentés [47]. Les faux aléatoires sont réalisés par une personne ne connaissant pas la forme de la signature à imiter. Les faux simples sont des signatures pour lesquelles le libellé est identique mais la graphie différente. Les faux expérimentés sont réalisés par des personnes ayant accès à la fois à la forme et à la dynamique, voire à des informations sur la méthode d'authentification.

Le faux aléatoire est obtenu en employant sa propre signature à la place de celle à imiter. A l'opposé du faux simple, le libellé d'un faux aléatoire est évidemment différent du libellé de l'authentique. Sa détection est donc a priori assez facile.
Le faux simple est rédigé sans tentative de copier la forme de la signature mais en connaissant le libellé c'est à dire le nom. C'est le faux le plus fréquemment rencontré en pratique. On peut identifier le scripteur du faux simple car ce dernier présente souvent un bon nombre de caractéristiques intrinsèques propres à son auteur.

Le faux par calque est obtenu en reproduisant fidèlement une signature authentique à l'aide d'un moyen quelconque de transfert de l'image de l'authentique sur un document. Il a toutes les caractéristiques d'un dessin. Cette technique est généralement bien adaptée aux systèmes d'authentification hors ligne. Le faux par calque manque de spontanéité, donne l'apparence de mouvements lents et d'une pression uniforme et les retouches sont souvent détectables.

On distingue deux types de faux par imitation, le faux par imitation servile et le faux par imitation libre. Lors d'une imitation servile d'une signature, le faussaire copie directement le modèle et s'y réfère aussi souvent que nécessaire. L'imitation servile de la signature authentique présente un dessin assez ressemblant à l'authentique. Parmi les divergences entre différents échantillons de ce type, on trouve les espacements, les alignements et l'inclinaison relative des lettres. On remarque également la présence d'une mauvaise inclinaison moyenne de l'écriture, un tracé lent et hésitant et la présence fréquente de retouches ou reprises.

Dans le cas d'une imitation libre, le faussaire procède par l'étude soignée de la signature authentique. Il mémorise l'image générale de la signature et le dessin des lettres, leurs espacements et autres détails picturaux. Le faussaire s'entraîne pour imiter la signature authentique, il compare le faux et l'authentique entre les essais et

répète la même procédure jusqu'à entière satisfaction. A la différence du faux par imitation servile, celui-ci est caractérisé par une allure spontanée. Les principales divergences de ce faux par rapport à l'authentique résident dans les proportions relatives des lettres, des espacements, les types des alignements et notamment un manque d'alternance des pleins et des déliés.

2.8. Variabilité des signatures manuscrites

2.8.1. Variation intra individu

Les signatures successives d'un même individu varient globalement et localement et diffèrent en orientation et en échelle. En effet, suivant le contexte, les signatures sont de longueurs et de durées différentes même si elles sont faites par un même scripteur et des variations aléatoires existent comme des ajouts ou retraits de traits. Par conséquent, comme nous l'avons déjà indiqué, si deux signatures de la même personne sont parfaitement identiques alors l'une d'entre elles peut être considérée comme un faux.

La plupart des articles traitant de l'authentification par signature manuscrite font état de personnes pour lesquelles le système d'authentification ne fonctionne pas. En effet, certaines personnes ont une signature trop instable pour pouvoir établir un modèle représentatif de leur signature. Cela peut être dû à l'utilisation d'un nouveau support nécessitant une période d'adaptation. Il est notamment perturbant d'écrire avec un stylet sur une surface particulière ou encore d'écrire dans une zone restreinte. Dans [48], l'auteur montre qu'il existe une forte corrélation positive entre une grande instabilité de la signature et une grande variance du temps total mis pour réaliser la signature. La durée totale de la signature peut donc être utilisée pour mesurer la variabilité intra individu d'une signature.

2.8.2. Variation inter individus

Les signatures sont très variées même pour des personnes d'un même pays. En effet, au-delà des habitudes culturelles, certaines personnes ont des signatures très complexes alors que d'autres écrivent uniquement leur nom. Cependant, on peut distinguer deux grandes catégories de signatures : les signatures occidentales et les signatures asiatiques. Les signatures occidentales peuvent elles-mêmes être classées en deux sous catégories : les paraphes très éloignés de la forme du nom telles les signatures européennes et les signatures très proches du nom telles certaines signatures anglo-saxonnes. Les signatures asiatiques sont très différentes des signatures occidentales; elles sont constituées de traits très courts séparés par des levés de stylet et orientés suivant un axe vertical. Par conséquent, les systèmes d'authentification par signatures manuscrites basés directement sur le style des signatures anglo-saxonnes ou asiatiques ne seront pas aussi performants dans le cas de signatures européennes.

2.9. Conclusion

Dans ce chapitre, nous avons présenté dans un premier temps les modes de fonctionnement d'un système biométrique avec leurs diagrammes des processus. Ensuite, on a discuté les différents avantages de l'utilisation de signature manuscrite comme une modalité biométrique et la différence entre la reconnaissance de signature en ligne et hors ligne, par la suite, on a cité les fausses signatures et leur influence sur le taux de reconnaissance.

Chapitre 3

Extraction des caractéristiques

3.1. Introduction

L'étape d'extraction des paramètres réduit les dimensions des images de signatures originales tout en préservant et en extrayant les informations importantes codées dans l'image. Un ensemble soigneusement sélectionné de caractéristiques transformera les images afin qu'il devienne plus facile de distinguer entre les classes authentiques et falsifiées, nous présentons dans ce chapitre les techniques que nous avons utilisées dans le but d'extraire des informations biométriques texturées.

L'analyse de texture réfère à la discipline de l'analyse d'images qui s'intéresse à la description des caractéristiques de l'image par des attributs texturaux. Cependant, il n'existe pas une définition universellement acceptée de ce qui est une texture de l'image, en général, plusieurs chercheurs utilisent des définitions différentes selon leurs domaines d'intérêt [49]. Dans ce chapitre, la texture est considérée comme la variation spatiale d'intensités de pixels, ce qui est une définition largement utilisée et acceptée dans le domaine d'imagerie. L'objectif de ce chapitre est de présenter une revue bibliographique des méthodes d'analyse de texture existantes, avec un intérêt pour les techniques utilisées en biométrie.

Nous nous sommes intéressés dans cette étude par les descripteurs de texture locaux inspirés principalement par ***LBP*** (la technique des motifs binaires locaux) et ***BSIF*** (Caractéristiques statistiques et binarisées de l'image).

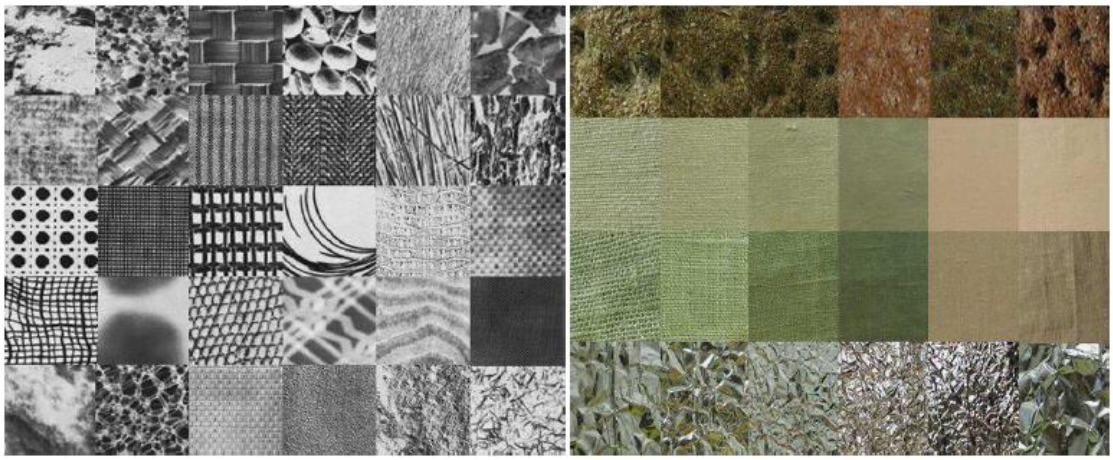
3.2. Notions fondamentales sur l'analyse de texture

L'analyse de texture est un domaine actif de recherches intenses et de vaste littérature. Néanmoins, il existe deux sujets fondamentaux qui ne sont pas résolus jusqu'à présent: (i) la définition de la notion de texture; et (ii) la création d'une taxonomie significative et sans ambiguïtés des descripteurs de texture existants. Le manque de solutions satisfaisantes à ces deux sujets clés est un point de faiblesse sérieux qui limite le progrès de la discipline. Nous croyons fortement que des avancées significatives dans le domaine peuvent être réalisées. Dans les paragraphes qui suivent, nous discutons des deux sujets en détails.

3.2.1. Définition de la texture

La texture est un terme largement utilisé dans la vision par ordinateurs, et c'est plutôt surprenant qu'un tel concept omniprésent n'a pas trouvé un consensus général. Ahonen et al. (2009) [50] ont correctement noté que c'est peut-être une des raisons pour lesquelles ni une théorie unificatrice, ni un cadre de descripteurs de texture ont été proposés jusqu'à présent.

La racine du mot latin (texere= à tisser) suggère que la texture est un peu liée à l'interaction, la combinaison, et l'imbrication d'éléments dans un ensemble complexe **(figure 3.1. ex. (a), (b)**). Le concept de texture comme la propriété visuelle d'une surface, cependant, est assez subjectif et imprécis. Nous pouvons reconnaître la texture quand nous la voyons, mais la définition d'une manière formelle est beaucoup plus difficile. Certainement il y a quelques attributs de texture qui sont largement convenus: cette texture est la propriété d'une zone (et pas d'un point), elle est liée à la variation de l'apparence, elle dépend fortement de l'échelle d'une image, et elle est perçu comme la combinaison de certains modèles basiques. Par exemple, Davies (2008) [51] affirme que la plupart des gens considèrent la texture comme « un motif aléatoire et régulier en même temps ». Petrou et Sevilla (2006) [52] considèrent la texture comme « une variation de données à des échelles plus petites que l'échelle d'intérêt ». En fait, beaucoup de définitions sont proposées dans la littérature: le lecteur peut trouver un petit recueil dans la référence [49] ; malheureusement, aucune de ces définitions n'a suscité un consensus général, principalement parce qu'il n'y a pas de modèle mathématique formel sur lequel nous pouvons en déduire une définition générale quantitative.



(a) **(b)**

Fig. 3. 1 : Exemples de textures: (a) base d'images Brodatz (b) base d'images KTH-TIPS2.

Considération: Dans le cadre de cette thèse, nous avons considéré la texture comme la variation spatiale d'intensités de pixels; c'est une définition largement utilisée et acceptée spécialement dans le domaine de l'imagerie.

3.2.2. Catégorisation des descripteurs de texture

Le deuxième sujet critique qui est, en fait, une conséquence directe du premier, concerne le développement d'une taxonomie pour les descripteurs de texture. Plusieurs tentatives pour classifier les descripteurs de texture sont faites jusqu'à présent.

A notre connaissance, la première tentative date vers la fin des années 1970, elle a été proposée par Haralick (1979) [53]. Ce dernier a divisé les descripteurs de texture

en statistiques et structurels, mais il a rapidement reconnu qu'il est très difficile de tracer une frontière nette entre les deux classes [54,55]. Cette division a été inspirée par le travail pionnier de Julesz (1975) [56], qui a conjecturé que la discrimination de texture dans le système visuel humain existe sous deux formes: perspective et cognitive. La première fournit une caractérisation immédiate de la texture qui est essentiellement statistique, tandis que la dernière nécessite un examen qui est généralement structurel.

Wu et Chen (1992) [57] ont affiné cette taxonomie de deux classes en divisant la classe des méthodes statistiques en cinq sous-classes: méthodes spatiales dépendante au niveau de gris, caractéristiques spatiales basées sur les fréquences, caractéristiques basées sur des modèles stochastiques, méthodes de filtrage, et approches heuristiques. Puis, vers la fin des années 1990, Tuceryan et Jain (1998) [49] ont proposé une classification à quatre catégories (statistiques, géométriques, basées sur le modèle, et de traitement du signal) qui a fortement influencé la littérature. Pourtant, la classification n'a pas été exempte de critiques, certains descripteurs de texture possèdent des « traits » très distinctifs qui appartiennent à plus d'une classe, et donc en général une séparation complètement croquante ne se tient pas. Récemment, Xie et Mirmehdi (2008) [58] ont suggéré que les quatre classes proposées par Tuceryan et Jain doivent être plutôt considérées comme des attributs qu'une méthode spécifique peut les posséder ou non. Une telle catégorisation représente, à notre avis, la meilleure tentative pour classifier les descripteurs de texture. Pourtant, toute classification fondée sur des catégories "sémantiques" ne sera jamais satisfaisante, en raison de sa nature intuitive et informelle. Au contraire, l'approche correcte doit être basée sur des définitions "mathématiques formelles".

Les difficultés mentionnées ci-dessus sont soulevées clairement quand il s'agit de trouver le bon placement pour la méthode LBP et ses variantes relatives. Bien que le LBP ait été proposé comme « une approche d'unification pour les modèles statistiques et structurels traditionnellement divergents dans l'analyse de texture » [59], il n'existe actuellement aucun consensus sur ce point, en raison de l'absence d'une taxonomie universellement acceptée. Plusieurs auteurs classent le LBP de différentes manières comme: purement statistique [60], purement structurel [61], stochastique [62], ou même à base de modèle [63].

3.2.3. Problèmes d'analyse de texture

Lors de l'application d'une l'analyse de texture dans un environnement réel, selon les mesures exigées, différents sous-problèmes d'analyse de texture sont rencontrés.

Tuceryan et Jain (1998) [49] ont listé quatre problèmes d'analyse de texture: la classification de texture, la segmentation de texture, la synthèse de texture, et la détermination d'une forme par texture. Par contre, Petrou et Sevilla (2006) [52] ont fait une liste de trois problèmes comprenant: la classification de texture, la

segmentation de texture, et la détection des défauts par texture. Dans ce qui suit, ces problèmes sont discutés en plus de détails.

a. Classification de texture

Dans la classification de texture, le but consiste à assigner un échantillon de texture inconnu dans l'une des classes prédéfinies (**figure 3.2**). L'attribution se faite sur la base de règles qui sont généralement dérivées automatiquement à partir d'un ensemble d'apprentissage composé par des échantillons de texture avec des classes connues.

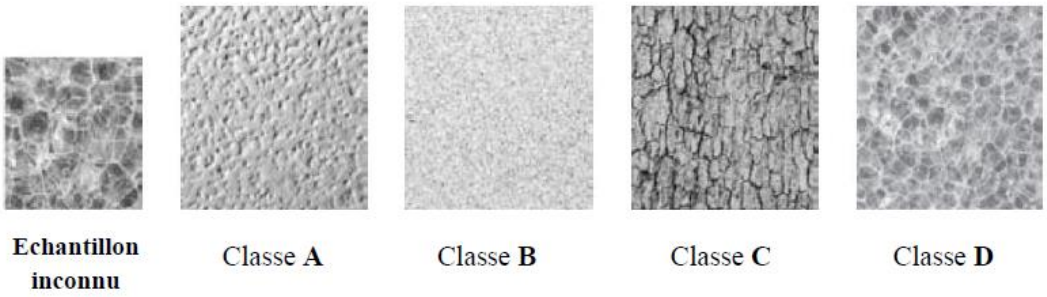


Fig. 3. 2 : Exemple de classification de texture.

Étant donné une image de texture segmentée pour être classifiée, les deux composantes essentielles sont l'extracteur de caractéristiques et l'algorithme de classification. Un aperçu sur les approches d'extraction des caractéristiques de texture est présenté dans la sous-section suivante (4.2.4). Pour une introduction générale et un examen sur les classificateurs de motifs statistiques, voir les références [63,64], ou pour un regard critique sur les progrès dans la recherche sur les classificateurs, voir la référence [65].

Dans la classification de texture, le classificateur de type k-NN avec différentes mesures de distances est considéré comme un choix commun [66,67]. Récemment, le SVM a gagné plus d'intérêt, les résultats rapportés avec ce classificateur ont surpassé les résultats du k-NN [68,69].

Le problème de la récupération de texture dans une certaine mesure est lié à la classification de texture. Essentiellement, la récupération de texture est une opération basée sur le contenu de l'image appliquée aux images de texture. Ainsi, l'objectif est de récupérer à partir d'une base de données autant d'échantillons de textures demandées que possible.

Cependant, la texture est plus souvent utilisée comme une caractéristique additionnelle pour une récupération générale de l'image.

b. Segmentation de texture

Dans la segmentation de texture, le but consiste à diviser une image en régions cohérentes par l'utilisation de l'information de texture (**figure 3.3**). Dans la segmentation supervisée de texture, le système dispose des modèles de textures pour être rencontrés dans les images à segmenter. D'autre part, la segmentation non-supervisée de texture a pour objectif de diviser une image en régions de textures similaires sans aucune information a priori sur les différentes textures. La

segmentation de l'image, quoiqu'un problème mal posé, a plusieurs applications pratiques, ainsi que la texture s'est avérée comme un signal utile dans la segmentation.

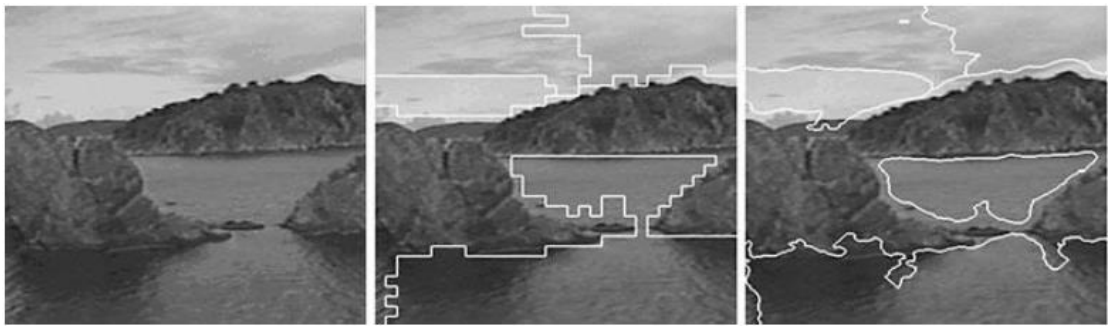


Figure 3. 3 : Exemple de segmentation de texture.

La détection des défauts par texture est un sous-problème de segmentation de texture, elle est généralement rencontrée dans l'inspection visuelle. Dans ce problème, nous avons un modèle de texture "acceptable", et l'objectif consiste à analyser l'image de texture pour trouver des défauts, qui sont des évènements locaux habituellement dérivés par un modèle.

c. Détermination d'une forme par texture

Le problème de la détermination d'une forme par texture consiste à déduire la forme de trois dimensions (3D) d'un objet à partir de son image. Il est prouvé que la texture est un repère important dans la perception de la forme 3D par les humains [70]. Parmi les recherches dans le domaine de la vision par ordinateurs, l'une des stratégies récentes proposée pour la détermination d'une forme par texture qui consiste à modéliser la déformation des éléments de textures individuelles, comme proposée par Lobay et Forsyth (2006) [72]. Cependant, ils précisent dans leur article que « les applications pour la détermination d'une forme par texture sont largement absentes ».

d. Synthèse de texture

L'objectif de la synthèse de texture est de synthétiser plusieurs échantillons de textures similaires de manière perceptuelle. Après plusieurs années de recherches dans le domaine de synthèse de textures, par application de contraintes statistiques sur les images de sortie [71], les meilleurs résultats semblent actuellement être produits par les approches basées sur les patchs (pièces) de l'image, suggérées pour la première fois dans la synthèse de texture par Efros et Freeman (2001) [75].

3.2.4. Description de texture

Différentes manières pour regrouper les modèles de texture sont discutées dans la littérature de l'analyse de texture. Ces taxonomies sont rarement approfondies, car certains modèles peuvent avoir des propriétés de plusieurs groupes et quelques modèles semblent n'appartenir à aucun groupe. Ces regroupements sont toujours utiles pour aider à comprendre la variété de différents modèles.

Comme nous l'avons discuté dans la section 3.2.2, la classification proposée par Tuceryan et Jain (1998) [49] divise les modèles de texture en quatre groupes:

méthodes statistiques telles que les matrices de cooccurrences et les caractéristiques d'auto-corrélation, méthodes géométriques basées sur l'analyse des propriétés géométriques des primitives de la texture, méthodes basées sur le modèle visant à fournir un prototype pouvant être utilisé à la fois à la description et à la synthèse de textures et méthodes de traitement du signal utilisant typiquement quelques mesures d'énergie à partir des images de texture filtrées.

En imagerie, les descripteurs d'apparence de l'image peuvent être considérés comme des descripteurs généraux de l'image, mais la plupart des descripteurs globaux proviennent effectivement du champ d'analyse de texture. Autrement dit, ils sont initialement proposés pour la classification ou la segmentation de texture.
L'utilisation des filtres de Gabor dans l'analyse de texture remonte aux années 1980. Turner (1986) [76] a étudié la discrimination de différentes textures par les réponses du filtre de Gabor. Plus tard, Bovic et al. (1990) [77] ainsi que Jain et Farrokhnia (1991) [78] ont appliqué les filtres de Gabor pour la segmentation non-supervisée de texture. Jusqu'ici, une grande variété de recherches à l'aide des filtres de Gabor dans différents problèmes d'analyse de texture a été stimulée. L'un des meilleurs descripteurs basé sur les filtres de Gabor est celui développé par Manjunath et Ma (1996) [79], où les caractéristiques de texture sont obtenues par le calcul des moyens et des écarts-types des réponses du filtre de Gabor sur une image de texture. Pour un bref aperçu et comparaison sur les différentes approches de description de texture basées sur les filtres de Gabor, voir la référence [80].

L'une des issues les plus récemment découvertes dans la description de texture, est le problème posé par les surfaces de trois dimensions. La texture perçue par ces surfaces n'est pas causée par des changements dans l'albédo de la surface seulement, mais aussi par l'auto-ombrage et l'auto-occlusion possibles provoqués par des petites variations d'échelle dans la forme de la surface. Cela cause des variations, dues à l'illumination ou aux changements de l'angle de visionnement, qui font que la texture devienne complexe et donc difficile à modéliser ou manipuler par un descripteur de texture.

Afin de restaurer le regroupement pour les sorties des filtres, Leung et Malik (2001) [81] ont proposé un descripteur de texture 3D qui enregistre précisément un ensemble d'images d'une texture par la convolution de chaque image enregistrée avec une banque de filtre. Ensuite, les prétendus textons 3D peuvent être formés par le regroupement des vecteurs comprenant des réponses de chaque filtre à la même position de chaque image enregistrée. L'histogramme des textons 3D est ensuite utilisé comme un descripteur.

Une stratégie récemment proposée pour la description de texture, consiste à prendre une représentation basée sur le patch (la pièce) local(e) et de l'appliquer à la description de texture. Cette approche a été proposée pour la première fois par Lazebnik et al. (2005) [82], qui ont présenté une méthode de représentation de texture en utilisant des détecteurs de la région d'intérêt et en regroupant les descripteurs locaux calculés au sein de ces régions.

3.2.5. Descripteurs de texture locaux

L'une des approches de description de texture qui a récemment gagné beaucoup d'intérêt est celle basée sur les descripteurs locaux de l'image. Contrairement aux descripteurs globaux où les caractéristiques codifient l'apparence de l'image entière, les descripteurs locaux considèrent les petites sous-régions de l'image.

Selon le contexte de l'application, les régions locales à décrire peuvent être obtenues autour de points d'intérêts automatiquement détectés [83] ou de régions covariantes affinées [83]. L'échantillonnage aléatoire a été proposé par Nowak et al. (2006) [85] avant l'échantillonnage dense, typique dans la description de texture, qui a été appliqué par Tuytelaars et Schmid (2007) [85]. Une grille fixe utilisée pour déterminer les régions locales a été proposée par Ahonen et al. (2006) [87] et Vogel et Schiele (2007) [88].

Comme le patch local à décrire, probablement transformé en une orientation canonique, est déterminé, il existe une variété d'options pour construire les caractéristiques photométriques. Nous pouvons appliquer certains descripteurs globaux sur chaque patch local de l'image ou employer des descripteurs spécifiquement conçus pour les régions locales. Une comparaison entre les descripteurs locaux, faite par Mikolajczyk et Schmid (2006) [89], a évalué plusieurs descripteurs locaux; ils ont conclu que l'histogramme de l'orientation locale du gradient (GLOH pour Gradient Location-Orientation Histogram) [90] fournit les meilleurs résultats, suivi du descripteur de la transformée de caractéristiques visuelles invariantes à l'échelle (SIFT) [92]. Ces deux descripteurs sont basés sur le calcul des histogrammes de l'orientation du gradient dans les sous-régions du patch à décrire. Les caractéristiques robustes et accélérées (SURF) sont un descripteur local introduit récemment par Bay et al. (2006) [93]. Le descripteur SURF est basé sur les ondelettes de Haar; il est rapide à calculer. Il a été également déterminé que SURF présente des résultats meilleurs que SIFT, en dépit de sa plus petite dimension de description [94].
Le descripteur de l'histogramme des gradients orientés (HOG pour Histogram of Oriented Gradients) [89] basé sur un histogramme pondéré des directions de gradient a montré de bonnes performances dans la détection humaine (ex., visage, action ou mouvement). En outre, l'opérateur de motif binaire local (LBP) a été également étendu pour satisfaire aux besoins de la région d'intérêt par Heikkilä et al. (2009) [91], grâce à sa puissance discriminative et à la simplicité de calcul.

3.2.5.1. Motif binaire local (LBP: Local Binary Pattern)

Les motifs binaires locaux ont initialement été proposés par Ojala en 1996 afin de caractériser les textures présentes dans des images en niveaux de gris [67]. Ils consistent à attribuer à chaque pixel P de l'image $I(i,j)$à analyser, une valeur caractérisant le motif local autour de ce pixel. Ces valeurs sont calculées en comparant le niveau de gris du pixel central P aux valeurs des niveaux de gris des pixels voisins.

Le concept du LBP est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Afin de générer un motif binaire, tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement (**figure 3.4**). Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant. On obtient donc pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. Plutôt que de décrire l'image par la séquence des motifs LBP, on peut choisir comme descripteur de texture un histogramme de dimension 255.

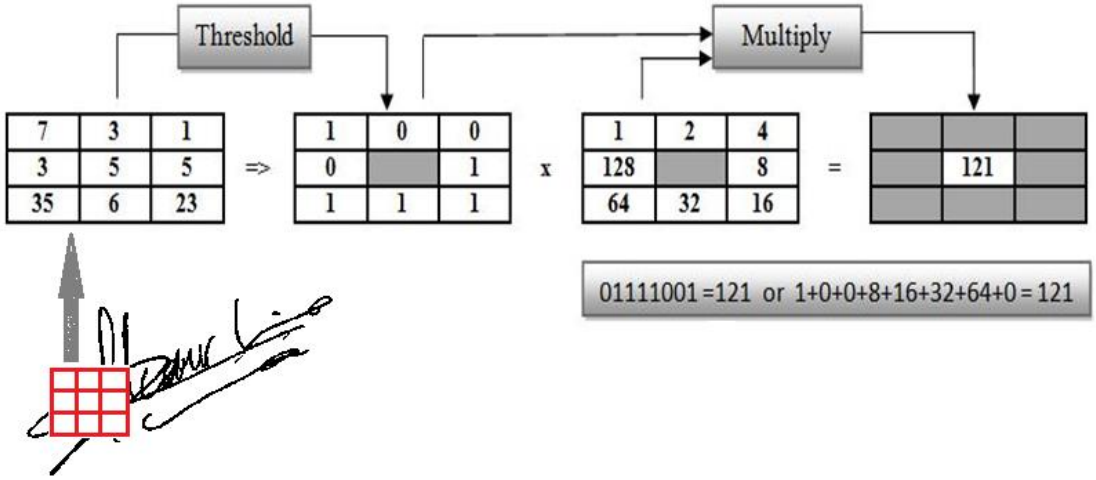


Fig. 3. 4 : Exemple d'extraction des caractéristiques en utilisant l'histogramme de l'opérateur LBP

Pour calculer un code LBP dans un voisinage de P pixels, dans un rayon R ($LBP_{P,R}$), on compte simplement les occurrences de niveaux de gris g_p plus grands ou égaux à la valeur centrale.

$$LBP_{P,R} = \sum_{i=0}^{P-1} u(g_i{}^{P,R} - g_c).2^i \qquad (3.1)$$

Où $u(\dots)$est la fonction signe et où g_i et g_c sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

$$u(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{autrement} \end{cases} \qquad (3.2)$$

La LBP a été étendu ultérieurement en utilisant des voisinages de taille différente (multi-échelle). Un voisinage pour un pixel central est réparti sur un cercle et construit à partir de deux paramètres : le nombre de voisins "P" sur le cercle et un rayon "R" pour définir une distance entre un pixel central et ses voisins. Soit une texture: $T = t(g_c, g_0 \dots \dots . g_{p-1}), g_c$correspond à la valeur de niveau de gris du pixel central etg_p, avec $p = 0, \dots . p - 1$, correspond au niveau de gris de P pixels espacés régulièrement sur un cercle de rayon R. Si les coordonnées de$g_c$ont égales à (0,0), alors les coordonnées de $g_p$sont données par l'équation suivante :

$$\{x_g = x_c + R.\cos\left(2.\pi.\frac{p}{P}\right) \quad , y_g = y_c - R.\sin\left(2.\pi.\frac{p}{P}\right) \tag{3.3}$$

Comme nous pouvons le voir sur **la figure 3.5**, les coordonnées d'un voisin ne sont pas forcément situées au centre d'un pixel. Dans ce cas, le niveau de gris est déterminé par l'intermédiaire d'une interpolation. Cette figure, illustre différentes voisinages obtenus pour différentes valeurs du couple (P, R)

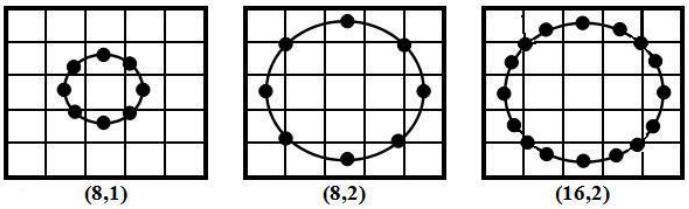


Fig. 3.5 LBP multi-échelle. Exemples de voisinages obtenus pour différentes valeurs de (P, R), source Ojala et al [67].

La propriété la plus importante de l'opérateur LBP dans les applications du monde réel réside dans son invariance contre les changements monotones du niveau de gris causés, par exemple, par des variations d'éclairage. Une autre propriété aussi importante réside dans sa simplicité de calcul, qui permet d'analyser des images compliquées en temps réel.

3.2.5.2. Caractéristiques statistiques et binarisées de l'image (BSIF : Binarized Statistical Image Features)

Le descripteur BSIF a été proposé par Kannala et Rahtu (2012) [94], il a été utilisé pour la reconnaissance de visage et la classification de texture. Basé sur LBP et LPQ, l'idée derrière le BSIF consiste à apprendre automatiquement un ensemble fixe de filtres à partir d'un petit ensemble d'images naturelles, au lieu d'utiliser des filtres fabriqués-à-la-main comme LBP ou LPQ. BSIF implique un apprentissage, au lieu d'un réglage manuel, pour obtenir une représentation statistiquement significative de l'image, qui permet d'encoder l'information efficace en utilisant la quantification par élément simple. L'apprentissage fournit également une manière facile et flexible pour ajuster la longueur du descripteur et de l'adapter aux applications présentant des caractéristiques d'images inhabituelles.

Pour caractériser les propriétés de la texture dans chaque sous-région de l'image, les histogrammes des labels BSIF sont alors utilisés. La valeur de chaque élément (bit) dans la chaîne du code binaire BSIF est calculée par binarisation de la réponse d'un filtre linéaire, avec un seuil à zéro. Chaque bit est associé à un filtre différent et la chaîne de bits détermine le nombre de filtres utilisés. L'ensemble de filtres est appris (formé) à partir d'un ensemble de patchs d'images naturelles en maximisant l'indépendance statistique des réponses du filtre.

Étant donné un patch d'image X de taille pixels lxl et un filtre linéaire W_i de la même taille, la réponse du filtre S_i est obtenue par:

$$s_i = \sum_{u,v} W_i(u,v) X(u,v) = w_i^t x \quad (3.4)$$

Où les vecteurs w et x contiennent les pixels de W_i et X.
La caractéristique binarisée b_i est obtenue par la mise de $b_i = 1$ si $s_i > 0$ et $b_i = 0$ sinon. Les filtres Wisont appris en utilisant l'analyse en composantes indépendantes (ICA) en maximisant l'indépendance statistique des$_i$
Le descripteur BSIF possède deux paramètres qui sont: la taille du filtre l et la longueur n de la chaîne binaire. Les filtres originaux proposés par Kannala et Rahtu (2012) [94] ont été appris avec 50 000 patchs d'images.

3.3. Conclusion

Dans ce chapitre, nous avons présenté les principales notions utilisées dans le domaine de l'analyse de texture, qui est un problème très difficile. Cette difficulté est due essentiellement au fait qu'il n'existe pas de définition précise et rigoureuse de la notion de texture. Le choix des attributs de texture d'une manière générale est un point délicat, puisqu'il dépend de plusieurs facteurs. On a choisi LBP et BSIF comme des descripteurs dans notre travail qui éclaire sur l'identification et la vérification de signature manuscrite hors ligne donc Les attributs sont donc à choisir avec précaution car non seulement ils dépendent de l'application considérée, mais ils influent également sur la performance de la discrimination.

La fonction du descripteur est de convertir les informations au niveau-pixel en une forme utile, qui capture les contenus les plus importants de l'image. Contrairement aux descripteurs globaux qui calculent les caractéristiques directement à partir de l'image entière, les descripteurs locaux, considérés comme les plus efficaces dans les conditions réelles, représentent les caractéristiques en petits patchs locaux de l'image.

Dans le cadre de cette thèse, nous avons étudié l'utilisation de deux descripteurs de texture locaux très récents, à savoir: LBP et BSIF, et nous avons fourni une vaste analyse sur deux bases de données MCYT-75, GPDS 100 et 160. Les descripteurs ont été analysés en termes de précision de classification et complexité algorithmique. En outre, les performances de ces descripteurs sous différents paramètres sont bien discutées dans le chapitre suivant.

Chapitre 4

Résultats expérimentaux et discussions

4.1.Introduction

Dans le chapitre précédent, nous avons présenté la technique dite "*Motif Binaire Local (LBP: Local Binary Pattern)*" largement utilisée en caractérisation des images texturées, ainsi que ces extensions les plus populaires en analyse de texture. Nous avons aussi étudié des variantes très récentes et plus adaptées à l'analyse de texture. « *Caractéristiques Statistiques et Binarisées de l'Image (BSIF: Binarized Statistical Image Features)*".

Dans ce chapitre, nous allons tester et comparer ces descripteurs de texture récents sur des images de données biométriques, à savoir: MCYT-75 et GPDS sur la signature manuscrite hors ligne, afin de mettre en évidence leur performances et leur efficacités dans la reconnaissance des individus; ces descripteurs sont comparés entre eux, en terme de pouvoir discriminant.

Pour tester les différentes approches, nous allons utiliser l'une des méthodes de classification multi-classes supervisées, à savoir: les k-plus proches voisins (k-NN). L'évaluation et la comparaison sont effectuées en utilisant les deux modes : identification et vérification.

4.2. Méthodologie

Notre système biométrique nécessite deux phases opérationnelles. La première est une phase d'apprentissage: elle consiste à enregistrer les caractéristiques de signature hors ligne de chaque individu afin de créer son propre modèle biométrique; puis a été enregistré dans la base de données. La deuxième est la phase de test qui consiste à enregistrer les mêmes caractéristiques et à les comparer aux modèles biométriques stockés dans la base de données si les données enregistrées correspondent à un modèle biométrique de la base de données. Le schéma général est représenté sur ***la figure 4.1.***

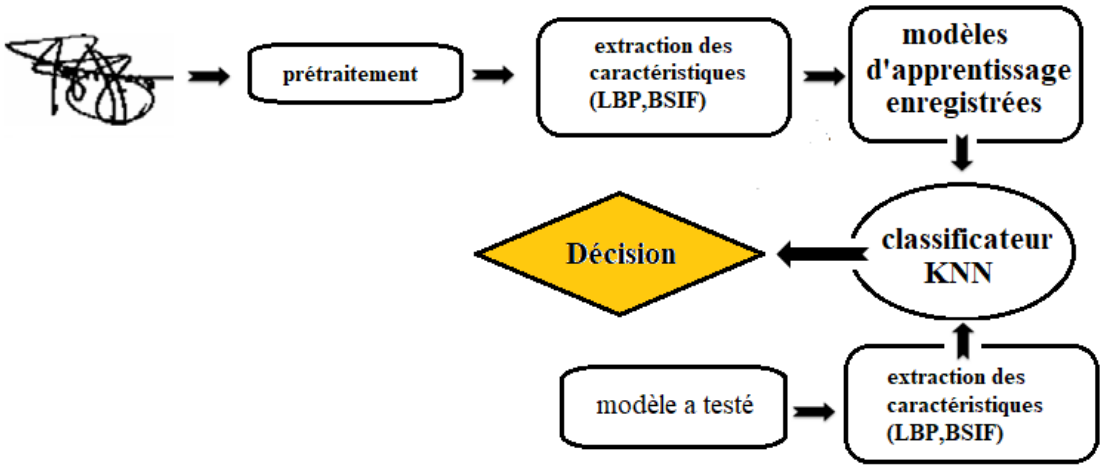


Fig. 4.1. Système de reconnaissance de signature manuscrite hors ligne proposé

4.2.1. Prétraitement

L'étape de prétraitement a été appliquée dans les phases d'apprentissage et de test. L'objectif de cette phase est de préparer la représentation de l'image source afin de faciliter la tâche des étapes suivantes pour rendre la signature standard et prête pour l'extraction de caractéristiques et pour améliorer les performances de reconnaissance.

Les bases de signatures sont numérisées en niveau de gris, avec un arrière-plan bien contrasté. Pour résoudre ce problème, les images des signatures ont été binarisées par postérisation [95]. Soit une image de signature de la base de données à 256 niveaux de gris. L'image postérisée est définie comme suit:

$$I_p(x,y) = round\left(round\left(\frac{I(x,y)n_L}{255}\right)\frac{255}{n_L}\right) \quad \textbf{(4.1)}$$

Où round (.) Arrondit les éléments aux entiers les plus proches. Dans cette thèse et avec les bases de données MCYT et GPDS, nous avons sélectionné $n_L = 3$ (bien segmenté), moins de cette valeur la signature est à moitié effacée. Donc, avec les traits de signature sont bien conservés et l'arrière-plan apparaît presque propre.

Dans l'image postérisée, les traits de signature apparaissent plus foncés avec un arrière-plan blanc. Par conséquent, pour obtenir l'image binarisée (traits noirs et fond blanc); une simple opération de seuillage est appliquée comme suit:

$$I_{bw}(x,y) = \begin{cases} 255 & if\ \ I_P(x,y)=255 \\ 0 & otherwise \end{cases} \quad \textbf{(4.2)}$$

L'image en noir et blanc est utilisée comme un masque pour segmenter la signature originale et la signature segmentée est obtenu comme suit:

$$I_s(x,y) = \begin{cases} 255 & if\ \ I_{bw}(x,y)=255 \\ I(x,y) & otherwise \end{cases} \quad \textbf{(4.3)}$$

Après cela, nous utilisons le déplacement de l'histogramme pour réduire l'influence des différents stylos à encre d'écriture sur la signature segmentée. Nous atteignons ceci en déplaçant l'histogramme des pixels de signature vers zéro, en gardant l'arrière-plan blanc avec un niveau de gris égal à 255. En garantissant que la valeur de niveau de gris du pixel de signature le plus sombre est toujours égale à 0. Cela peut être réalisé en soustrayant la valeur de niveau de gris minimum dans l'image à partir des pixels de signature, comme suit:

$$I_G(x,y) = \begin{cases} I_s(x,y) & if\ \ I_s(x,y)=255 \\ I_s(x,y) - \min\{I_s(x,y)\} & otherwise \end{cases} \quad \textbf{(4.4)}$$

$I_G(x,y)$: L'histogramme segmenté d'image déplacé vers zéro.

4.2.2 Extraction des caractéristiques

Après la segmentation et le déplacement de l'histogramme de signature, l'image est rognée pour fixer la taille de la signature et elle est redimensionnée à N = 256 et M = 256. Le but de ces ajustements est d'améliorer l'invariance d'échelle. En tant que méthode d'interpolation, nous utilisons le voisin le plus proche. Ceci afin de garder la texture de l'encre aussi invariante que possible.

L'opérateur LBP (ou BSIF) est appliqué à l'image de la signature. Ensuite, l'image résultante est divisée en bloc es se chevauchant après l'application de l'opérateur LBP (ou BSIF). Pour chaque bloc, les statistiques de la LBP (ou BSIF) sont résumées par histogramme. Le descripteur de signature final est obtenu en concaténant les histogrammes de différents blocs.

La méthode de décomposition par chevauchement est basée sur la décomposition d'une image dans un ensemble de correctifs de taille mxm avec un pourcentage de décomposition superposé. Étant donné une image de tailleNxM, le nombre de tous les correctifs de longueur (mxm) obtenus par la méthode de décomposition par chevauchement est égal:$\left(\frac{N-m}{x_{overlap}}+1\right)\left(\frac{M-m}{y_{overlap}}+1\right)$ et arrondit la valeur aux entiers les plus proches Vers l'infini. $x_{overlap}$, $y_{overlap}$sont respectivement les étapes de déplacement dans les directions horizontale et verticale.

4.2.3. Classification

4.2.3.1. La méthode des K plus proches voisins

L'algorithme des k-plus proches voisins (k-nn : pour k-neighrest neighbors en anglais) est un algorithme intuitif, aisément paramétrable pour traiter un problème de classification avec un nombre quelconque d'étiquettes.

Dans ce cadre, on dispose d'une base de données d'apprentissage constituée de N couples « entrée-sortie ». Pour estimer la sortie associée à une nouvelle entrée x, la méthode des k plus proches voisins consiste à prendre en compte (de façon identique) les k échantillons d'apprentissage dont l'entrée est la plus proche de la nouvelle entrée x, selon une distance à définir. Dans notre travail en a choisi la distance chi carré

4.2.3.2. La distance chi carré ($\mathbf{X^2}$)

La distance chi au carré d (x, y) est un test statistique permettant de tester l'adéquation d'une série de données à une famille de lois de probabilités ou de tester l'indépendance entre deux variables aléatoires.

La distance de l'histogramme Chi-carré est l'une des mesures de distance qui peuvent être utilisées pour trouver la dissimilarité entre deux histogrammes ; $x = [x1, \dots, xn]$ et$y = [y1, \dots, yn]$, ayant n cases à la fois. De plus, les deux histogrammes sont normalisés.

La mesure de distance d est généralement définie par:

$$d(x, y) = \frac{1}{2}\sum_{i=1}^{n} \frac{(xi - yi)^2}{xi + yi} \qquad \textbf{(4.5)}$$

4.2.3.3. La méthode de zonage (zoning)

Cette méthode redimensionnée l'image de taille 256 * 256 pixels (eg. Notre travail) est divisé en 4 ou 16 zones chacun de taille 128* 128 et 64*64 pixels respectivement. On a appliqué l'extraction de caractéristique pour chaque zone sous un histogramme de signature. Ces histogrammes de signatures sont concaténés dans un seul histogramme, ensuite ils ont sauvegardé dans une base de modèles.

4.3.Résultats expérimentaux et discussion

4.3.1. Bases de données

Nous avons utilisé deux bases de données MCYT-75 et GPDS (100 et 160). Les deux ont été numérisés à 600 dpi, ce qui garantit une représentation suffisante de la texture grise. Les principales différences entre elles sont les stylos utilisés. Dans la base de données MCYT, tous les signataires authentiques et falsifiés sont signés avec le même stylo sur la même surface. Au lieu de cela, dans la base de données GPDS,

tous les utilisateurs ont signé avec leurs propres stylos sur différentes surfaces. Deux corpus de signature hors ligne accessibles au public ont été utilisés.

4.3.1.1.GPDS-100

Le corpus de signature GPDS-100 contient 24 signatures authentiques et 30 contrefaçons de 100 individus. Donc, il y a 100 x 24 donnant 2400 signatures authentiques et 100 x 30 donnant 3000 contrefaçons [96]. Comme on l'a vu précédemment, les signataires ont utilisé leur propre stylo sur du papier blanc A4, après que les formulaires de signature ont été recueillis, chacun a été numérisé sur 256 niveaux de gris à une résolution de 600 dpi.

4.3.1.2.MCYT -75

La base de données du MCYT [97], comprend 75 signataires provenant de quatre sites espagnols différents. Le corpus comprend 15 signatures authentiques et 15 faux simulés pour chaque signataire. Les signatures authentiques ont été acquises en deux sessions. Les faussaires reçoivent les images signatures des clients à falsifier et, après plusieurs entraînements avec eux, ils sont invités à imiter la forme. Toutes les données de signatures ont été acquises avec le même stylo encreur et les mêmes modèles de papier, sur une tablette à stylet similaire. Les modèles de papier ont été numérisés à 600 dpi. Cette base de données hors connexion de signature est disponible publiquement à l'adresse :
https://atvs.ii.uam.es/atvs/databases.jsp

4.3.2. Résultats d'identification de signature

Dans ce travail, nous avons testé les résultats de divers descripteurs de texture récents: LBP et BSIF sur les bases de données MCYT-75 et GPDS-100 pour la tâche d'identification de signature manuscrite hors ligne, ces descripteurs sont comparés afin de mettre en évidence l'efficacité et la performance des deux caractéristiques**.**

Nous avons pris dix images «10» pour chaque personne dans les bases de données en tant qu'ensemble d'apprentissage et les autres images manuscrites de la même personne «authentique» ont été utilisées comme ensemble de test (***figure 4.2),*** sont présentées dans le ***Tableau 1***.

Tableau 4.1 Distribution d'images entre l'apprentissage / tests en utilisant dix (10) images de chaque personne dans d'apprentissage.

Base de données	MCYT-75	GPDS-100
Nombres des personnes	75	100
Nombres des images	1125	2400
Images utilisées dans l'apprentissage	750	1000
Images utilisées dans le tests	375	1400

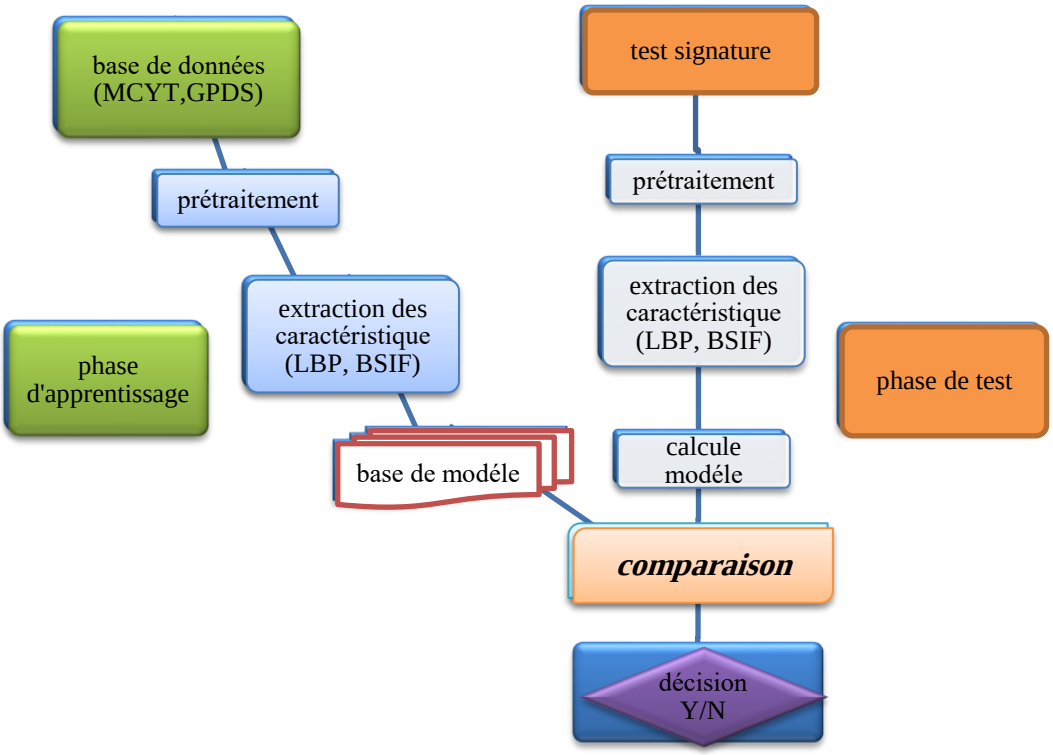


Fig. 4.2. Schéma synoptique de notre système d'authentification de signature hors ligne proposé

Nous avons divisé notre expérience en trois étapes; dans la première étape, nous notons simplement les résultats primaires avec les paramètres standards. Puis, dans un deuxième temps, tous les paramètres des descripteurs sont optimisés afin d'obtenir les meilleures valeurs de chaque caractéristique; enfin, la méthode de zonage est appliquée à la fois aux descripteurs BSIF et LBP dans le but d'explorer les effets de la procédure de zonage sur l'étape d'extraction des caractéristiques et donc la performance du système proposé.

Dans la première étape des expériences, nous avons utilisé les paramètres de base des descripteurs tirés de l'article original de Kannala et Rahtu (2012) [94]. Le LBP a été choisi avec différents paramètres (8, 1), (8, 2), (16, 2) et le BSIF avec un filtre de longueur de 11x11 et de 8 bits.

Le classificateur K-NN a été utilisé avec une distance de « chi-square ». Sur la base de quelques expériences préliminaires, nous avons trouvé que la distance du « chi-square » donne de meilleurs résultats comparés à d'autres distances telles que la distance du city block, euclidiennes ou dehamming. Comme le montre le ***Tableau 2***, les résultats obtenus indiquent que le descripteur BSIF donne les meilleures performances sur les deux bases de données.

Tableau 4.2 Taux de reconnaissance utilisant les paramètres de base des deux descripteurs LBP et BSIF

Base de données	MCYT-75	GPDS-100
LBP(8.1)	82.7	60.7
LBP(8.2)	89.3	80.1
LBP (16.2)	90.7	86.0
BSIF	91.2	88.3

Dans la deuxième étape des expériences, nous avons effectué plusieurs tests supplémentaires sur BSIF, où nous avons utilisé tous les paramètres de la taille de la fenêtre de filtrage et tous les nombres de bits qui composent la chaîne de code binaire pour trouver les paramètres optimaux permettant d'obtenir les meilleurs résultats.

Cette procédure a été appliquée pour les deux bases de données impliquées dans la présente étude MCYT-75 et GPDS-100, comme indiqué dans les ***Tableaux 3et 4.***

Tableau 4.3 Taux de reconnaissance utilisant tous les paramètres BSIF appliqués sur la base de données MCYT-75

paramétres BSIF (bits)	3x3	5x5	7x7	9x9	11x11	13x13	15x15	17x17
5	74.9	83.2	85.9	84.8	82.9	81.6	81.6	77.6
6	84.0	89.3	90.7	87.5	87.7	86.7	84.5	88.0
7	81.3	90.1	90.7	90.7	90.7	88.8	89.1	88.0
8	83.5	91.2	92.0	91.5	91.2	91.2	89.6	89.1
9	-	93.3	92.8	93.1	93.6	92.3	92.8	92.0
10	-	93.3	93.1	94.7	93.6	94.4	94.7	94.1
11	-	93.1	94.1	93.9	93.6	93.1	93.6	92.8
12	-	92.5	95.2	***95.7***	94.1	94.4	93.6	93.3

Tableau 4.4 Taux de reconnaissance utilisant tous les paramétres de BSIF appliqués sur la base de données GPDS-100

Paramétres BSIF (bits)	3x3	5x5	7x7	9x9	11x11	13x13	15x15	17x17
5	66.9	72.1	73.9	73.9	72.8	70.4	70.1	69.6
6	70.4	78.1	80.7	81.6	81.3	79.9	79.6	77.4
7	74.9	81.0	84.6	86.6	86.7	86.6	84.5	82.1
8	72.9	82.1	87.1	88.1	88.3	88.4	86.8	84.7
9	-	82.2	87.0	88.5	89.7	89.3	89.4	88.3
10	-	83.1	87.9	89.2	91.1	91.5	91.1	90.4
11	-	83.2	86.6	89.3	90.3	90.9	91.4	91.4
12	-	82.4	86.1	89.1	90.7	90.8	91.5	***91.9***

La meilleure valeur du descripteur BSIF dans la base de données MCYT-75 est de 95,7% obtenue avec une taille de fenêtre de 9x9 et 12 bits, tandis que le meilleur résultat pour la base de données GPDS-100 est de 91,9% avec une taille de fenêtre de 17x17 et 12 bits.

Dans la dernière étape des expériences réalisées dans la présente étude, nous avons appliqué la méthode de zonage avec chevauchement pour les deux descripteurs LBP et BSIF afin d'évaluer son effet sur la performance des deux descripteurs. Ainsi, nous avons pris les meilleurs paramètres de BSIF dans les deux bases de données MCYT-75 et GPDS-100. Les tableaux 5 et 6 montrent les résultats; avec également plusieurs paramètres testés en utilisant le descripteur LBP.

Tableau 4.5 Taux de reconnaissance utilisant des descripteurs BSIF et LBP sur la base de données de signatures hors ligne MCYT-75, avec zonage, chevauchement et modification de la taille des blocs.

Extractions des paramétres	Taille de bloc et chevauchement	[256 256]	[128 128]		[64 64]	
		Sans chevauchemt	[0 0]	[0.5 0.5]	[0 0]	[0.5 0.5]
Différents paramétres de LBP	LBP(4,1)	68.0	83.7	90.4	93.1	94.4
	LBP(4,2)	79.2	89.0	93.9	94.9	95.7
	LBP(4,3)	76.5	88.8	93.1	94.9	95.2
	LBP(8,1)	82.7	91.2	95.7	94.4	96.0
	LBP(8,2)	89.3	94.7	96.5	96.3	97.1
	LBP(8,3)	92.0	94.7	96.8	96.5	97.1
	LBP(12,1)	85.6	91.7	95.2	94.4	96.5
	LBP(12,2)	90.7	94.7	96.0	96.3	96.8
	LBP(12,3)	93.9	94.4	97.1	96.8	**97.3**
	LBP(16,1)	84.0	91.2	93.9	94.7	96.3
	LBP(16,2)	90.7	93.3	94.9	96.3	96.8
	LBP(16,3)	93.1	94.7	96.5	96.5	**97.3**
BSIF avec le meilleur filtre	window size 9x9 and 12-bits	95.7	75.2	76.0	77.1	78.7

Selon le tableau 5, le descripteur LBP donne des résultats impressionnants avec la méthode de zonage par division d'images, suivie par le descripteur BSIF. Par conséquent, la meilleure valeur obtenue est de 97,3% avec LBP (12,3) et (16,3) avec un bloc de taille 64 et un chevauchement est égal à la moitié.

Tableau 4.6 Taux de reconnaissance utilisant des descripteurs BSIF et LBP sur la base de données de signatures hors ligne GPDS-100, avec zonage, chevauchement et modification de la taille des blocs

Extractions des paramétres \ Taille de bloc et chevauchement		[256 256]	[128 128]		[64 64]	
		Sans chevauchemt	[0 0]	[0.5 0.5]	[0 0]	[0.5 0.5]
différentspar amétres de LBP	LBP(4,1)	56.4	85.5	89.4	93.7	95.0
	LBP(4,2)	59.9	86.7	90.8	93.6	95.1
	LBP(4,3)	59.6	86.9	91.4	93.6	94.9
	LBP(8,1)	60.7	87.3	90.7	93.8	95.6
	LBP(8,2)	80.1	92.4	93.9	94.6	95.9
	LBP(8,3)	79.6	90.3	92.4	94.1	94.8
	LBP(12,1)	62.9	80.1	86.4	90.5	91.9
	LBP(12,2)	82.0	93.5	94.2	94.8	**96.1**
	LBP(12,3)	86.7	94.3	94.9	95.4	96.0
	LBP(16,1)	58.6	86.9	90.5	93.9	95.2
	LBP(16,2)	86.0	92.8	93.7	94.5	96.0
	LBP(16,3)	82.9	91.1	94.1	93.9	95.4
BSIF avec le meilleur filtre	window size 9x9 and 12-bits	89.1	63.1	63.2	65.6	67.0

Comme le montre le tableau 6, le meilleur résultat obtenu après l'application de la procédure de zonage est obtenu par le descripteur LBP, qui est de 96,1%, la taille de bloc de 64 et le chevauchement est égal à la moitié. En revanche, nous avons remarqué que les descripteurs BSIF donnaient des résultats plus faibles lorsqu'ils étaient appliqués avec la procédure de zonage.

Le descripteur BSIF donnent de meilleurs résultats que le descripteur LBP dans le cas où l'histogramme est calculé sur l'ensemble de l'image (BSIF / LBP). Cependant, dans le cas où l'histogramme est calculé sur bloc d'image avec chevauchement (BSIF / LBP), le descripteur LBP donnent des meilleurs résultats.

La taille du vecteur de caractéristiques finales (histogramme de l'image BSIF) dans le cas global est inférieure à la taille du vecteur de caractéristique finale (histogrammes de LBP) dans les blocs qui se chevauchent, ce qui conduit à plus de complexité de calcul. L'avantage des descripteurs BSIF serait donc dans les applications en temps réel.

4.3.3. Résultats de vérification de signature

Dans la seconde partie de l'expérience, nous avons testé les performances de vérification de notre système par deux bases de données (GPDS, MCYT). Ainsi, les premiers corpus de signature GPDS-100 et GPDS-160 sont divisés en trois sous-ensembles égaux comme serdouk et al. 2016 [98]. Deux parties sont utilisées dans le système d'entraînement (16 signatures authentiques); tandis que le sous-ensemble restant est utilisé dans le système de test.

La deuxième base de données MCYT-75 est divisée également en apprentissage et test, nous prenons 10 images de signature dans l'apprentissage et 5 images dans la phase de test.
Le tableau 7 présente la comparaison des performances de notre système avec l'état de l'art sur les bases de données : GPDS-100, GPDS-160 et MCYT-75.

Tableau 4.7 Comparaison avec l'état de l'art sur les bases de données MCYT-75 ,GPDS-100 / GPDS-160 (erreurs en%)

bases de données	Référence	paramétres	FAR	FRR	EER
GPDS-100	Serdouk et al. 2006	GLBP, LRF	11.38	13.16	12.52
	Shekar and bharathi 2014	PCA_MLP	4.44	5.33	/
	Système proposé	**LBP (zonage + chevauchemt), KNN (la distance chi-square)**	***4.65***	***3.75***	***4.2***
GPDS-160	Ferrer et al. 2005	Caractéristiques géométriques	12.60	14.10	/
	Yilmaz 2015	LBP,HOG	/	/	6.97
	Guerbai et al. 2015	Transformation de Curvelet	/	/	15.07
	Batista et al. 2012	Segmentation de grille	/	/	16.84
	Nguyen et. al. 2009	Caractéristiques globales	/	/	17.25
	Nguyen et. al. 2007	SVM	/	/	20.07
	Eskander et. al. 2013	Writerdependentclassifier	/	/	22.71
	Kumar et al. 2012	Surroundedness	/	/	13.76
	Vargas et al. 2008	Polar Distribution	14.66	10.01	/
	Solar et al. 2008	Matching Using Local Interest Points	14.20	16.40	/
	Hu and Chen (GPDS-150) 2013	LBP, GLCM, HOG	/	/	7.66
	Système proposé	**LBP (zonage + chevauchemt) , KNN (la distance chi-square)**	***5.69***	***3.91***	***4.8***
MCYT-75	Ooi et al. 2015	DRT + PCA (PNN)	**/**	**/**	9.87
	Soleimani et al. 2016	HOG (DMML)	**/**	**/**	9.86
	Système proposé	**LBP (zonage + chevauchemt) , KNN (la distance chi-square)**	***6.23***	***9.33***	***7.78***

Dans toutes les bases de données, nous remarquons une amélioration de la performance par rapport à d'autres travaux publiés dans la littérature. Ainsi, pour le GPDS-100, nous avons obtenu des FAR et des FRR de 4,65%, 3,75% contre 4,49% et 5,33% respectivement pour le FAR et le FRR [99]. Sur le GPDS-160, nous avons obtenu un EER de 4,8%, comparé au meilleur EER de 6,67% [100], et avec MCYT-75, nous avons obtenu une EER de 7,78% contre 9,86% [101].

4.4. Conclusion

Dans ce chapitre, nous avons présenté notre système d'identification et de vérification de signature hors ligne proposé, une évaluation de notre système a été effectuée sur les bases de données MCYT-75, GPDS-100 et GPDS-160. Nous nous sommes concentrés sur la recherche des meilleurs paramètres du descripteur BSIF. Dans la dernière étape, nous avons appliqué la méthode de division d'image connue sous le nom de zonage avec chevauchement avec les descripteurs BSIF et LBP. Les résultats ont montré que le descripteur LBP surpasse le descripteur BSIF.

Conclusion générale

La nécessité d'accès sécurisés automatisés à des environnements physiques ou virtuels est en pleine croissance. Ce besoin requière des moyens fiables pour vérifier l'identité d'une personne qui se présente au système d'accès. Les moyens classiques reposants sur des mots de passe ou des cartes magnétiques associées à un code personnel présentent un certain nombre d'inconvénients. Un mot de passe peut être oublié ou même cédé à quelqu'un d'autre ; les cartes d'accès peuvent également être perdues ou volées.

Les systèmes biométriques sont devenus des outils de plus en plus importants pour la sécurité de l'individu et de l'information; ils fournissent une vérification ou une identification automatique de l'identité, qui assure de bonnes performances. En littérature, plusieurs modalités ont été étudiées et comparées. Nous nous sommes intéressés dans cette thèse par l'un des modalités comportementale, en particulier la signature manuscrite, puisqu'elles fournissent une identification efficace, simple, très acceptable par le public et surtout pas chère.

La biométrie regroupe deux axes principaux, en effet elle peut être une identification ou une vérification. Dans une application d'identification, le dispositif biométrique requit une information biométrique et la compare avec chaque information stockée dans la base de données, c'est une comparaison un à plusieurs (1:N). Alors que pour la vérification ou l'authentification, l'utilisateur annonce son identité par une information biométrique, et le système compare la donnée caractéristique obtenue à partir de l'information entrée, avec la donnée enregistrée correspondante à l'identité prétendue, c'est une comparaison un à un (1:1).

Dans ce travail, nous avons présenté une méthode pour la reconnaissance automatique de signature d'écriture hors ligne en utilisant deux caractéristiques de texture locales à savoir LBP et BSIF. La performance du système est présentée en référence à deux bases de données expérimentales de signatures hors ligne contenant des échantillons de 75 et 100 individus. Les expériences réalisées dans cette étude ont été divisées en trois étapes. La première concerne uniquement l'utilisation de descripteurs BSIF et LBP standard dans le système proposé, des expériences préliminaires montrent que le descripteur BSIF a donné de meilleurs résultats par rapport au descripteur LBP. Dans un deuxième temps, nous nous sommes concentrés sur la recherche des meilleurs paramètres du descripteur BSIF sur les deux bases de données. Dans la dernière étape, nous avons appliqué la méthode de division d'image connue sous le nom de zonage avec chevauchement sur des descripteurs BSIF et LBP. Les résultats ont montré que le descripteur LBP surpasse le descripteur BSIF. Les

meilleurs résultats ont atteint un taux d'identification de 97,3% avec la base de données MCYT-75 et de 96,1% avec la base de données GPDS-100.

Pour prouver la performance de notre système, nous avons calculé les paramètres de la phase de vérification (FAR, FRR et EER) et nous l'avons comparé aux résultats dans la littérature, donc nous notons EER égal à 4,2% en GPDS-100, 4,8% en GPDS-160 et 7,78% dans MCYT-75. Et nous avons noté que tous ces résultats dépassaient les différents résultats de performance dans la littérature.

❖ Perspective

Les technologies biométriques sont également de plus en plus souvent utilisées dans des applications qui peuvent rapidement et facilement identifier une personne, mais L'inconvénient majeur de certaines techniques biométriques est qu'elles peuvent être reproduites par d'autres personnes, par exemple on peut reproduire les empreintes digitales sur du silicone, cela a conduit à développer d'autres techniques, en effet, et comme un perspective, le fait d'introduire deux ou plusieurs traits biométriques augmente la performance du système, c'est ce qu'on appelle "La biométrie Multimodale", elle consiste à la multiplication des modalités biométriques, des algorithmes d'analyse ou des bases de données utilisées, elle est de plus en plus utilisée, car elle offre des systèmes de reconnaissance performants et fiables.

Aujourd'hui, les organisations commerciales jouent un rôle de premier plan dans l'utilisation de ces technologies et le développement de nouveaux produits, c'est pour ça, on va essayer au futur d'implémenter notre système après l'amélioration de résultat avec la biométrie Multimodale sur un circuit logique programmable de type FPGA.

Références

[01] Benzaoui, A., Hadid, A. and Boukrouche, A. (2014) 'Ear biometric recognition using local texture descriptors', *IET Biometrics*, Vol. 23, No. 3, pp.9–17.

[02] Bharadi, V.A. and Kekre, H.B. (2010) 'Off-line signature recognition systems', *International Journal of Computer Application*, Vol. 1, No. 27, pp.48–56.

[03] S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition : Security and privacy concerns. IEEE Security & Privacy, 1 :33–42, 2003.

[04] Huang, S.; Elgammal, A.; Lu, J.; Yang, D., "Cross-Speed Gait Recognition Using Speed-Invariant Gait Templates and Globality–Locality Preserving Projections," in Information Forensics and Security, IEEE Transactions on , vol.10, no.10, pp.2071-2083, Oct. 2015

[05] Ansari, A.Q.; Hanmandlu, M.; Kour, J.; Singh, A.K., "Online signature verification using segment-level fuzzy modelling," in Biometrics, IET , vol.3, no.3, pp.113-127, Sept. 2014

[06] Wenxiong Kang; Qiuxia Wu, "Pose-Invariant Hand Shape Recognition Based on Finger Geometry," in Systems, Man, and Cybernetics: Systems, IEEE Transactions on , vol.44, no.11, pp.1510-1521, Nov. 2014.

[07] Ahmed, A.A.; Traore, I., "Biometric Recognition Based on Free-Text Keystroke Dynamics," in Cybernetics, IEEE Transactions on , vol.44, no.4, pp.458-472, April 2014.

[08] Orcan Alpar, Keystroke recognition in user authentication using ANN based RGB histogram technique, Engineering Applications of Artificial Intelligence, Volume 32, June 2014, Pages 213-217.

[09] Haifeng Hu, "Multiview Gait Recognition Based on Patch Distribution Features and Uncorrelated Multilinear Sparse Local Discriminant Canonical Correlation Analysis," in Circuits and Systems for Video Technology, IEEE Transactions on , vol.24, no.4, pp.617-630, April 2014.

[10] Basmajian JV, de Luca CJ. Muscles Alive – The Functions Revealed by Electromyography. The Williams & Wilkins Company; Baltimore, 1985.

[11] F. Ahmed and D. Mohamed: *A review on fingerprint classification techniques*. In Proceedings of the International IEEE Conference on Computer Technology and Development (ICCTD). Vol.2, pp.411-415, Kota Kinabalu (Malaisie), 2009.

[12] Nicolas MORIZET Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris. Thèse de doctorat Soutenue le 18 Mars 2009 à l'Ecole Nationale Supérieure des Télécommunications de Paris Spécialité : Signal et Images.

[13] Billeb, S.; Rathgeb, C.; Reininger, H.; Kasper, K.; Busch, C., "Biometric template protection for speaker recognition based on universal background models," in Biometrics, IET , vol.4, no.2, pp.116-126, 2015.

[14] Caetano Garcia, D.; de Queiroz, R.L., "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," in Information Forensics and Security, IEEE Transactions on , vol.10, no.4, pp.778-786, April 2015

[15] Borah, Tripti Rani; Sarma, Kandarpa Kumar; Talukdar, Pran Hari, "Retina recognition system using adaptive neuro fuzzy inference system," in Computer, Communication and Control (IC4), 2015 International Conference on, pp.1-6, 10-12 Sept. 2015.

[16] Raja, K.B.; Raghavendra, R.; Busch, C., "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information," in Information Forensics and Security, IEEE Transactions on , vol.10, no.10, pp.2048-2056, Oct. 2015

[17] Soldera, J.; Alberto Ramirez Behaine, C.; Scharcanski, J., "Customized Orthogonal Locality Preserving Projections With Soft-Margin Maximization for Face Recognition," in Instrumentation and Measurement, IEEE Transactions on , vol.64, no.9, pp.2417-2426, Sept. 2015

[18] Muwei Jian; Kin-Man Lam, "Simultaneous Hallucination and Recognition of Low-Resolution Faces Based on Singular Value Decomposition," in Circuits and Systems for Video Technology, IEEE Transactions on , vol.25, no.11, pp.1761-1772, Nov. 2015.

[19] J. Daugman: *How Iris Recognition Works ?*. IEEE Transactions on Circuits and Systems for Video Technology. Vol.14, No.01, pp.21-30, 2004.

[20] Guoqiang Li; Busch, C.; Bian Yang, "A novel approach used for measuring fingerprint orientation of arch fingerprint," in Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on , vol., no., pp.1309-1314, 26-30 May 2014.

[21] Ying Li Han ; Tae Hong Min; Rae-Hong Park, "Efficient iris localisation using a guided filter" IET Image Processing, Volume 9, Issue 5, May 2015, p. 405 – 412.

[22] B. Arbab-Zavar and M.S. Nixon: *On Guided Model-Based Analysis for Ear Biometrics*. Computer Vision and Image Understanding (Elsevier). Vol.115, No.04, pp.487-502, 2011.

[23] D.O. Gorodnichy: *Evolution and Evaluation of Biometric Systems*. In Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defence Applications (CISDA). pp.1-8, Ottawa (Canada), 2009.

[24] A.K. Jain, R. Bolle, and S. Pankati, editors: *Biometrics: Personal Identification in Network Society*. Springer-Verlag, New York (USA), 1999.

[25] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo. Biometric authentication. Encyclopedia of Information Science and Technology, pages 346–354, 2008. [cit´e p. 8, 9, 158

[26] S. Liu and M. Silverman: A Practical Guide to Biometric Security Technology. IEEE IT Professional. Vol.03, No.01, pp.27-32, 2001.

[27] S. Prabhakar, S. Pankanti, and A.K. Jain: *Biometric Recognition: Security and Privacy Concerns*. IEEE Security & Privacy. Vol.01, No.02, pp.33-42, 2003.

[28] Anil.k. jain, P . Flynn, A. ross, « handbook of biometrics », Springer, 2007

[29] Anil k. jain stan Z. Li, « encyclopedia of biometrics », Springer 2009

[30] ISO/IEC 19795-1. Information technology – biometric performance testing and reporting – part 1 : Principles and framework, 2006.

[31] S. Prabhakar and A.K. Jain: *Decision-Level Fusion in Fingerprint Verification*. Pattern Recognition (Elsevier). Vol.35, No.04, pp.861-874, 2002.

[32] T. Fawcett: *An Introduction to ROC Analysis*. Pattern Recognition Letters (Elsevier). Vol.27, No.08, pp.861-874, 2006.

[33] A. Nait-Ali: *Hidden Biometrics: Towards using Biosignals and Biomedical Images for Security Applications*. In Proceedings of the 7th IEEE Workshop on Systems, Signal Processing and their Applications (WOOSPA). pp.352-356, Tipaza (Algeria), 2011.

[34] Manoj Kumar, M.; Puhan, N.B., "Off-line signature verification: upper and lower envelope shape analysis using chord moments," in Biometrics, IET , vol.3, no.4, pp.347-354, 2014.

[35] Aloui K., Biométrie du cerveau humain, PhD Thesis, Université Paris-Est Créteil, France, 2012.

[36] Basmajian JV, de Luca CJ. Muscles Alive – The Functions Revealed by Electromyography. The Williams & Wilkins Company; Baltimore, 1985.

[37] Aloui K., Nait-ali A., Nacer S., “A novel approach based Brain Biometrics: some preliminary results for Individual identification”, IEEE Workshop on Computational Intelligence in Biometrics and Identity Management, Paris, France, April 2011.

[38] Plataniotis K., Hatzinakos D., Lee J., “ECG biometric recognition without fiducial detection”, Proceedings of Biometrics Symposiums (BSYM ’06), Baltimore, MD, USA, September 2006.

[39] Chantaf S., Naït-ali A., Karasinski P., Khalil M., “ECG modeling using wavelet networks: application to biometrics”, International Journal of Biometrics, vol. 2, no. 3, pp. 236–248, 2010.

[40] Chantaf S., Biométrie par signaux physiologiques, PhD Thèse, Université Paris-Est Créteil, France, 2011.

[41] Biel L., Pettersson O., Philipson L., WIDE P., “ECG analysis: a new approach in human identification”, IEEE Transactions on Instrumentation and Measurement, vol. 50, no. 30, pp. 808–812, 2001.

[42] Manoj Kumar, M.; Puhan, N.B., "Off-line signature verification: upper and lower envelope shape analysis using chord moments," in Biometrics, IET , vol.3, no.4, pp.347-354, 2014.

[43] J. Jang, K. Kim, Y. Lee, "*Efficient Algorithm of Eye Image Check for Robust Iris Recognition System*", Computer Analysis of Images and Patterns, Springer, pp. 301-308, 2003.

[44] R. Sabourin, G. Genest et F. J. Prêteux, "Off-Line Signature Verification by Local Granulometric Size Distribution", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 9, pp. 976-988, 1997.

[45] C. Santos, E.J.R. Justino, F. Bortolozzi et R. Sabourin, "An Off-Line Signature Verification Method based on the Questioned Document Expert's Approach and a Neural Network Classifier", International Workshop On Frontiers in Handwriting Recognition (IWFHR), Tokyo (Japon), pp. 498-502., 2004.

[46] M. Wirotius, A. Seropian et N. Vincent, "Writer Identification from Gray Level Distribution", Proceedings of the International Conference on Document Analysis and Recognition (ICDAR'03), Edinburgh (Ecosse). pp. 1168-1172, 2003.

[47] R. Sabourin et G. Genest, "Définition et évaluation d'une famille de représentations pour la vérification hors-ligne des signatures", Traitement du Signal, vol. 12, n. 6, pp. 585-596, 1995.

[48] K. Tanabe, M. Yoshihara, H. Kameya et S. Mori, "Automatic signature verification based on the dynamic of pressure", Proceedings of the International Conference on Document Analysis and Recognition (ICDAR'01), pp. 1045-1049, 2001.

[49]. M. Tuceryan and A.K. Jain: *Texture analysis*. In C.H. Chen, L.F. Pau, and P.S.P. Wang, editors: *Handbook of Pattern Recognition and Computer Vision (2nd eds)*. World Scientific Publishing. pp.207-248, (Singafore),1998.

[50]. T. Ahonen, J. Matas, C. He, and M. Pietikäinen: *Rotation invariant image description with local binary pattern histogram fourier features.* In Proceedings of the 16th Scandinavian Conference (SCIA). Lecture Notes in Computer Science (Springer). Vol.5575, pp.61-70, Oslo (Norway), 2009.

[51]. E.R. Davies: *Introduction to texture analysis*. In M. Mirmehdi, X. Xie, and J. Suri, editors: *Handbook of texture analysis*. Imperial College Press. pp.1-31, London (UK), 2008.

[52]. M. Petrou and P.G. Sevilla: *Image Processing: Dealing with texture*. Wiley Online Library, 2006.

[53]. R.M. Haralick: *Statistical and structural approaches to texture*. Proceedings of the IEEE. Vol.67, No.5, pp.786-804, 1979.

[54]. L.V. Gool, P. Dewaele, and A. Oosterlinck: *Texture analysis anno 1983*. Computer Vision, Graphics, and Image Processing (Elsevier). Vol.29, No.3, pp.336-357, 1985.

[55]. H. Wechsler: *Texture analysis – A survey*. Signal Processing (Elsevier). Vol.2, No.3, pp.271-282, 1980.

[56]. B. Julesz: *Experiments in the visual perception of texture*. Scientific American. Vol.232, No.4, pp.34-43, 1975.

[57]. C.M. Wu and Y.C. Chen: *Statistical feature matrix for texture analysis*. Graphical Models and Image Processing (Elsevier). Vol.54, No.5, pp.407-419, 1992.

[58]. X. Xie and M. Mirmehdi: *A galaxy of texture features*. In M. Mirmehdi, X. Xie, and J. Suri, editors: *Handbook of texture analysis*. Imperial College Press. pp.375-406, London (UK), 2008.

[59]. T. Mäenpää and M. Pietikäinen: *Texture analysis with local binary patterns*. In C.H. Chen and P.S.P. Wang, editors: *Handbook of Pattern Recognition and Computer Vision (3rd eds)*. World Scientific Publishing. pp.197-216, (Singafore), 2005.

[60]. F. Tajeripour, M. Saberi, M. Rezaei, and S.F. Ershad: *Texture classification approach based on combination of random threshold vector technique and co-occurrence matrixes*. In Proceedings of the IEEE International Conference on Computer Science and Network Technology (ICCSNT). Vol.4, pp.2303-2306, Harbin (China), 2011.

[61]. Y. He and N. Sang: *Robust illumination invariant texture classification using gradient local binary patterns*. In Proceedings of the IEEE International Workshop on Multi-Platform/Multi-Sensor Remote Sensing and Mapping. pp.1-6, Xiamen (China), 2011.

[62]. N. Sebe, M.S. Lew: *Texture features for content-based retrieval*. In M.S. Lew, editor: *Principles of Visual Information Retrieval*. Springer-Verlag, pp.51-85, London (UK), 2011.

[63]. O.A.B. Penatti, E. Valle, and R.S. Torres: *Comparative study of global color and texture descriptors for web image retieval*. Journal of Visual Communication and Image Representation (Elsevier). Vol.23, No.2, pp.359-380, 2012.

[64]. R.O. Duda, P.E. Hart, and D.G. Stork: *Pattern classification (2nd eds)*. John Wiley & Sons, New York, 2001.

[65]. C.M. Bishop: *Pattern recognition and machine learning*. Springer-Verlag, New York, 2006.

[66]. D.J. Hand: *Clasiffier technology and the illusion of progress*. Statistical Science. Vol.21, No.1, pp.1-15, 2006.

[67]. T. Ojala, M. Pietikäinen, and D. Harwood: *A comparative study of texture measures with classifiction based on featured distribution*. Pattern Recognition (Elsevier). Vol.29, No.1, pp.51-59, 1996.

[68]. M. Varma and A. Zisserman: *A statistical approach to texture classification from single images*. International Journal of Computer Vision (Springer). Vol.62, No.1-2, pp.61-81, 2005.

[69]. E. Hayman, B. Caputo, M. Fritz, and J.O. Eklundh: *On the significance of real-world conditions for material classification*. In Proceedings of the 08th European Conference on Computer Vision (ECCV). Lecture Notes in Computer Science (Springer). Vol.3024, pp.253-266, Prague (Czech Republic), 2004.

[70]. J. Zhang, M. Marszalek, S. Lazebnik, and C. Schmid: *Local features and kernels for classification of texture and object categories: comprehensive study*. International Journal of Computer Vision (Springer). Vol.73, No.2, pp.213-238, 2007.

[71]. J.T. Todd: *The visual perception of 3D shape*. Trends in Cognitive Sciences. Vol.8, No.3, pp.115-121, 2004.

[72]. A. Lobay and D.A. Forsyth: Shape *from texture without boundaries*. Internationl Journal of Computer Vision (Elsevier). Vol.67, No.1, pp.71-91, 2006.

[73]. J.S.D. Bonet and P. Viola: *A non-parametric multi-scale statistical model for natural images*. Advances in Neural Information Processing (MIT Press). Vol.10, pp.773-779, 1997.

[74]. J. Portilla and E.P. Simoncelli: *A parametric texture model based on joint statistics of complex wavelet coefficients*. International Journal of Computer Vision (Springer). Vol.40, No.1, pp.49-70, 2000.

[75]. A.A. Efros and W.T. Freeman: *Image quilting for texture synthesis and transfer*. In Proceedings of the 28th Annual Conference on Computer Graphics and Interactive Techniques (SIGGRAPH). pp.341-346, New York (USA), 2001.

[76]. M.R. Turner: *Texture discrimination by Gabor functions*. Biological Cybernetics (Springer). Vol.55, No.2-3, pp.71-82, 1986.

[77]. A.C. Bovik, M. Clark, and W.S. Geisler: *Multichannel texture analysis using localized spatial filters*. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). Vol.12, No.1, pp.55-73, 1990.

[78]. A.K. Jain and F. Farrokhnia: *Unsupervised texture segmentation using Gabor filters*. Pattern Recognition (Elsevier). Vol.24, No.12, pp.1167-1186, 1991.

[79]. B.S. Manjunah and W.Y. Ma: *Texture features for browsing and retrieval of image data*. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). Vol.18, No.8, pp.837-842, 1996.

[80]. S.E. Grigorescu, N. Petkov, and P. Kruizinga: *Comparison of texture features based on Gabor filters*. IEEE Transactions on Image Processing. Vol.11, No.10, pp.1160-1167, 2002.

[81]. T. Leung and J. Malik: *Representing and recognizing the visual appearance of materials using three-dimensional textons*. International Journal of Computer Vision (Springer). Vol.43, No.1, pp.29-44, 2001.

[82]. S. Lazebnik, C. Schmid, and J. Ponce: A *sparse texture representation using local affine regions*. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). Vol.27, No.8, pp.1265-1278, 2005.

[83]. C. Schmid, R. Mohr, and C. Bauckhage: *Evaluation of interest point detectors*. International Journal of Computer Vision (Springer). Vol.37, No.2, pp.151-172, 2000.

[84]. K. Mikolajczyk, Y. Tuytelaars, C. Schmid, A. Zisserman, J. Matas, F. Schaffalitzky, T. Kadir, and L.V. Gool: *A comparison of affine region detectors*. International Journal of Computer Vision (Springer). Vol.65, No.1-2, pp.43-72, 2005.

[85]. E. Nowak, F. Jurie, and B. Triggs: *Sampling strategies for bag-of-features image classification*. In Proceedings of the 9th European Conference on Computer Vision (ECCV). Lecture Notes in Computer Science (Springer). Vol.3954, pp.490-503, Graz (Austria), 2006.

[86]. T. Tuytelaars and C. Schmid: *Vector quantizing feature space with a regular lattice*. In Proceedings of the 11th IEEE International Conference on Computer Vision (ICCV). pp.1-8, Rio de Janero (Brazil), 2007.

[87]. T. Ahonen, A. Hadid, and M. Pietikäinen: *Face description with local binary patterns: Application to face recognition*. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). Vol.28, No.12, pp.2037-2041, 2006.

[88]. J. Vogel and B. Schiele: *Semantic modeling of natural scenes for content-based image retrieval*. International Journal of Computer Vision (Springer). Vol.72, No.2, pp.133-157, 2007.

[89]. M. Mikolajczyk and C. Schmid: *A performance evaluation of local descriptors*. IEEE Transactions on Pattern Analysis and Machine Intelligence (PAMI). Vol.27, No.10, pp.1615-1630, 2005.

[90]. N. Dalal and B. Triggs: *Histograms of oriented gradients for human detection*. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Vol.1, pp.886-893, San Diego (USA), 2005.

[91]. M. Heikkilä, M. Pietikäinen, and C. Schmid: *Description of interest regions with local binary patterns*. Pattern Recognition (Elsevier). Vol.42, No.3, pp.425-436, 2009.

[92]. D.G. Lowe: *Object recognition from local scale-invariant features*. In Proceedings of the 7th IEEE International Conference on Computer Vision (ICCV). Vol.02, pp.1150-1157, Kerkyra (Greece), 1999.

[93]. H. Bay, T. Tuytelaars, and L.V. Gool: *SURF: speeded up robust features*. In Proceedings of the 9th European Conference on Computer Vision (ECCV). Lecture Notes in Computer Science (Springer). Vol.3951, pp.404-417, Graz (Austria), 2006.

[94]. J. Kannala and E. Rahtu: *BSIF: binarized statistical image features*. In Proceedings of the 21st International IEEE Conference on Pattern Recognition (ICPR). pp.1363-1366, Tsukuba (Japan), 2012.

[95]. Vargas, J.F., Ferrer, M.A., Travieso, C.M. and Alonso, J.B. (2011) 'Off-line signature verification based on grey level information using texture features', Pattern Recognit., Vol. 44, No. 2, pp.375–385.

[96]. Ferrer, M.A., Alonso, J.B. and Travieso, C.M. (2005) 'Offline geometric parameters for automatic signature verification using fixed-point arithmetic', *IEEE Trans. Pattern Anal. Mach. Intell.*, Vol. 27, No. 6, pp.993–997.

[97]. Ortega-Garcia, J., Fierrez-Aguilar, J., Simon, D., Gonzalez, J., Faundez-Zanuy, M., Espinosa, V. et al. (2003) 'MCYT baseline corpus: a bimodal biometric database', Vision, Image and Signal Processing, IEE Proceedings, Vol. 150, pp.395–401.

[98]. Serdouk, Y., Nemmour, H. and Chibani, Y. (2016) 'New off-line handwritten signature verification method based on artificial immune recognition system', Expert Systems with Applications, DOI: 10.1016/j.eswa.2016.01.001.

[99]. Shekar, B.H. and Bharathi, R.K. (2014) 'Off-line signature verification based on principal component analysis and multi-layer perceptions', *Advances in Intelligent Systems and Computing*, Vol. 235, Springer International Publishing, Switzerland, DOI: 10.1007/978-3-319-01778-5_11.

[100]. Yilmaz, M.B. (2015) Offline Signature Verification with User-Based and Global Classifiers of Local Features, PhD dissertation, Sabancı University.

[101]. Soleimani, A., Araabi, B.N. and Fouladi, K. (2016) 'Deep multi task metric learning for offline signature verification', Pattern Recognition Letters, DOI: 10.1016/j.patrec.2016.05.023.

ANNEXE

Notions fondamentales sur la classification, les k-plus proches voisins (k-NN)

1. Introduction à la classification

La classification, en général, se réfère au classement ou au groupement d'éléments de données dans des ensembles similaires. Cette information est souvent utile dans l'étape d'analyse pour n'importe quel système de traitement du signal ou de données. La classification a deux significations distinctes. Nous pouvons recevoir une série d'observations avec l'objectif d'établir l'existence des classes ou des groupes dans les données. Nous pouvons savoir avec certitude qu'il ya tant de classes, et l'objectif consiste à instaurer une règle selon laquelle nous pouvons classer une nouvelle observation dans l'une des classes existantes. Le premier type est connu comme l'apprentissage non supervisé et le second comme l'apprentissage supervisé.

La classification d'image est en général similaire à la classification des données, mais elle peut être différente en fonction de l'application dans laquelle elle est utilisée. La classification est souvent la dernière étape d'un processus général de reconnaissance des formes. Il s'agit généralement d'un tri d'objets dans une image ou plusieurs images dans des classes distinctes. Typiquement, l'image est segmentée ou traitée afin d'isoler les différents objets ou formes les uns des autres, et les différents objets ou images sont étiquetés. Une étape d'extraction de caractéristiques (attributs) réduit les données en mesurant certaines propriétés ou caractéristiques des objets ou images étiquetés. Ces attributs sont ensuite transmis à un classificateur qui évalue ces caractéristiques et prend une décision relative à la classe de chaque objet ou image. La qualité de l'image acquise dépend de la résolution, la sensibilité, la bande passante et du rapport signal sur bruit du système d'imagerie. Un prétraitement tel que le filtrage est souvent nécessaire. Les attributs extraits peuvent être transformés dans un espace de caractéristiques alternative afin de produire de meilleures caractéristiques, avant d'être envoyés au classificateur.

L’objectif visé dans notre cas par la classification est de pouvoir distinguer entre N classes correspondantes et d’attribuer l‘identité d’un individu inconnu à la classe correspondante (N: le nombre total des individus dans la base de données du système biométrique). Cette méthode est basée sur l’apprentissage suivi de la classification. La phase d’apprentissage correspond à l’extraction d’attributs caractéristiques à partir de l’image dans l’ensemble d'apprentissage. La classification est la phase au cours de laquelle sont utilisés les attributs précédemment extraits afin d’atteindre l’objectif initial.

1.1. Classification non-supervisée

Cette méthode de classification est aussi appelée "*classification automatique*", (Clustering en anglais) ou encore "*regroupement*". Aucune information à priori sur les classes n'est connue. Nous cherchons donc à regrouper les différents exemples en fonction de la valeur de leurs caractéristiques de manière à créer des classes homogènes. Nous supposons que nous disposons d'un ensemble d'objets que l'on note par caractérisé par un ensemble de caractéristiques "*D*", l'objectif du regroupement est de trouver les groupes auxquels appartient chaque objet "*x*" que nous notons par Ce qui revient à déterminer une fonction notée "*Ys*" qui associe à chaque élément de *X* un ou plusieurs éléments de *C*. Il faut pouvoir affecter une nouvelle observation à une classe. Les observations disponibles ne sont pas initialement identifiées comme appartenant à telle ou telle population. L'absence d'étiquette de classe est un lourd handicap qui n'est que très partiellement surmontable. Ce procédé nécessite généralement de fixer au préalable le nombre de classes désirées, que ce soit de manière empirique ou automatique. Parmi les méthodes non-supervisées les plus utilisées, nous citons deux types d'approches: les centres mobiles (*k*-means) et la classification hiérarchique.

1.2. Classification supervisée

Dans cette méthode de classification, nous disposons déjà d'exemples dont la classe est connue et étiquetée. Une information sur les données à traiter est disponible et utilisée pour entrainer le processus de classification, cela constitue la phase d'apprentissage du modèle. Cette information appelée ensemble d'apprentissage est généralement constituée d'un ensemble d'individus {caractéristiques, classe associée}. Dans le cas de la classification des identités, l'ensemble d'apprentissage est constitué d'un ensemble d'identités "types". Chaque individu est donc composé du couple (caractéristiques de l'identité, classe associée). Cet ensemble est alors appris par un algorithme classique de classification supervisée parmi lesquels nous citons: les *k*-plus proches voisins (*k*-NN), les réseaux de neurones, les séparateurs à vaste marge (SVM), etc. Une fois la phase d'apprentissage réalisée, l'algorithme de classification est alors utilisé afin de déterminer la classification d'un ensemble d'individus tests composé d'un grand nombre d'échantillons. Cette approche de classification d'identités supervisée reste un domaine de recherche très actif. Dans notre analyse des données biométriques, nous nous intéressons à cette approche pour attribuer une identité inconnue à son propre individu. Dans ce qui suit, nous allons décrire sommairement les classificateurs que nous avons utilisés dans le cadre de ce travail.

2. *k*-plus proches voisins (*k*-NN)

L'algorithme des *k* plus proches voisins (noté *k*-NN) fait partie des méthodes de classification les plus couramment utilisées. Il permet de traiter des nuages de points non linéairement séparables. Cette approche a l'avantage d'être à la fois facile

et efficace. L'algorithme *k*-NN figure parmi les algorithmes simples d'apprentissage artificiel. Dans un contexte de classification d'une nouvelle observation *x*, l'idée fondatrice est de faire voter les plus proches voisins de cette observation. La classe de *x* est déterminée en fonction de la classe majoritaire parmi les *k* plus proches voisins de l'observation *x.* La méthode *k*-NN est donc une méthode basée sur le voisinage, non-paramétrique; ceci signifiant que l'algorithme permet de faire une classification sans faire d'hypothèse sur la fonction qui relie la variable dépendante aux variables indépendantes.

2.1. Méthode *1*-NN

La méthode du plus proche voisin est une méthode non paramétrique où une nouvelle observation est classée dans la classe d'appartenance de l'observation de l'échantillon d'apprentissage qui lui est la plus proche, vis-à-vis des covariables utilisées. La détermination de leur similarité est basée sur des mesures de distance. Formellement, soit *L* l'ensemble de données à disposition ou échantillon d'apprentissage:

$$L = \{(y_i, x_i), i = 1, \dots, n_L\} \quad \text{(A.1)}$$

Où : y (1, ….. c) désigne la classe de l'individu "*i"* et le vecteur représente les variables prédicatrices de l'individu "*i*". La détermination du plus proche voisin est basée sur une fonction distance notée.

La distance *euclidienne* ou *dis-similarité* entre deux individus caractérisés par "*p*" Co-variables est définie par:

$$d\left((x_1, x_2, \dots., x_p), (u_1, u_2, \dots, u_p)\right) = \sqrt{(x_1 - u_1)^2 + (x_2 - u_2)^2 + \ \dots + (x_p - u_p)^2}$$

Ainsi, pour une nouvelle observation (y,x) le plus proche voisin ($y_{(1)}$, $x_{(1)}$) dans l'échantillon d'apprentissage est déterminé par:

$$d(x, x_{(1)} = min_i(d(x, x_{(1)})) \quad \text{(A.3)}$$

Alors $y=y_{(1)}$, la classe du plus proche voisin, est sélectionnée pour la prédiction de *y*. Les notations $x_{(j)}$ et $y_{(j)}$ représentent respectivement le plus $j^{éme}$ proche voisin de *x* et sa classe d'appartenance. La distance euclidienne est définie comme suit:

$$d(x_i, x_j) = \left[\sum_{s=1}^{p} (x_{is} - x_{js})^2\right]^{\frac{1}{2}} \quad \text{(A.4)}$$

2.2. Méthode *k*-NN

La méthode des *k* plus proches voisins est une extension de l'idée précédente, qui est largement et communément utilisée en pratique. La plus proche observation n'est plus la seule observation utilisée pour la classification. Nous utilisons désormais les *k* plus proches observations. Ainsi la décision est en faveur de la classe majoritairement représentée par les *k* voisins. Soit K_A le nombre d'observations issues du groupe des plus proches voisins appartenant à la classe *A*.

$$\sum_{A=1}^{c} K_A = k$$

Ainsi une nouvelle observation est prédite dans la classe *l* avec $l = max_A(K_A)$.

Cela évite que la classe prédite ne soit déterminée seulement à partir d'une seule observation. La mise en œuvre de cette technique ne dépend que du paramètre *k*: pour $k = 1$, nous utilisons la méthode du seul plus proche voisin comme technique locale maximale, pour $k = ln$, nous utilisons la classe majoritaire sur l'ensemble intégral des observations.

Le paramètre *k* doit être déterminé par l'utilisateur: $k \in N$. En classification binaire, il est utile de choisir *k* impair pour éviter les votes égalitaires. Le meilleur choix de *k* dépend du jeu de données. En général, les grandes valeurs de *k* réduisent l'effet du bruit sur la classification et donc le risque de sur-apprentissage, mais rendent les frontières entre classes moins distinctes. Il convient donc de faire un choix de compromis entre la variabilité associée à une faible valeur de *k* contre un sur-lissage (c'est à dire, gommage des détails) pour une forte valeur de *k*. Un bon *k* peut être sélectionné par diverses techniques heuristiques, par exemple, la validation-croisée.

La Figure A présente cette méthode avec $k = 5$, pour des points image projetés dans un espace d'attributs de dimension $d = 2$ et pour un nombre de classe $NC = 2$. Pour classer l'image-test, dont le point représentatif dans le sous-espace d'attributs est rouge, nous cherchons tout d'abord les 5 points prototypes les plus proches (au sens de la distance Euclidienne). Ces images sont celles présentées par des flèches avec le point représentatif de l'image à classer. Il y a 3 images appartenant à la classe C1 et 2 images appartenant à la classe C2. L'image-test est donc assignée à la classe C1.

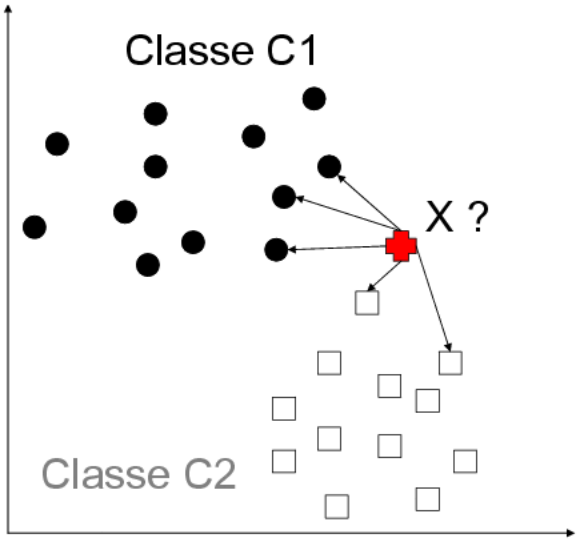


Fig. A : Illustration de la méthode des k-plus proches voisins (k-NN) avec k=5.

Pour chaque image, nous obtenons un taux de classification qui est estimé par le rapport entre le plus proche voisin "*ki*" de la classe correcte et le nombre total des plus proches voisins *k*:

$$P\left(\frac{C_i}{x}\right) = \frac{K_i}{K}$$

$P\left(\frac{C_i}{x}\right)$: Peut être considéré comme la probabilité a posteriori d'une instance *x* d'appartenir à la classe *Ci* selon la règle vote du *k*-NN. L'intérêt de ce type de classificateur est qu'il ne nécessite pas de réglage des paramètres préalables autres que le nombre des voisins "*k*".


الحمد لله رب العالمين