REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département de Génie Electrotechnique et Automatique

Réf:……/2021

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER Académique**

Domaine: Sciences et Technologie

Filière: Automatique

Spécialité: Automatique et informatique industriel

Par: (Doufa Ismahane et Tadjine Abdelkhaleq)

Thème

Titre du mémoire

Identification biométrique des personnes par signature manuscrite

Soutenu publiquement, le 14/07/2021, devant le jury composé de:

Mme.BOUCERREDJ Leila	MCA	Univ.Guelma	Encadreur
M.MOUSSAOUI Abdelkrim	Professeur	Univ.Guelma	Président
M .BABOURI Abdesselam	Professeur	Univ.Guelma	Examinateur

Année Universitaire: 2021/2022

Remerciement

Tout d'abord, nous remercions Dieu Tout Puissant de nous avoir donné la force, la volonté,et le privilège d'étudier et de réaliser ce travail

Nous tenons à remercier sincèrement notre encadreur Madame boucerredj laila , s'est toujours montré l'écoute et était très disponible tout au long de la réalisation de ce mémoire, ainsi pour l'inspiration et l'aide.

Nous remercions les membres du jury pour leurs éminentes contributions à l'évaluation de Ce projet.

Enfin, nous adressonsnos plus sincères Remerciements à tous nos proches et amis, qui ont toujours soutenu et encouragé au cours de la réalisation de ce travail.

Merci à toutes et tous.

Dédicace

A ma gentile mère et mon cher père qui m'ont tant donné à faire

moi ce que je suis.

A mon cher frère et mes chères soeurs avec

Tous mes meilleurs voeuxLa vie pratique.

A tous mes collègues de Et mon invité, je voudrais mentionner chacun d'Abd elghani Amayrai – Abdelghani boukria

- Boughada Gharib, les personnes respectées qui m'ont soutenu et guidé quand j'en avais besoin.

pour tous ceux que j'aime,

Je dédie ce travail.

abdelkhaleq

Dédicace

A ma mère, que dieu lui fasse miséricorde et ma pére qui m'ont tant donné pour faire de moi ce que je suis.

A mon fiancé bien-aimé Samir.

A mon cher frère et mes chères sœurs, avec Tous mes souhaits de succès dans leur vie.
A tous mes chers amis
A tous mes respectueux collègues.
A tous ceux que j'aime,

Je dédie ce travaille.

Ismahane

Résumé

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu. Elle est 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, 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.

Notre travail consiste à la mise au point d'un programme destiné à identifier un individu par signatures manuscrites hors ligne. Nous utilisant la méthode «LBQ et LBP», qui se base sur une analyse des informations acquise dans la méthode de prétraitement, ensuite l'extraction des caractéristiques biométriques et puis calculer le taux de reconnaissanceen utilisant le logiciel Matlab pour visualiser les résultats à vouloir obtenir.Après, Les résultats sont pris et discutés.

Mots-clés: Biométrie,signature manuscrite, processus d'indentification, les modèles binaires locaux (LBP), Local Phase Quantization (LPQ).

ملخص

كان التوقيع بخط اليد هو الأسلوب الأكثر استخدامًا لعدة قرون. إنها أكثر وسائل المصادقة الحيوية استخدامًا والمقبولة. يمثل التوقيع المكتوب بخط اليد للفرد حلاً وسطًا جيدًا، في حين أنه يمكن الاعتماد عليه نسبيًا، فمن السهل الحصول عليه، ومقبول اجتماعيًا كوسيلة للاعتراف. التوقيع هو وسيلة تستخدم لفترة طويلة، لتوثيق المستندات، لجعل الأشخاص مسؤولين عن الالتزامات (العقود، وما إلى ذلك). لذلك يتم التعرف على التوقيع كأسلوب تحقق مرتبط بهوية الشخص.

الهدف من هذا العمل هو تطوير برنامج لتحديد هوية الفرد من خلال التوقيعات المكتوبة بخط اليد في وضع عدم الاتصال. استخدمنا طريقة "LBQو LBP"، والتي تعتمد على تحليل المعلومات المكتسبة في طريقة المعالجة المسبقة، ثم استخراج الخصائص الحيوية ثم حساب معدل التعرف باستخدام برنامج Matlabلمعالجة النتائج المراد الحصول عليها. بعد ذلك، يتم أخذ النتائج ومناقشتها.

الكلمات المفتاحية: القياسات الحيوية، التوقيع بخط اليد، عملية تحديد الهوية، النماذج الثنائية المحلية (LBP)، تكميم الطور المحلي (LPQ).

Summary

The handwritten signature has been the most widely used method for several centuries. It is the most widely used and accepted biometric means of authentication. The handwritten signature of an individual represents a good compromise, while being relatively reliable, it is easy to acquire, socially accepted as a mode of recognition. The signature is a means used for a long time, to authenticate documents, to make people responsible for commitments (contracts, etc.). The signature is therefore recognized as a validation mode associated with the identity of a person.

The aim of our work is to develop a program to identify an individual by handwritten signatures offline. We used the "LBQ and LBP" method, which is based on an analysis of the information acquired in the preprocessing method, then extracting the biometric characteristics and then calculating the recognition rate using Matlab software to visualize the results to be obtained. Afterwards, the results are taken and discussed.

Keywords: Biometrics, handwritten signature, identification process, local binary models (LBP), Local Phase Quantization (LPQ).

Sommaire :

Liste de figures

Liste de figures

Liste de tableaux

Liste des abréviations

PCA : Analyse composant principale

LDA : Analyse Discriminante Linéaire

KPCA : kernel Analyse composant principale

KNN : k near est Neighbors.

DoG : Différence of Gaussiens

CNIL:la Commission Nationale de l'Informatique et des Libertés

EER : Equal Error Rate

FAR : False Accepte Rate (le taux de faux acceptés)

FRR : False Rejection Rate (le taux de vrais rejetés)

LBP : Local Binary Pattern

LPQ : Local Phase Quantization

BDD : Base de données

Introduction générale

Nous vivons actuellement une véritable révolution d'accès à l'information, dans tous les domaines de l'activité humaine. En fait, la sécurité des systèmes d'information est devenue un domaine de recherche d'une très grande importance, l'identification de l'individu est essentielle pour assurer la sécurité des systèmes et organisations, la conception d'un système d'identification fiable, efficace et puissant est une étape nécessaire. Dans ce sens, la biométrie est un exemple pratique parce qu'elle est de plus en plus présente dans la vie quotidienne: au travail des opérations bancaires, l'accès à certains endroits militaires ou industriels.

La biométrie désigne l'ensemble des technologies de reconnaissance physiologiques et comportementales des individus telles que: l'iris, la voix, les empreintes digitales, le visage, la signature, l'empreinte palmaire….etc.

Dans les applications de contrôle d'accès, la biométrie permet d'apporter un niveau de sécurité supérieur en ce qui concerne des accès logiques (ordinateurs, comptes bancaires, etc.) ou des accès physiques (bâtiments sécurisés, aéroports, laboratoires etc.). La biométrie regroupe deux axes principaux : une identification (reconnaissance) et une authentification.

Dans le cas d'identification, le système biométrique demande une information biométrique et la compare avec chaque information stockée dans la base de données. Alors que pour l'authentification l'utilisateur annonce son identité par une information biométrique, et le système compare les données obtenues à partir de l'information entrée avec la donnée enregistrée.

Il existe plusieurs techniques biométriques qui sont utilisées dans le contrôle d'accès. Chaque technique biométrique a ses avantages et inconvénients. Dans le cadre de ce travail, notre objectif consiste à réaliser un système de reconnaissance biométriques basé sur la signature en tant que modalité biométrique, le choix de cette modalité a été motivé par ce qu'elle est considérée comme une modalité émergente dans ce domaine, entité unique, stable dans le temps et structure riche d'information. Le présent document est organisé comme suit :

Le premier chapitre : continent des généralités sur la biométrie, dans ce chapitre nous avons introduit les concepts des systèmes biométriques, leurs modalités et leurs différentes applications.

Le deuxième chapitre : consacré à un aperçu sur la reconnaissance des formes. Tout d'abord, nous présentons les différents algorithmes qui utilisés dans les systèmes biométriques. Également, ces algorithmes se devisent en trois catégories : les algorithmes de prétraitement, les algorithmes extraction de caractéristiques et les algorithmes de classification.

Dans le troisième chapitre : nous présentons plus en détails les concepts de l'authentification par signature manuscrite et les travaux réalisés dans ce domaine.

Finalement, le quatrième chapitre est consacré pour le processus de notre programme d'identification des signatures manuscrites et les résultats expérimentaux basé sur la méthode LBP et LPQ sous le logiciel Matlab. Et dernièrement une partie comparative entre ces méthodes est illustrée dans ce chapitre. Nous terminons ce mémoire par une conclusion générale.

Chapitre 01
Généralités sur la biométrie

I.1. Introduction

Dans nos jours, la sécurité des individus est devenue un souci majeur, puisque le besoin de se protéger augmente jour après jour. Les méthodes de sécurité classiques des systèmes d'informations ne sont pas efficaces. En effet, il existe deux manières de cette sécurité [1].La première repose sur la connaissance de la personne comme « un mot de passe » ou « un code PIN»; dans ce cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. La seconde est basée sur ce que possède la personne comme « un badge » ou « une carte à puce »; dans ce cas, le badge peut être perdu ou volé. Pour contourner cette limitation, un autre moyen de sécurité a été développé qui permet d'utiliser, non pas l'information qu'un individu possède ou connait, mais une information intrinsèque à cette personne. Cette nouvelle façon d'identification des individus est dite: « la biométrie ». Dans ce chapitre, nous commençons par la présentation de quelques généralités sur la biométrie telles que: sa définition, ses caractéristiques, et leur domaines d'application. Ensuite, nous définissons les systèmes biométriques et le principe général de ses fonctionnements. A la fin, nous terminons le chapitre par la présentation de quelques modalités biométriques et une comparaison entre ces modalités.

I.2. Généralités sur la biométrie

I.2.1. Définition

Le terme "biométrie" provient des mots grecs «bios» qui veut dire la vie et du mot «métrique» qui signifie mesure [2]. Donc, la biométrie désigne la technique qui permet d'associer une identité à un individu grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques physiques ou comportementales de cette personne, qui sont préalablement enregistrées dans une base de données (ex, empreintes digitales, visage, voix, etc.) [3].

I.2.2. Caractéristiques biométriques

Le choix des caractéristiques physiques est important. Il faut qu'elles soient toutes à la fois [2,4]:

- Universelles : existent chez tous les individus.

- Uniques : possibilité de différencier un individu par rapport à un autre.

- Permanentes : stables et invariantes au cours du temps.

- Enregistrables : possibilité d'enregistrer les caractéristiques d'un individu à l'aide d'un capteur approprié qui ne cause aucun dérangement pour l'individu.

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

I.2.3. Domaines d'applications

Le champ d'application de la biométrie est très vaste. En effet, tous les domaines qui nécessitent de vérifier ou déterminer l'identité d'une personne sont concernés. D'où les applications de la biométrie peuvent être divisées en trois groupes principaux [5]:

- Applications commerciales: telles que l'ouverture d'un réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, les cartes de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

- Applications gouvernementales: telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

- Applications légales: telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc.

I.3. Les systèmes biométriques

Un système biométrique est un système de reconnaissance d'individus qui permet d'identifier une personne sur la base de ses caractères physiologiques ou comportementaux [6]. Selon le contexte de l'application, un système biométrique comporte toujours deux phases de fonctionnement (Figure I.1):

I.3.1. La phase d'enrôlement ou d'apprentissage

Cette phase consiste à créer un modèle biométrique d'un individu qui doit être une référence pour la phase de reconnaissance. Pour ce faire, les caractéristiques biométriques de l'individu sont mesurées par un capteur biométrique, puis représentées sous forme numérique et enfin stockées dans une base de données. Pour assurer une certaine puissance du système aux variations temporelles de données, plusieurs échantillons d'acquisitions de la même donnée peuvent être réalisés. Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue « hors-ligne » [7].

I.3.2. La phase de reconnaissance

La reconnaissance peut être une vérification ou une identification:

❖ Le mode de vérification ou d'authentification :

La vérification est une comparaison "un à un", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisies avec le modèle biométrique de cette personne stocké dans la base de données du système [6].

❖ Le mode d'identification :

L'identification permet d'établir l'identité d'une personne à partir d'une basse de donnée. En d'autres termes, elle répond à des questions de type: « Qui suis-je ? », il s'agie d'une comparaison (un a N).

A ces deux modes de fonctionnement du système s'ajoutent souvent les deux processus suivants [6]:

- La mise à jour: le système biométrique peut périodiquement corriger le gabarit de référence lors d'un contrôle de façon à prendre en compte l'évolution de la donnée biométrique de la personne.
- La fin de vie: le gabarit et autres données de référence propres à la personne sont détruites pour prendre en compte sa suppression du système de contrôle centralisé.

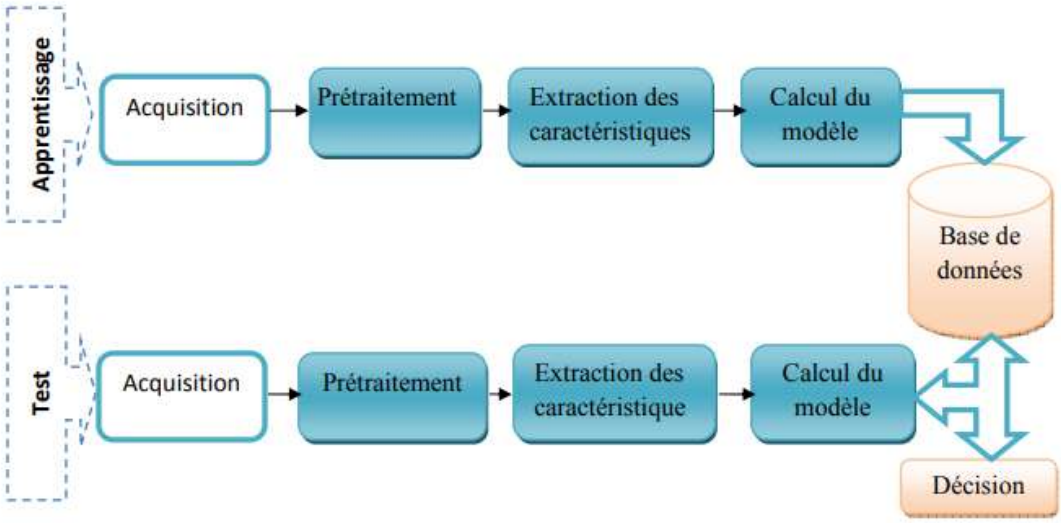


Figure I.1 : Architecture d'un système de reconnaissance biométrique.

Tout système biométrique comporte deux processus qui se chargent à réaliser les opérations d'enregistrement et de tests:

- Processus d'enregistrement: Ce processus a pour but d'enregistrer les caractéristiques des utilisateurs dans la base de données.
- Processus de tests (identification /vérification): Ce processus réalise l'identification ou la vérification d'une personne. Dans chacun des deux processus précédents, le système exécute quatre opérations fondamentales, à savoir [2]:

L'acquisition: Cette phase consiste à utilisé un capteur pour acquérir une caractéristique spécifique de l'individu, plusieurs processus peuvent être utilisés pour l'acquisition tels que: le microphone dans le cas de la voix.

L'extraction: Après l'acquisition d'une image, nous réalisons l'extraction des caractéristiques dont le processus d'authentification a besoin. Donc, ce module sert à traiter l'image afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur, qui peuvent être ensuite utilisées pour reconnaitre les personnes.

La classification (comparaison): En examinant les modèles stockés dans la base de données (vecteurs), les caractéristiques biométriques extraites sont comparées avec ce vecteur et en marquant le degré de similitude (différence ou distance).

La décision: En ce qui concerne l'authentification, la stratégie de décision nous permet de vérifier l'identité affirmée par un utilisateur ou déterminer l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) vecteur(s) stocké(s).

I.4. Les modalités biométriques

La biométrie est basée sur les caractéristiques biométriques de l'individu, ces caractéristiques peuvent être encore classées en trois grandes catégories [6]:

- L'analyse morphologique ou physique (empreintes digitales, forme de la main, traits du visage,...).

- Les traces biologiques (odeur, ADN,...).

- L'analyse comportementale (dynamique du tracé de la signature, frappe sur un clavier…)

I.4.1. Biométrie physique

I.4.1.1 Empreintes digitales: La reconnaissance des individus par empreintes digitales est la technique biométrique la plus utilisée. Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minuties) et constituent un motif unique, universel et permanant, comme montré dans la Figure (I.2). Les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes.

Il existe plusieurs types de minuties. Ce type de technique biométrique est utilisé par les institutions financières pour leurs clients et se trouve en même temps dans les hôpitaux, les écoles, les aéroports…etc. [3,8].

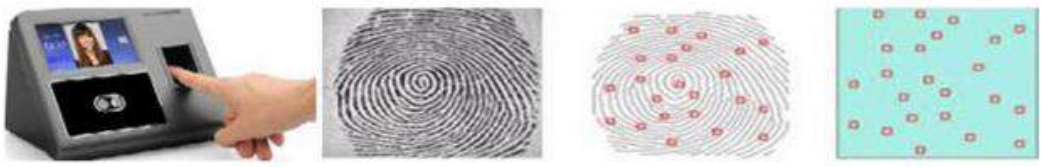


Figure I.2: Système biométrique basé sur les empreintes digitales.

- **Avantage :**

  - Coût faible.

  - Taille du lecteur biométrique n'est pas volumineuse.

  - Système reste très simple à mettre en place.

  - Utilisation facile.

- **Inconvénients :**

  -L'inscription de toutes les parties concernées, ce qui peut poser un problème dans le cas où une maladie soit physique ou psychologique [9].

I.4.1.2 Visage: Nos visages sont des objets complexes avec des traits qui peuvent varier dans le temps, comme montré dans la Figure (I.3). L'écart entre les deux yeux, l'écartement des narines ou encore la largeur de la bouche peuvent permettre d'identifier un individu. Cette méthode doit pouvoir tenir compte de certain changement de la physionomie (lunettes, barbe, chirurgie esthétique) et de l'environnement (conditions d'éclairage). Parfois, il est impossible de différencier deux jumeaux. [9 ,10]

Figure I.3 : Le visage de l'être humain en tant que modalité biométriques.

- **Avantage :**
  - Technique acceptée par le public.
  - Fonctionnement simple, peut être effectué à distance, et sans coopération de l'utilisateur.
  - Technique peu coûteuse et peut s'appuyer sur l'équipement d'acquisition des images actuel.
- **Inconvénients :**
  - Les vrais jumeaux ne sont pas différentiables.
  - Les changements physiques peuvent tromper le système.
  - La technique est trop sensible a l'environnement (éclairage, l'angle de l'appareil photos…etc.).

I.4.1.3 Iris: L'iris est une région sous forme d'anneau, située entre la pupille et le blanc de l'œil, elle est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. La reconnaissance de l'iris a été développée dans les années 80, elle est donc considérée comme une technologie récente. L'image de l'iris est capturée par un appareil qui contient une caméra infrarouge, lorsque la personne se place à une courte distance de l'appareil (Figure I.4) [9].

Figure I.4: système biométrique basé sur l'Iris.

- **Avantage :**
  - Les vrais jumeaux sont non confondus.

- Les structures de l'iris restent stables durant toute la vie.
- Grande quantité d'informations contenue dans l'iris.

Inconvénients :

- L'acquisition des images exige une certaine formation et de la pratique.
- La fiabilité diminue proportionnellement en fonction de la distance entre l'œil et la camera.
- Les gens ont du mal à accepter cette biométrie.

I.4.1.4 Empreintes des articulations des doigts: C'est une technologie biométrique basée sur la surface arrière du doigt, elle contient des caractéristiques distinctives telles que les lignes principales, les lignes secondaires et les crêtes, qui peuvent être extraites à partir des images à basse résolution (Figure I.5). La main contient plusieurs doigts, pour cela, il faut conserver les informations à chaque doigt pour une reconnaissance précise dans le domaine d'identification [8].

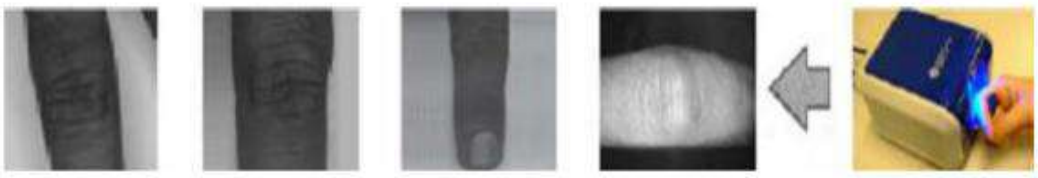


Figure I.5 : système biométrique basé sur les articulations des doigts.

Avantage :

- Technique acceptable.
- Utilisation simple.
- En combinant tous les doigts de la main, il est possible d'établir un système biométrique robuste et précis.

Inconvénients :

- Très similaire pour les jumeaux.
- Problème dans le cas d'une coupure d'un doigt.
- Pose incorrecte du doigt sur le lecteur provoque une grande erreur.

I.4.1.5 Empreinte palmaire: Cette technique utilise la surface intérieure de la paume pour l'identification et/ou la vérification des personnes (Figure I.6). Elle est bien adaptée pour les systèmes à moyenne sécurité telle que le contrôle d'accès physique ou logique [8].

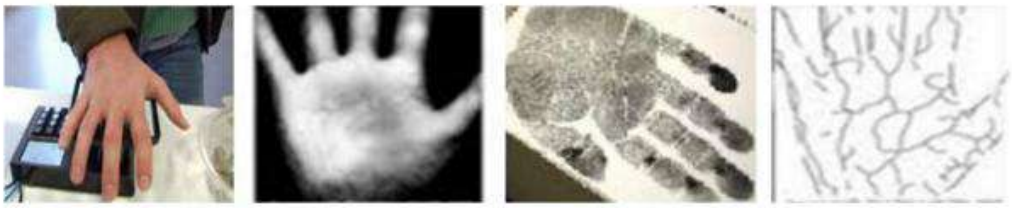


Figure I.6 : Système biométrique basé sur les empreintes palmaires.

- **Avantage :**
  - Facile à utiliser, elle a une grande acceptation par le public.
  - Après l'utilisation, la main reste propre et ne laisse aucune trace.
  - Presque disponible par tous les individus.
- **Inconvénients :**
  - Peut être similaire dans des jumeaux ou dans des membres de la famille.
  - Elle n'est pas permanente en termes de changements tels que: le vieillissement naturel.

I.4.2. Biométrie comportementale

I.4.2.1 Voix: La voix humaine varie d'une personne à une autre et peut se constituer de composantes physiologiques et comportementales. L'identification par la voix est basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) et utilisées dans la synthèse du son [7]. La reconnaissance des locuteurs est plus utilisée par les téléphones, les corps policiers, les hôpitaux…etc. (Figure I.7).

Figure I.7: Système biométrique basé sur la voix.

- **Avantage :**
  - Très bien acceptée parce que la voix est un signal naturel à produire.
  - La dynamique des ondes produites est unique.
- **Inconvénients :**
  - Biométrie moins permanente.

- Les caractéristiques comportementales changent avec le temps.
- Possibilité de fraude par enregistrement.
- Sensibilité aux bruits lors d'acquisition.

I.4.2.2 Frappe dynamique sur le clavier: C'est un système de reconnaissance d'un individu basé sur la manière de ses écritures par un dispositif logiciel qui calcule la vitesse de la frappe, la suite des lettres, le temps de frappe et la pause entre chaque mot [7] (Figure I.8).

Figure I.8 : Système biométrique basé sur la frappe dynamique sur le clavier.

- **Avantage :**
  - Forte acceptation par l'utilisateur.
  - Sécurité bien précise.
- **Inconvénients :**
  - N'est pas plus pratique.
  - N'est pas permanente durant toute la vie (âge, émotion, fatigue).

I.4.2.3 Démarche: Chaque personne a une façon particulière de marche, nous pouvons identifier les individus à partir de la nature du mouvement des jambes, des bras et des articulations ou le mouvement spécial obtenu par une caméra vidéo afin de l'envoyer à un ordinateur pour l'analyse afin de déterminer la vitesse et l'accélération de chaque individu [7] (Figure I.9).

Figure I. 9: Système biométrique basé sur la démarche.

- **Avantage :**
  - Très acceptable par les individus.

- **Inconvénient :**
  - N'est pas permanente (âge, fatigue, maladie).

I.4.2.4 Signature manuscrite: C'est une écriture personnelle d'un individu (Figure I.10), la vérification de la signature est basée sur deux modes:

Mode statique: la vérification de la signature statique met l'accent sur les formes géométriques de la signature, dans ce mode, en générale, la signature est normalisée à une taille connue ensuite décomposer en élément simple.

Mode dynamique: il utilise les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature [8].

Figure I. 10: Système biométrique basé sur la signature manuscrite.

- **Avantage :**
  - Très acceptable par l'utilisateur.
  - Peut protéger l'ensemble de vos fichiers personnels.
- **Inconvénients :**
  - Grande variabilité durant le temps (nous ne pouvons pas maintenir la même forme de la signature pour toute la vie).
  - Grande possibilité de fraude.

I.5. Conclusion

Chaque technologie biométrique possède des avantages mais aussi des inconvénients, acceptables ou inacceptables suivant les applications. Ces technologies n'offrent pas les mêmes niveaux de sécurité ni les mêmes facilités d'emploi ou encore pas la même précision. Dans ce chapitre nous avons introduit les concepts des systèmes biométriques, leurs architectures et leurs différentes applications. Nous avons aussi constaté que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre. Dans le chapitre suivant, nous allons étudier la reconnaissance biométrique basée sur Signature manuscrite.

Chapitre 02
Technologie biométrique

II. 1. INTRODUCTION

Le système de reconnaissance faciale, comme tous les systèmes biométriques est constitué de trois étapes essentielles : prétraitement, l'extraction des caractéristiques et la classification.

Dans la premier étape de prétraitement, en utilise des algorithmes qui traitées les images de signatures pour faciliter l'extraction des caractéristiques. Ensuite dans La deuxième étape définir les algorithmes holistiques (linaire /non linaire) sert à traiter l'image du signature afin d'extraire uniquement les caractéristiques biométriques, sous forme d'un vecteur, qui ensuite peuvent être utilisées pour reconnaitre l'individu. Ces caractéristiques sont uniques à chaque personne et stable. En fin la reconnaissance est faite par la comparaison (classification) du vecteur de caractéristique avec une base de données.

En représente Dans Ce chapitre les différents algorithmes qui utilisés dans les systèmes biométriques. Également, ces algorithmes se devisent en trois catégories : les algorithmes de prétraitement, les algorithmes extraction de caractéristiques et les algorithmes de classification. Ces derniers classés en deux approches Les algorithmes basés les approches holistiques qui sont deux types, algorithme linaire comme PCA "Analyse composant principale", LDA "Analyse Discriminante Linéaire". Et algorithme non linaire comme KPCA " kernel Analyse composant principale". En plus de donner un aperçu de certains algorithmes de classification tels que KNN (k near est neighbors).

II.2. Les algorithmes de prétraitement

II.2.1. Le filtre DoG (Difference of Gaussians)

En imagerie, différence de gaussiennes (DoG) est un algorithme d'amélioration des Caractéristiques qui consiste à soustraire une version floue d'une image originale d'une autre version moins floue de l'original. Dans le cas simple des images en niveaux de gris, les images floues sont obtenues en convertissant les images originales en niveaux de gris avec des noyaux gaussiens ayant des écarts-types différents. Le flou d'une image à l'aide d'un noyau gaussien ne supprime que les informations

spatiales à haute fréquence. La soustraction d'une image à l'autre préserve les informations spatiales situées dans la plage de fréquences conservée dans les deux images floues **[12]**.

Ainsi que, la différence entre les Gaussiens est un filtre passe-bande, qui élimine la Composante haute fréquence représentant le bruit, ainsi que certaine composante basse fréquence représentant les zones homogènes de l'image. Les composantes de fréquence dans la bande passante sont supposées être associées aux bords dans les images **[11]**.

Étant donnée, **σL** et **σH** définissent les basses et hautes fréquences respectivement. Ces fréquences de coupure dépendent de la qualité de l'image. Ici si la valeur de **σL** trop élevé entraînera la perte de l'information utiles car l'information se trouve principalement dans des basses filtrée ***Ip (x, y)*** est traitée comme suit **[11]**:

$$\mathbf{Ip(x, y)=DOG * I (x, y)} \qquad \text{(II.1)}$$

Le filtre DOG est calculé par l'équation :

$$\mathbf{DOG} = \frac{1}{2\pi\,\sigma_l{}^2}\, e^{\frac{x^2+y^2}{2\sigma_l{}^2}} - \frac{1}{2\pi\,\sigma_H{}^2}\, e^{\frac{x^2+y^2}{2\sigma_H{}^2\ 2}} \qquad \text{(II. 2)}$$

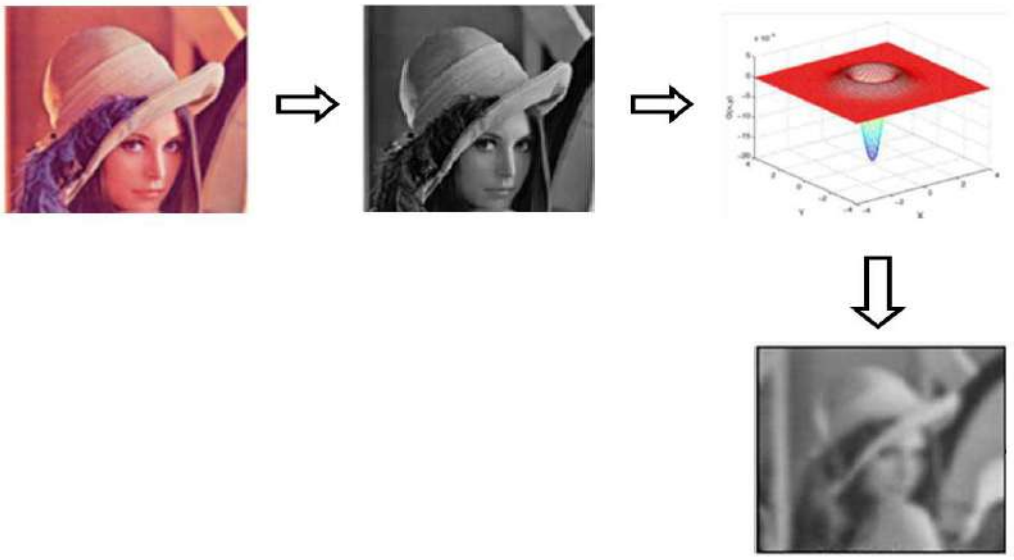


Figure II.1. L'application de filtre DoG sur une image originale [12].

II.3. Les algorithmes extraction de caractéristiques

II.3.1. Les méthodes holistiques

Les méthodes holistiques sont basées sur des techniques d'analyse statistique bien

Connues comme PCA et LDA.

II.3.1.1. Les méthodes linaires

Il y'a deux méthodes linaires :

II.3.1.1.a. PCA (Analyse Composant Principale)

Dans les statistiques, l'analyse en composantes principales (PCA) est une technique qui peut être utilisée pour simplifier un ensemble de données. PCA peut être utilisé pour réduire la dimensionnalité dans un ensemble de données tout en conservant les caractéristiques de l'ensemble des données qui contribuent le plus à sa variance, en gardant les composants principaux d'ordre inférieur et en ignorant d'ordre supérieur . L'idée est que ces composants à faible ordre contiennent souvent les aspects « les plus importants » des données **[13].**

La tâche de reconnaissance faciale est discriminant les signaux d'entrée (données

d'image) en plusieurs classes (personnes). L'entrée des signaux sont très bruyants (par exemple, le bruit est causé par différentes conditions d'éclairage, pose, etc.), mais les images d'entrée ne sont pas complètement aléatoire et en dépit de leurs différences il existe des modèles qui se produisent dans tout signal d'entrée. Ces modèles, qui peut être observée dans tous les signaux pourraient être dans le domaine de la reconnaissance faciale, la présence de certains objets (yeux, nez, bouche) dans tout le visage, ainsi que les distances relatives entre ces objets. Ces caractéristiques sont appelées Eigen faces dans le domaine de reconnaissance faciale (ou composants principaux généralement). Ils peuvent être extraits à partir de données d'image originale moyenne de l'outil mathématique appelé analyse des composantes principaux (PCA) **[13]**.

Au moyen de PCA, on peut transformer chaque image originale de la formation mis en Eigen face correspondant. Ainsi, le but de PCA est de réduire la grande

dimensionnalité de l'espace de visage (observé variables) à la plus petite dimension intrinsèque de l'espace de fonction (variables indépendantes), qui sont nécessaires pour décrire la données sur le plan économique **[13]**.

Pour générer un ensemble d'Eigen faces, un grand nombre d'images numérisées des

visages humains, pris sous le même éclairage conditions, sont normalisées pour aligner les yeux et la bouche. Ils sont alors tous formé avec la même résolution de pixels (N × N), puis traité comme N2 des vecteurs de dimension dont les composantes sont les valeurs de leurs pixels. Les vecteurs propres de la matrice de covariance de la distribution statistique des vecteurs d'images de visage sont ensuite extraits. Étant donné que les vecteurs propres appartiennent à le même espace vectoriel que des images de visage, ils peuvent être Considérés comme si elles étaient m × n images de visage de pixels, d'où le nom Eigen faces.

Dans cette façon, le principal Eigen face ressemble à un visage humain moyen **[13]**. Soit une image de visage Γ (x, y) à deux dimensions M par réseau N de valeurs d'intensité.

L'Analyse en Composante Principale sera appliquée sur la base des images de visages, désormais représentée par une matrice individus, caractéristiques selon l'algorithme suivant :

Etape 1 : Préparer les données

La première étape consiste à obtenir un ensemble S de **(N×N)** images de visage. Chaque image est transformé en un vecteur de taille **N2×1** et placé dans l'ensemble.

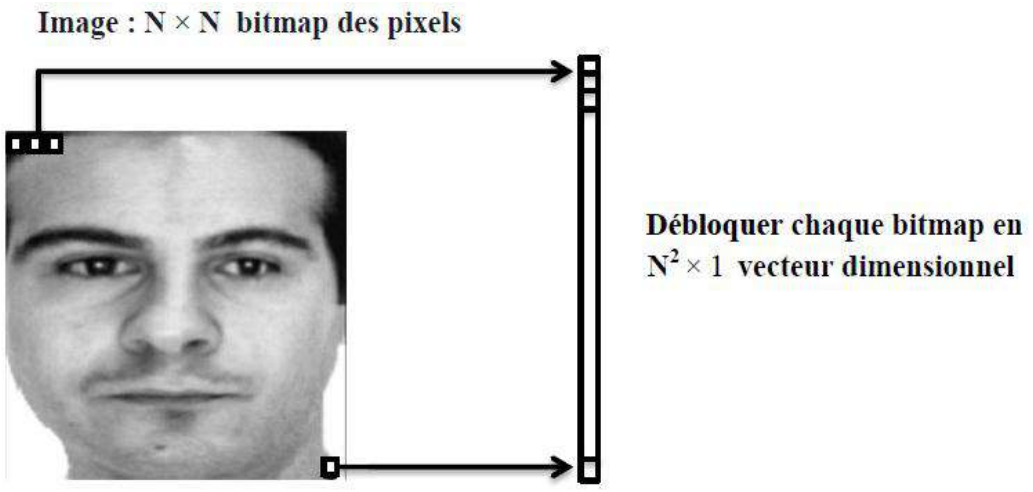


Figure II.2. Conversion de l'image N × N ver N 2× 1 vecteur

La matrice d'entraînement ***XT=[*X1, X2 … Xq*].*Xj** désigne le vecteur de **Jieme** image Avec

$1 \leq j \leq q$

Chaque vecteur ***(*Xj*)*** appartenant à l'un des classes **C1, C2… Cp.**

$$X_T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{q1} \\ a_{12} & a_{22} & \dots & a_{q1} \\ \vdots & \vdots & & \vdots \\ a_{1m} & a_{2m} & \dots & a_{qm} \end{pmatrix} = (X_1, X_2, \dots, X_q) \quad \text{(II.3)}$$

Etape 2 : Obtenir la moyenne

Après l'obtention de l'ensemble, l'image moyenne μ doit être obtenue sous la forme:

$$\mu = \frac{1}{q} \sum_{j=1}^{q} X_J \quad \text{(II.4)}$$

Figure II.3. Image moyenne

Etape 3 : Soustraire la moyenne de l'image originale

La différence entre l'image d'entrée et l'image moyenne doit être calculée et le résultat est stocké dans $\bar{\emptyset}_j$.

$$\bar{\emptyset}_j = X_j - \mu \tag{II.5}$$

Etape 4: Calculer la matrice de covariance

La matrice de covariance C est calculée de la manière suivante :

$$C = \frac{1}{M} \sum_{n=1}^{M} \emptyset_n \emptyset_n^T$$

$$= AA^T$$

$$A = [\emptyset_1, \emptyset_2, \emptyset_3, \emptyset_4 \dots \emptyset_M] \tag{II.6}$$

Etape 5: Calculer les vecteurs propres et valeurs propres de la matrice de covariance Avec la Réduction de la dimensionnalité.

Dans ce cas la taille de C est q×q

$$C = A^T A \quad Où \; A = [\emptyset_1, \emptyset_2, \dots \emptyset_q] \tag{II.7}$$

Si le nombre des images apprentissage est q=100 par exemple donc on obtient 100 Vecteurs propres et la longueur de chaque vecteur est 100.

Etape 6: La Conversion des k vecteurs propres de dimension inférieure à la dimension initiale des images originale.

Si u_i ont les vecteurs propres de $C = AA^T$ et v_i sont les vecteurs propres de $C = A^T A$

$$u_i = Av_i \tag{II.8}$$

Etape 7: Sélectionnez les K meilleurs vecteurs propres, sachant que cet espace Vectoriel s'appelle l'espace des Eigen faces (La représentation graphique des k meilleurs vecteurs propres s'appelle Eigen face en anglais). (Voir la figure II.4)

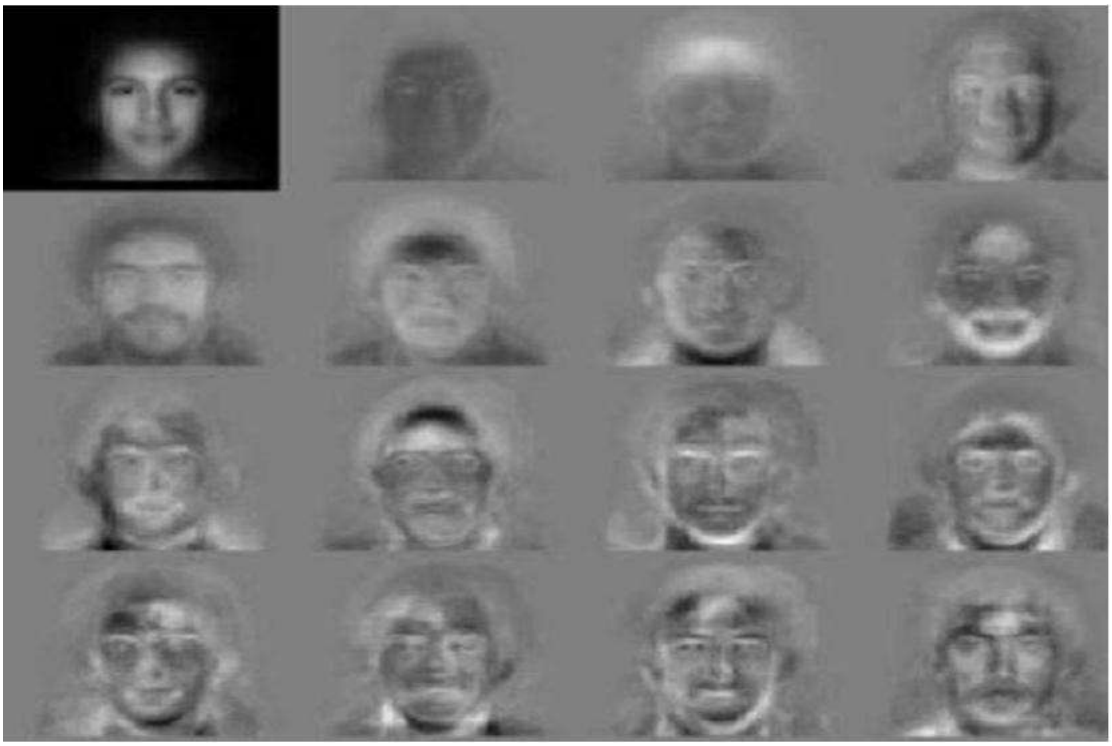


Figure II.4. Exemples les 15 Premier Eigen faces [32]

Dans la phase de test une image d'une personne inconnue est entrée au système alors le système convertir l'image d'entrée en un vecteur puis le normalisé. Ce vecteur normalisé a été projeté sur l'espace Eigen faces pour obtenir le vecteur de poids «weight vector». Celui-ci considéra comme la nouvelle représentation d'image d'entrée. Puis le système calcule la distance entre le vecteur poids d'image en entrée et les vecteurs poids dans la base de données. Enfin une décision est prête à partir de cette distance [11] (Voir figure II.5)

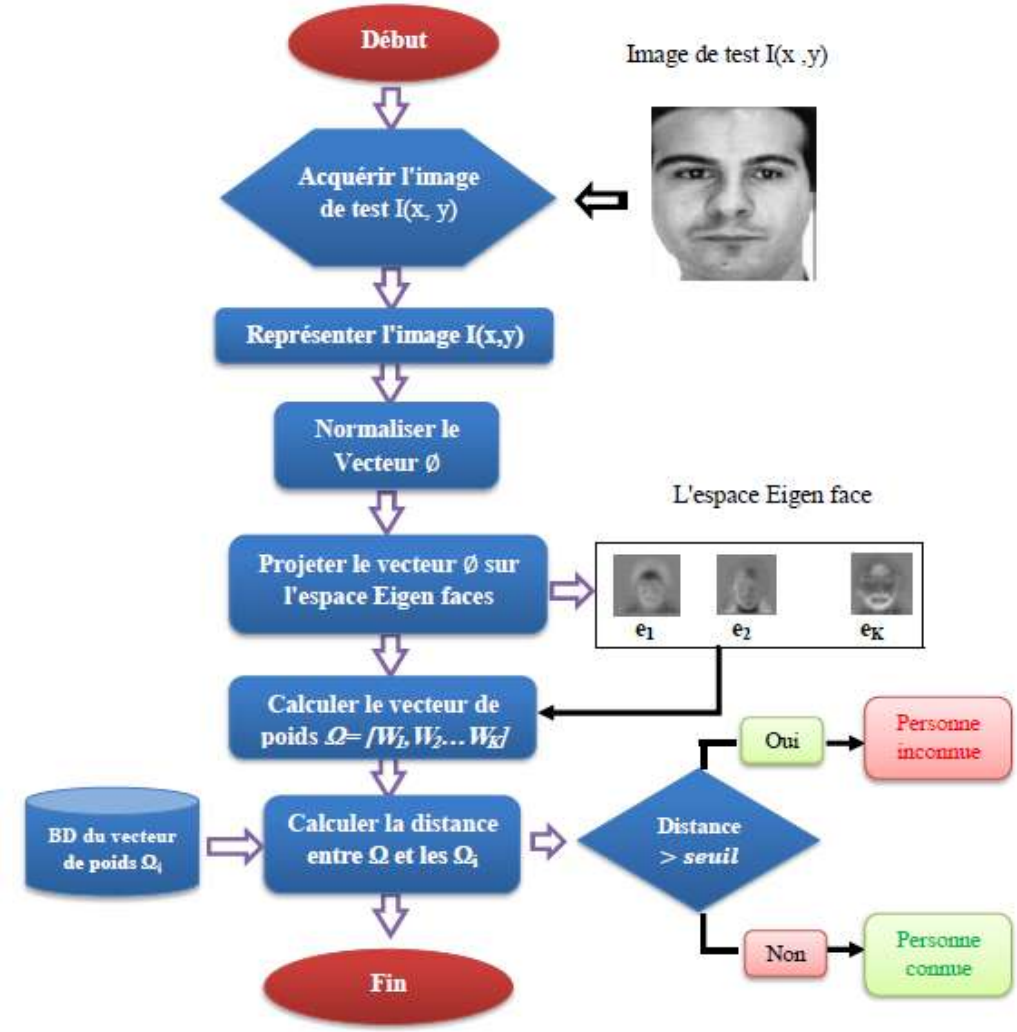


Figure II.5. Système de reconnaissance des personnes par PCA

II.3.1.1.b. LDA (analyse discriminante linéaire)

LDA est né des travaux de Bel humeur et al. De la Yale University (USA), en 1997 **[14]**.Il est aussi connu sous le nom de « Fisher faces ». Contrairement à l'algorithme PCA, celui de la LDA effectue une véritable séparation de classes. Pour pouvoir l'utiliser, il faut donc au préalable organiser la base d'apprentissage d'images en plusieurs classes : une classe par personne et plusieurs images par classe. La LDA analyse les vecteurs propres de la matrice de dispersion des données, avec pour objectif de maximiser les variations entre les images d'individus différents (inter classes) tout en minimisant les variations entre les images d'un même individu (intra classes) **[14-15]**.

Donc LDA c'est une technique populaire, utilisée pour trouver la combinaison linéaire des caractéristiques qui séparent mieux les classes d'objets. Les combinaisons résultantes peuvent être utilisées comme classificateur linéaire, ou pour la réduction des caractéristiques avant la classification **[16,17].**

Soit la matrice d'entrainement $X_T = [X1, X_2 \cdots X_q]$. X_j désigne le vecteur caractéristique d'image (j). Chaque X_j appartenant à l'un des N classe $C_1, C_2 \cdots C_n$ avec $1 \leq j \leq q$ [2]. Sous–espace LDA a été construit de sorte qu'il minimise la variance intra-classe S_b «betweenclass scatter matrix» et maximise la variance inter classe S_w «within-class squatter matrix» **[11]**:

$$S_B = \sum_{i=1}^{N} n_i(\mu_i - \mu)(\mu_i - \mu)^T \quad \text{(II.9)}$$

$$S_W = \sum_{i=1}^{N} \sum_{X_j \in C_i} (X_j - \mu_i)(X_j - \mu_i)^T \quad \text{(II.10)}$$

Où n_i représente le nombre d'échantillons dans l'iéme classe, μi désigne la moyenne des données d'apprentissage appartenant à $j^{iéme}$classe, **N** le nombre de classes et **μ** représente la moyenne globale de toutes les données d'entraînement. Et puis on dérive la matrice de transformation W qui maximise le critère discriminant de Fisher:

$$T(w) = W_{opt} = arg_w max \frac{|W^T S_B W|}{|W^T S_W W|} = [W_1 W_2 \dots W_d] \quad \text{(II.11)}$$

La solution optimale à ce problème d'optimisation est donnée par la résolution du

Problème généralisé des vecteurs propres

$$S_B W = \gamma S_W W \quad \text{(II.12)}$$

Ça revient à la recherche des vecteurs propres de la matrice $S_W^{-1} S_B$ La représentation

Graphique de ces vecteurs propres s'appelle en anglais Fisher faces. La langueur du vecteur caractéristique après l'application de LDA au plus N-1. Avec N est le nombre total des classes.

II.4.Les méthodes de classifications

II.4.1. KNN (k-nearest neighbors)

C'est un algorithme simple qui stocke tous les cas disponibles de données d'entraînement et classe les nouveaux cas en fonction de la majorité de ses voisins, en calculant la distance qui les sépare. Ces fonctions peuvent être la distance euclidienne, Manhattan, Minkowski et Hamming. Si K = 1, l'état est simplement affecté à la catégorie adjacente la plus proche. La nouvelle catégorie de points de données est prédite en recherchant dans le groupe de formation entier les catégories les plus étroitement liées **[20]**.

L'astuce consiste à déterminer les similitudes entre les données. Le moyen le plus simple de déterminer la similarité, si toutes les données sont identiques (par exemple, en pouces) - consiste à utiliser la distance euclidienne. L'application de l'algorithme KNN consomme beaucoup de mémoire pour stocker toutes les données, mais n'effectue aucun calcul à moins qu'il soit nécessaire de prévoir. Vous pouvez également mettre à jour les cas de formation au fil du temps pour maintenir les prévisions exactes **[20]**.

Donc le principe de cet algorithme de classification est très simple. On lui fournit un ensemble des données d'apprentissages **D**, une fonction de distance d et un entier **k** .Pour tout nouveau point de test x, pour lequel il doit prendre une décision, l'algorithme recherche dans **D** les **k** points les plus proches de **x** au sens de la distance **d**, et attribue **x** à la classe qui est la plus fréquente parmi ces **k** voisins**.(**figure II.8)

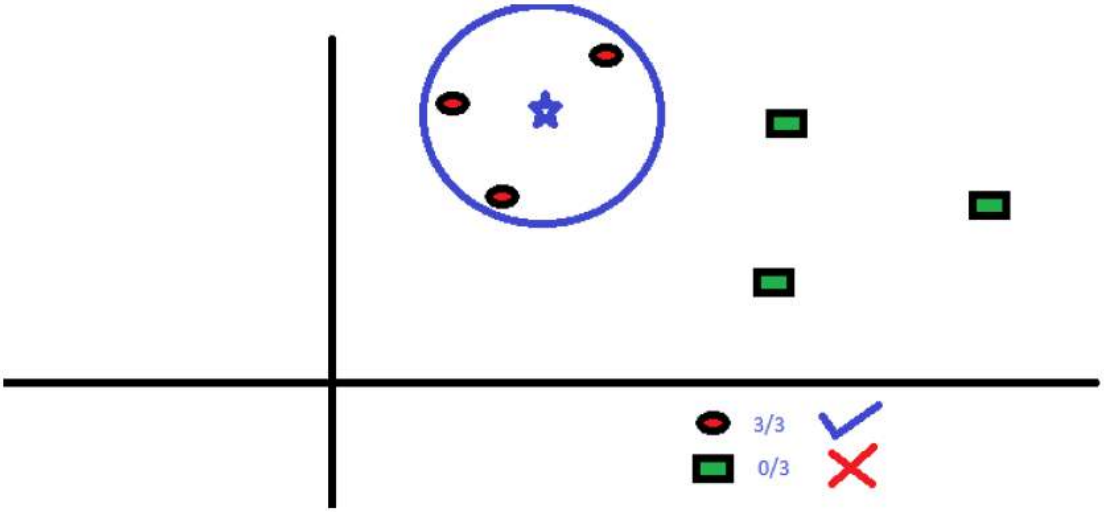


Figure II.6. Exemple d'application de KNN

II.4.1.1 Choix de k

✓ Pour les grandes valeurs de k :

- Moins sensible au bruit.
- Une grande base d'apprentissage permet une plus grande plus grande valeur de k.

✓ Pour les petites valeurs de k :

- Rend mieux compte de structure fine.
- Nécessaire pour les petites bases d'apprentissage.

II.4.1.2 Les distances Euclidienne :

La distance la plus connue est la distance Euclidienne, qui définit l'espace cartésien.

Donné pour des vecteurs de dimension n par l'équation suivante **[21]:**

$$\mathbf{d\ (x,\ y)} = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \qquad \text{(II.13)}$$

La distance Euclidienne est souvent utilisée au carré.

• **Distance cosine :**

La distance cosine est calculée à partir d'un moins un le cosinus de l'angle inclus entre les points **[21]**, défini par l'équation suivant:

$$d_{st} = \left(1 - \frac{x_s y_t'}{\sqrt{(x_s x_s')(y_t y_t')}}\right) \quad \text{(II.14)}$$

• **Distance Mahalanobis**

La distance de Mahalanobis est une mesure entre un et une distribution des données **[21]**, définie par l'équation suivant:

$$d_{st}^2 = (x_s - y_t)C^{-1}(x_s - y_t)' \quad \text{(II.15)}$$

Où **C** est la matrice de covariance

• **Distance corrélation**

La distance basée sur la corrélation est une mesure de la dépendance statistique entre deux vecteurs **[21]**, définie par l'équation suivant:

$$d_{st} = \left(1 - \frac{(x_s - \overline{x_s})(y_t - \overline{y_t})'}{\sqrt{(x_s - \overline{x_s})(x_s - \overline{x_s})'}\sqrt{(y_t - \overline{y_t})(y_t - \overline{y_t})'}}\right) \quad \text{(II.16)}$$

Où

$$\overline{x_s} = \frac{1}{n}\sum_j x_{sj}$$

$$\overline{y_s} = \frac{1}{n}\sum_j y_{sj} \quad \text{(II.17)}$$

• **Distance Spearman**

La distance de Spearman est calculée à partir de un moins la corrélation de Spearman entre les observations **[21]**, définie par l'équation suivant:

$$d_{st} = 1 - \frac{(r_s - \bar{r}_s)(r_t - \bar{r}_t)'}{\sqrt{(r_s - \bar{r}_s)(r_s - \bar{r}_s)'}\sqrt{(r_t - \bar{r}_t)(r_t - \bar{r}_t)'}} \quad \text{(II.18)}$$

Où

rsj est le rang de ***xsj*** repris ***x1j***, ***x2j***, ...*xmx*, *j*.

rtj est le rang de ***ytj*** pris en charge ***y1j, y2j***, ...*ymy*, *j*.

rs et ***rt*** sont les vecteurs de rang par coordonnées

de xs et yt,

c'est-à-dire rs = (rs1, rs2, ... rsn) et rt = (rt1, rt2,... rtn).

II.5. Conclusion

Dans ce chapitre nous avons étudié les différentes méthodes de prétraitement, d'extraction des caractéristiques et de classification. Dans le premier module, l'image est soumise à un traitement initial lors de l'entrée dans le canal du système biométrique afin de l'améliorer et d'éliminer les interférences, cette étape basé sur des algorithmes comme filtre DOG. Au module d'extraction des caractéristiques, les systèmes de reconnaissances faits des étapes plus importantes avant le stockage des informations dans ces bases de données. Ces étapes sont basées sur des algorithmes spécifiques comme : L'extraction de caractéristiques : pour obtenir les caractéristiques de chaque image acquise sous forme de vecteur. Il-y-a plusieurs méthodes pour faire cette opération comme PCA, LDA. La classification des données, dernière étape fait classer les caractéristiques semblables d'un ou plusieurs individus à la même classe, cette étape est appliquée par des algorithmes comme KNN , LPQ et LBP.

Chapitre 03
Authentification et signature

III.1. Introduction

Dans ce chapitre, nous dressons un panorama des différentes méthodes d'authentification biométrique. Puis nous présentons plus en détails les concepts de l'authentification par signature manuscrite et les travaux réalisés dans ce domaine dans le monde universitaire et industriel.

III.2. Contexte

La multiplication des outils informatiques nous oblige à saisir plusieurs fois par jour des combinaisons de caractères constituant un identifiant/mot de passe. Cette contrainte, qui vise à augmenter la sécurité, amène notamment les internautes à se simplifier la vie en privilégiant l'utilisation de mots de passe faciles à mémoriser, voire à les inscrire sur un petit papier scotché sous le clavier... Le constat est inquiétant : 91% des mots de passe utilisés par des internautes sont "connus", c'est-à-dire issus de l'environnement familier de la personne et jugés non viables par des spécialistes du cryptage :

- 21 % utilisent leur prénom, celui d'un membre de la famille ou de leur animal
- 15 % ont un lien avec une date clé (date de naissance, moment historique)
- 30 % des personnes partagent leur mot de passe avec leur partenaire

Plus généralement, les techniques d'authentification basées sur ce que l'on possède et sur ce que l'on sait présentent de nombreux inconvénients. Les objets permettant l'authentification sont souvent perdus ou volés et les mots permettant de s'identifier sont facilement oubliés. De plus, ce type de données est souvent partagé par plusieurs personnes. Par ailleurs, d'un point de vue sécurité, l'utilisation d'un mot de passe valide sur un réseau n'assure pas que la personne qui s'est connectée est bien celle qu'elle prétend être. On sait seulement qu'elle possédait la bonne clé d'accès. L'identité la protection des données privées ne peut pas être garantie et l'utilisation frauduleuse d'un de ces mécanismes ne peut pas être prouvée. Ces limitations des systèmes classiques d'authentification entraînent une perte de confiance et une augmentation des possibilités de fraude. La biométrie apporte une solution à ces différents problèmes. D'une part, le partage des données permettant l'authentification devient impossible. D'autre part, la confiance dans l'authentification est accrue puisque la personne doit être physiquement présente.

III.2.1. Le cadre juridique

L'aspect légal est un point important de la biométrie. Cette technologie mettant en jeu un individu, personne physique, constitue une donnée à caractère personnel c'est-à-dire, selon la définition posée par la Loi n°2004-801 du 6 août 2004, une "information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres" [22]. En cela, tout traitement portant sur la reconnaissance biométrique entre dans le champ d'investigation de la Commission Nationale de l'Informatique et des Libertés (CNIL) [23]. Dans deux délibérations rendues le même jour, le 8 avril 2004 (délibérations n°04-017 et 04-018), la CNIL a fixé quelques points de repère qui montrent la vigilance dont elle fait preuve face à cette technologie.

Dans la première délibération, le centre hospitalier de Hyères envisageait de mettre en œuvre un traitement consistant à horodater les entrées et sorties de son personnel en s'appuyant sur un dispositif de reconnaissance de l'empreinte digitale. La CNIL a émis un avis défavorable à la mise en œuvre de ce traitement ayant pour objectif la gestion du temps de travail.

Pour motiver cet avis négatif, la CNIL s'appuie sur deux types d'arguments. D'une part, elle critique la centralisation des données biométriques sur un serveur central, voyant là une solution qui "n'est pas de nature à garantir la personne concernée de toute utilisation détournée de ses données biométriques", d'autre part, elle se fonde sur une disposition insérée dans le Code du Travail selon laquelle "nul ne peut apporter aux droits des personnes et des libertés individuelles ou collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché" (article L 120-2 du code du travail).

La CNIL considère dès lors que "seul un impératif de sécurité est susceptible de justifier la centralisation de données biométriques". Elle y voit au contraire dans le cas du centre hospitalier d'Hyères un traitement disproportionné par rapport à la finalité recherchée, soit la gestion du temps de travail. Dans la seconde délibération du même jour, la CNIL va en revanche donner un avis favorable à l'établissement public Aéroports de Paris pour un système de contrôle d'accès aux zones réservées, dans un objectif de sûreté, des aéroports d'Orly et de Roissy. Logiquement et compte tenu de la première délibération évoquée ci-dessus, la Commission retient ici que "seuls sont enregistrés sur le badge, le gabarit biométrique, le numéro du badge et le code PIN

Associé au badge" notant par là que les données biométriques résident avec la personne et que, au regard de l'application concernée, "ces données sont adéquates, pertinentes et non excessives".

"Ces deux délibérations ont été rendues sous l'empire de la loi ancienne de 1978 mais, quant aux règles de fond qu'elles posent, il n'y a aucune raison qu'elles ne soient pas prises en compte aujourd'hui. La biométrie est une technologie sans doute utile notamment à l'authentification, mais son usage doit sans doute respecter un certain nombre de règles légales à ne pas oublier" [24].

III. 2.1.1 L'absence de reconnaissance juridique de la Biométrie

A l'heure actuelle, l'utilisation des systèmes biométriques ne fait pas l'objet d'un régime juridique particulier. La CNIL, dans le cadre de son rapport annuel d'activité présenté au mois de juillet 2004, a fait part de sa position sur les différentes techniques biométriques et les dangers découlant de leur utilisation. En effet, la CNIL considère qu'un élément d'identification biométrique ou sa traduction informatique sous forme de gabarit constitue une donnée à caractère personnel entrant dans le champ d'application de la loi "informatique et liberté" au même titre que d'autres données personnelles (nom, adresse, etc.). Dans ces conditions, la conservation ou le stockage des éléments biométriques d'identification s'apparente à la conservation d'une base de données et relève, en conséquence, de l'ensemble de la législation sur la protection des données. Plus particulièrement, la constitution de bases de données doit respecter les principes clés de finalité et de proportionnalité. En effet, la CNIL considère que "seul un impératif particulier de sécurité est susceptible de justifier la Centralisation de données biométriques" [25].

III.2.1.2 Les perspectives d'utilisation des techniques Biométriques

Au regard de ce qui précède, la CNIL formule plusieurs propositions destinées à encadrer l'utilisation des techniques biométriques :

a) Le non conservation de données biométriques dans des bases de données

Les technologies biométriques de reconnaissance qui ne reposent pas sur le stockage d'éléments d'identification biométrique dans une base de données ne soulèvent pas de difficultés particulières au regard de la loi "informatique et liberté", dès lors que l'élément d'identification biométrique est conservé par l'utilisateur et uniquement par lui (sur une carte à puce, etc.) ou sur un appareil dont il a l'usage exclusif (téléphone portable, appareils nomades, etc.).

b) le stockage de données biométriques lié à des impératifs de sécurité

Lorsqu'une base de données est constituée, le contrôle de finalité et de proportionnalité peut conduire à accepter la mise en œuvre de telles bases de données si un impératif particulier de sécurité le justifie (contrôle d'accès à des bâtiments hautement sécurisés de la Banque de France ; bâtiments de stockage de plutonium ; etc.).

III.2.2. But de l'authentification : vérification ou identification?

Le terme "authentification" couvre en fait deux sous problèmes : l'identification et lavérification.

L'identification consiste à déterminer, à partir d'une base de référence, la personne dont ladonnée biométrique est la plus proche de celle testée. Dans ce cas, la réponse du système sera le nom de la personne ou le rejet de la donnée biométrique si aucune des références stockées dans la base n'est assez proche de la donnée testée.

La vérification correspond à une notion différente en ce sens qu'elle n'est pas reliée à une base de données. Cela consiste à vérifier si l'élément biométrique testé correspond bien à la personne qui prétend le posséder. Par conséquent, la réponse ne peut prendre que deux valeurs, l'acceptation ou le rejet de la donnée biométrique suivant le degré de similarité entre l'élément biométrique testé et une référence en tenant compte du niveau de sécurité souhaité. Dans cette thèse, nous nous sommes plus intéressés au problème de la vérification qu'à celui de l'identification. 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.

III.2.3. Architecture d'un système d'authentification Biométrique

L'architecture générale d'un système d'authentification basée sur la biométrie est décrite dans la Figure (III.1)

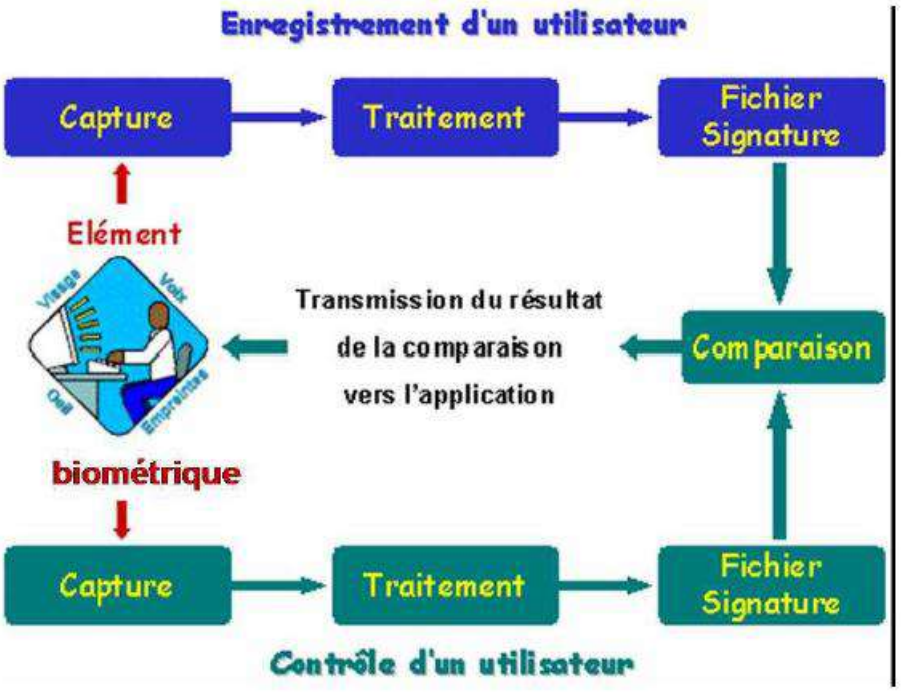


Figure (III.1): Architecture d'un système d'authentification biométrique.

Dans un premier temps, l'utilisateur doit s'enregistrer. Ce processus, appelé aussi enrôlement, est constitué d'une phase de capture de l'élément biométrique qui est répétée un certain nombre de fois pour avoir un aperçu de la variabilité de cet élément, d'une phase de traitement permettant l'extraction des caractéristiques de celui-ci et, à partir des données extraites, d'une phase de création d'un modèle représentatif de l'utilisateur. Une fois enregistré, l'utilisateur peut alors s'authentifier. Les trois premières phases sont identiques à celles effectuées lors de l'enregistrement. La comparaison se fait alors entre les données extraites de l'élément biométrique testé et le ou les modèles enregistrés correspondants.

III.2.4. Evaluation

Lors de l'opération d'authentification, un capteur, de même nature que celui utilisé pour l'enrôlement, est utilisé pour générer un nouveau fichier brut qui va subir les mêmes opérations d'analyse que le fichier modèle (référence). Un nouveau fichier signature sera produit. Une analyse de corrélation plutôt qu'une vérification d'identité est réalisée entre les deux fichiers signature car, bien évidemment, en pratique les deux fichiers signature ne sont jamais identiques. Il en résulte un coefficient de ressemblance qui peut varier de 0 à 100 %.

Selon les critères de la sévérité souhaités par l'application en question, il suffit simplement de vérifier si la ressemblance est supérieure ou inférieure au seuil fixé à l'avance. Il va de soi quel'acceptation d'une transaction pour un distributeur de billets nécessite un seuil beaucoup plus sévère que celui autorisant l'accès à une salle de concert.

L'évaluation d'un système d'authentification ne peut pas être réalisée en utilisant uniquement le taux d'erreur classique parce que toutes les erreurs n'ont pas le même impact et les contraintes des applications peuvent changer. Nous devons donc différencier le taux de faux acceptés (FAR) indiquant les faux non détectés par le système et le taux de vrais rejetés (FRR) indiquant les signatures authentiques rejetées par le système Le EER (Equal Error Rate) correspond au taux d'erreur pour lequel FAR est égal à FRR.

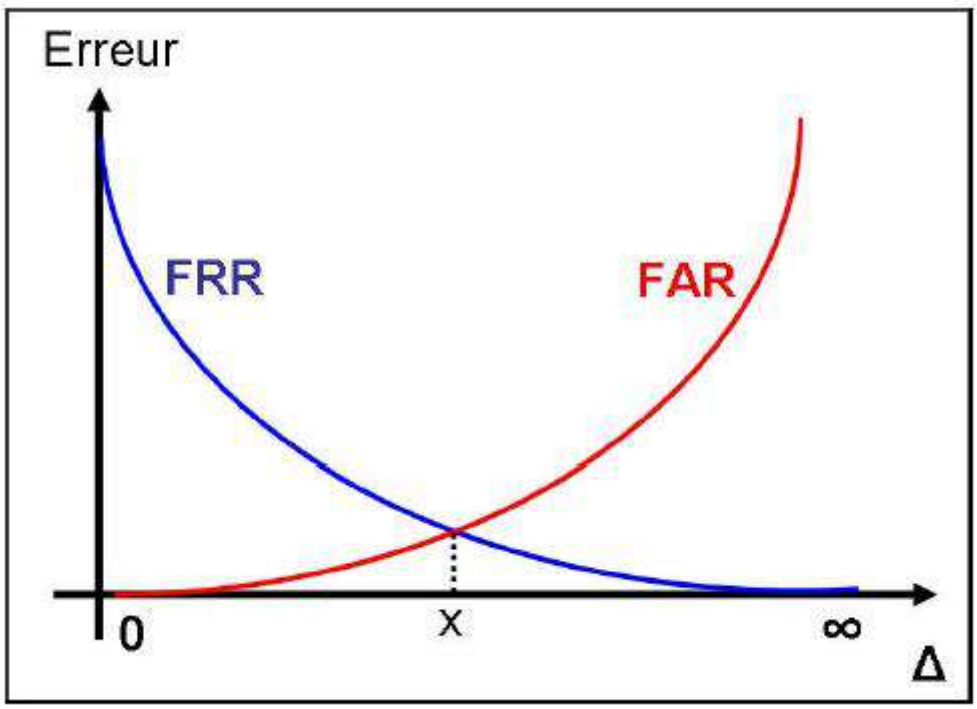


Figure (III.2): Evolution de FRR et de FAR en fonction du seuil.

Le graphe de la Figure (III.2) est purement démonstratif représente un paramètre du système, variant de 0 à l'infini. Très succinctement, on voit que plus la marge d'erreur autorisée est importante, plus le taux de fausses acceptations augmente, c'est-à-dire que l'on va accepter deplus en plus de personnes qui ne sont pas autorisées (et donc la sécurité du système diminue).Par contre on voit que le taux de rejet des personnes autorisées diminue également, ce quirend le système plus fonctionnel et répond mieux aux attentes des utilisateurs. A l'autreextrémité, si l'on diminue la marge d'erreur acceptée par le procédé de mesure biométrique, les tendances des 2 taux sont inversées : on va de moins en moins accepter des individusessayant de frauder mais on va, par la même occasion, avoir un taux de rejet sur des

personnes autorisées qui sera trop important pour être toléré dans la plupart des cas. Le compromis habituel est de régler le système selon la jonction des courbes, c'est à dire de fixer le paramètre à la valeur x où le couple (FAR, FRR) est "minimal". Les valeurs de ces paramètres, FAR et FRR, doivent être fixées en fonction de l'application. En général, on ne peut pas fixer les deux simultanément. Pour un produit industriel, la valeur de FRR doit être faible afin d'éviter la répétition de la phase d'authentification quand une personne autorisée a été rejetée et doit faire un nouvel essai. Pour notre projet, l'objectif est de garder la valeur de FRR en dessous de 2% car les utilisateurs de systèmes d'authentification ne tolèrent pas de taux plus élevé.

Après cette présentation générale de ce qu'est la biométrie et des différents moyens d'authentification associés, nous allons décrire de manière plus détaillée l'authentification par signature manuscrite et dresser un panorama des travaux effectués dans ce domaine.

III.3. L'authentification par signature manuscrite

"La signature identifie celui qui l'appose, manifeste le consentement des parties aux Obligations et confère l'authenticité à l'acte". (C. civ., art. 1316, al. 1 nouveau).

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu pour manifester sa propre volonté. Elle est aujourd'hui, et le demeurera sans doute dans le futur, le moyen biométrique d'authentification le plus utilisé. L'utilisation de la signature manuscrite repose sur l'hypothèse que ce sont plus des mouvements instinctifs que des actes conscients qui sont impliqués dans la réalisation de la signature. Ce postulat implique que certaines caractéristiques de la signature sont stables donc constantes pour un signataire. Ainsi, 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 (ou les) signature(s) 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 :

c) le support et le stylet utilisés

d) l'importance du document sur lequel on appose la signature

e) 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 :

1. Fonction d'identification. Le système d'authentification doit être suffisamment fiable pour être reconnu comme moyen de non répudiation.
2. Fonction d'adhésion au contenu .Culturellement le fait d'apposer sa signature manuscrite signifie que l'on adhère au contenu indépendamment du support.
3. Fonction de garantie de l'intégrité .La garantie de l'intégrité du document peut être assurée par une fonction de hachage.
4. 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.
5. 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 surl'importance de l'acte contrairement aux méthodes actuelles où l'on entre un code PIN.

III.3.1 Principes de fonctionnement

Classiquement, la conception d'un système d'authentification nécessite d'apporter des solutions à cinq problèmes :

1. Acquisition des données
2. Prétraitement
3. Extraction des caractéristiques et/ou parties stables
4. Comparaison (et donc décision)
5. Evaluation des performances

Dans le cas de la signature en ligne, ces problèmes se déclinent de la manière suivante :

1. L'acquisition des données se fait au moyen d'un stylet électronique. L'utilisateur signe à plusieurs reprises (au moins cinq fois) afin d'établir une référence. La signature de référence peut être, par exemple, une moyenne des signatures servant d'exemple.
2. Le prétraitement consiste à réduire le bruit, lisser le signal dans le temps et l'espace, normaliser les données (mise à l'échelle, centrage…) et à les coder.
3. Sur l'ensemble des supports, des données de deux types peuvent être extraites localement ou globalement. Elles peuvent concerner la forme ou la dynamique.

4. Les données relatives aux variations locales du signal en entrée concernent, par exemple, la position, la vitesse, l'accélération, … Ces dernières peuvent être couplées à des données plus générales comme la longueur, le temps total, des moyennes…
5. La comparaison entre la signature testée et la ou les signatures servant de référence correspond à un calcul de distance. Si la distance entre ces signatures est inférieure à un certain seuil, la signature est reconnue comme authentique sinon elle est reconnue comme un faux.
6. Afin d'évaluer le système, la constitution d'une base de test contenant un nombre important de signatures authentiques est indispensable.

III.3.2. 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 [26]. 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.

III.3.2.1 Types de Faux

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.

III.3.2.2 Remarques

On parle de faux par déguisement si le scripteur réalise une signature différente de sa signature habituelle dans le but de la renier ultérieurement. On remarque que le faux par imitation libre est le faux le plus difficile à détecter et également le plus difficile à produire.

Enfin, notons que le pourcentage de faux acceptés est très difficile à évaluer car il est impossible d'obtenir des faux réalisés par des faussaires professionnels.

III.3.2.3 Création de fausses signatures : mode d'emploi

Afin de mieux détecter les fausses signatures, il peut être intéressant d'avoir une réflexion sur la manière dont les faussaires pourraient procéder.

La première difficulté concernant la création de fausses signatures est de collecter les données nécessaires c'est à dire :

- plusieurs exemples de signatures originales pour évaluer la forme de la signature, ses variations et la gestuelle du scripteur
- plusieurs enregistrements de vidéos de la personne en train de signer pour évaluer la dynamique de la signature et ses variations

Réaliser une imitation d'une signature requiert beaucoup d'entraînement car il est très difficile, voire impossible, d'imiter à la fois la forme et la dynamique. La durée de l'entraînement est proportionnelle à la difficulté de reproduction de la signature. En effet, une signature stable avec beaucoup de changements de direction et de rythme sera beaucoup plus difficile à reproduire qu'une signature relativement variable constituée d'un tracé simple et sans changement de rythme.

Une autre difficulté réside dans le fait qu'il n'est pas possible pour le faussaire de s'entraîner sur un système existant puisque celui-ci se bloque au bout d'un certain nombre de tentatives d'authentification. C'est le même principe qui est utilisé pour le code PIN d'une carte bancaire

ou d'une puce de téléphone portable. Après, en général, trois échecs lors de la phase d'authentification, la carte ou le téléphone est verrouillé.

Le faussaire devra éventuellement essayer de trouver le fichier référence de l'utilisateur dont il souhaite imiter la signature.

Le faussaire devra donner une réponse aux questions :

- quelles sont les données collectées lors de la signature?
- quelles sont les caractéristiques extraites de la signature?
- comment sont-elles extraites de la signature?

La signature ne doit pas être identique aux signatures précédentes car un contrôle de rejeu est effectué. Cela signifie que ces fausses signatures ne pourront pas être l'œuvre d'un robot auquel on aurait fourni une vidéo de la personne en train de signer.

III.3.3. 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 la 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.

III.3.4. Différences entre hors ligne et en ligne

Dans un système hors ligne, la signature est effectuée sur un support papier puis scannée. 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. Au contraire, lors d'une acquisition en ligne, le trait n'a pas d'épaisseur et est représenté avec la même intensité sur les systèmes ne permettant pas l'acquisition de la pression. Hormis pour l'étude de la forme, les techniques appliquées en hors-ligne ne peuvent donc pas, en général, être adaptées aux techniques en ligne puisqu'elles sont basées la plupart du temps sur l'étude des niveaux de gris de l'image [27, 28, 29].

Dans le cas d'un système en ligne, la signature est effectuée sur une tablette graphique ou toutautre support muni d'un stylet électronique. La signature est donc représentée par une suite depoints définis par au moins 3 valeurs : x, y, t. Nous avons remarqué, lors de nosexpérimentations, que les dispositifs actuels d'acquisition de l'écriture manuscrite en lignesont loin d'offrir une ergonomie suffisante pour que les usagers les utilisent sans stress. Eneffet, la gêne occasionnée entraîne des efforts supplémentaires. Beaucoup de personnesadaptent ou modifient leur manière d'écrire et de signer lors du passage sur un supportnumérique. Cela est critique lorsqu'il s'agit de signer car on ne signe pas de la même manièresur papier ou avec un stylet et un temps d'adaptation au support numérique est donc nécessaire avant d'obtenir une stabilité suffisante de la signature.

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

III.4.conclusion

Dans ce chapitre, nous avons présenté dans un premier temps les modes de fonctionnement d'un système biométrique avec leurs diagrammes des processus et le cadre juridique. 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 04

Processus de notre programme d'identification des signatures manuscrites

IV.1. Introduction

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu. Elle est 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, 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 [31].

Dans ce chapitre nous allons expliquer avec détails le fonctionnement et le processus de notre programme d'identification des signatures manuscrites d'une manière générale et abrégé, plusieurs programmes et méthodes sont mises en œuvre pour l'identification des signatures, en utilisant la simulation sur Matlab pour visualiser les résultats à vouloir obtenir.

IV.2. Différences entre signature en ligne ou hors ligne

IV.2.1 Système hors ligne

Dans un système hors ligne, la signature est effectuée sur un support papier puis scannée. 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. Au contraire, lors d'une acquisition en ligne, le trait n'a pas d'épaisseur et est représenté avec la même intensité sur les systèmes ne permettant pas l'acquisition de la pression. Hormis pour l'étude de la forme, les techniques appliquées en hors-ligne ne peuvent donc pas, en général, être adaptées aux techniques en ligne puisqu'elles sont basées la plupart du temps sur l'étude des niveaux de gris de l'image

IV.2.2. Système en ligne

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. La signature est donc représentée par une suite de points définis par au moins 3 valeurs : x, y, t. Les dispositifs actuels d'acquisition de l'écriture manuscrite en ligne sont loin d'offrir une ergonomie suffisante pour que les usagers les utilisent sans stress. Beaucoup de personnes adaptent ou modifient leur manière d'écrire et de signer lors du passage sur un support numérique. Cela est critique lorsqu'il s'agit de signer car on ne signe pas de la même manière sur papier ou avec un stylet et un temps d'adaptation au

support numérique est donc nécessaire avant d'obtenir une stabilité suffisante de la signature [30].

IV.3. Fonctionnent d'un systèmes biométriques :Enrôlement, vérification et identification.

Les systèmes biométriques fonctionnent selon trois modes que sont l'enrôlement, la vérification d'identité et l'identification [31]:

- **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. Le module d'enrôlement correspond à l'enregistrement biométrique des individus dans la base de données du système.
- **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 : N. 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.

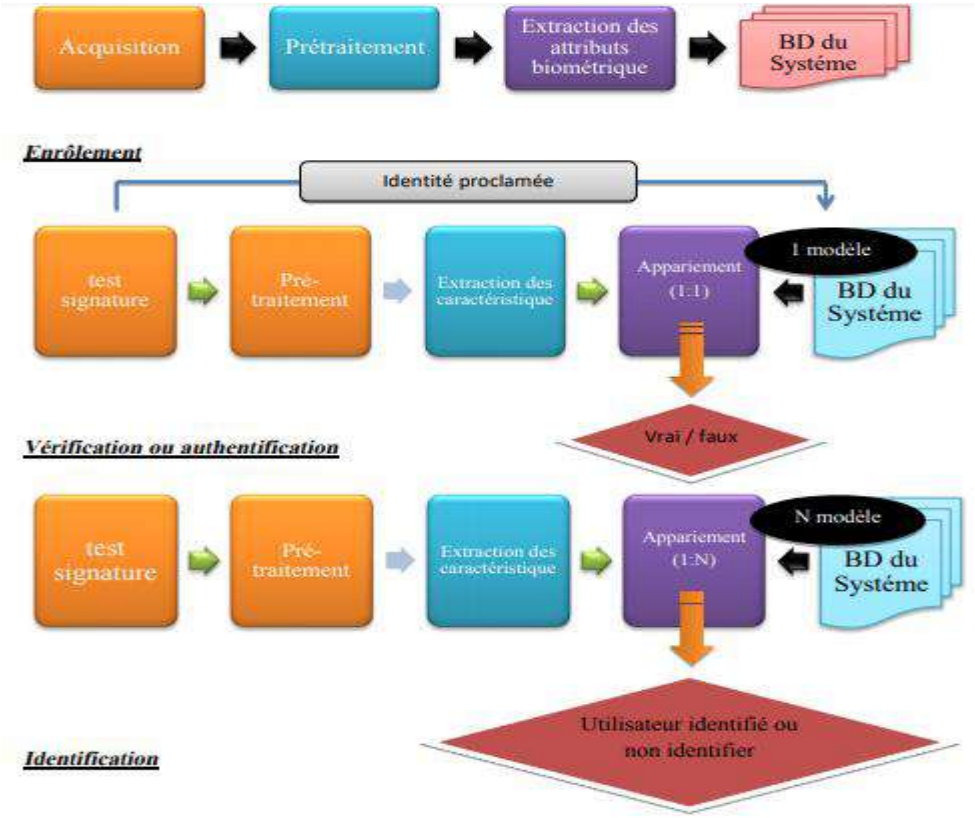


Figure IV.1 :schéma de fonctionnement d'un système biométrique. Diagrammes des processus d'enroulement, de vérification et d'identification.

Les schémas d'un système de vérification et d'un système d'identification sont illustrés dans la figure(IV.1) [31].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.

IV.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 à la base de données GPDS 100.

IV.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. 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.

❖ **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 de la base GPDS 100 on a choisi de normaliser tous les images a une taille de 255. Le classificateur va effectuer plus efficacement sur les images homogènes. La figure ci-dessous donne quelques résultats de la normalisation de la taille.

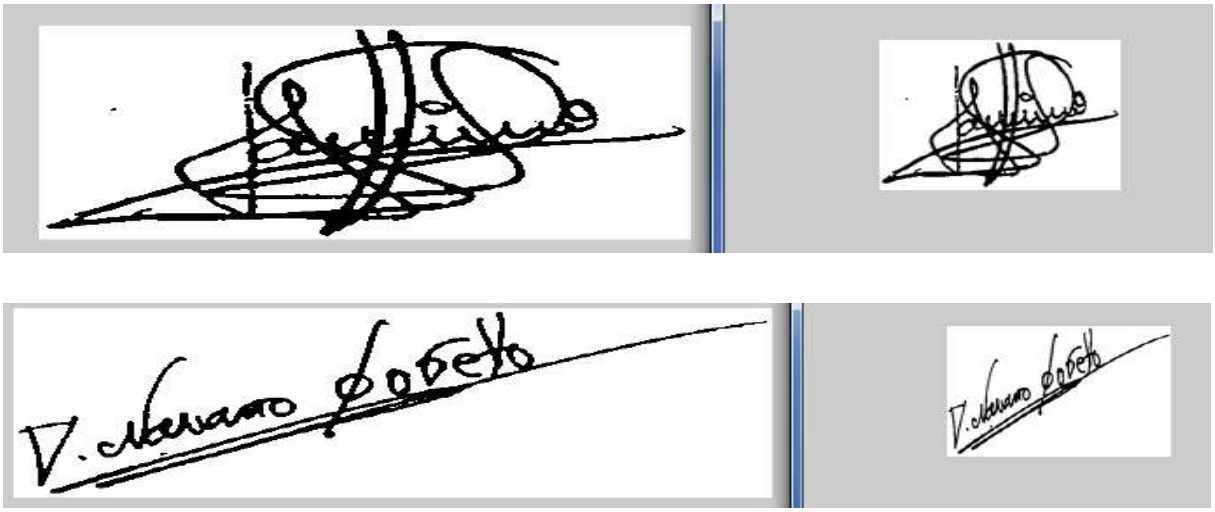


Figure IV .2 : Un échantillon de signatures avant (à gauche) et après (à droite) normalisation de la taille.

❖ **Squelettisation** : dans la plus part des cas, la forme à reconnaitre ne dépendpas 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.

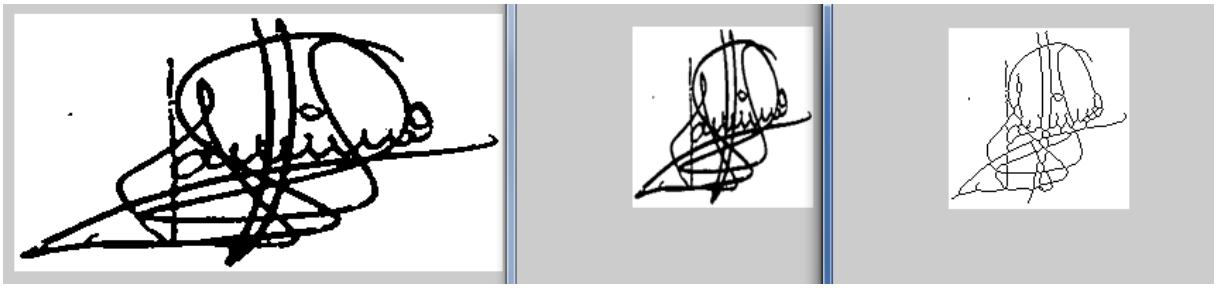


Figure IV.3 : la squelettisation d'un échantillon de signature.

IV.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.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.

IV.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.

IV.4.3.1 Phase d'apprentissage

L'étape d'apprentissage consiste à caractériser les classes de formes de maniéré à bien distinguer les familles homogènes de formes. L'apprentissage consiste à mémoriser les représentations calculées dans la phase analyse pour les individus connus.

IV.4.3.2 Phase de test

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.

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.

IV.5.Extraction des caractéristiques

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.Nous nous sommes intéressés dans cette étude par les descripteurs de texture locaux inspirés principalement par ***LBP*** (la technique des motifs binaires locaux) et ***LPQ*** (Local Phase Quantization).

IV.5.1.LBP de base

Le concept du LBP est le suivant : un code binaire décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Tous les voisins prendront alors une valeur 1 si leur valeur est supérieure ou égale au pixel courant et 0 sinon. On va alors multiplier cette matrice composée de 0 et 1 par les poids LBP et sommer tous ses éléments pour obtenir la valeur LBP du pixel courant [32] On obtiendra donc des pixels dont l'intensité se situe entre 0 et 255 comme dans une image 8 bits ordinaire (Figure. IV.4).

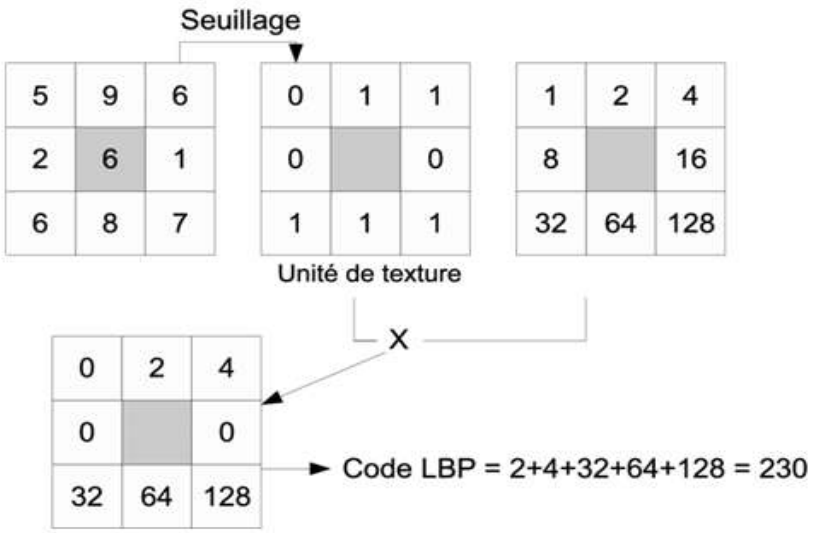


Figure IV.4 : Illustration de calcul d'un LBP

Le LBP de base est défini par :

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} S(g_p - g_c) \times 2^p \qquad \text{(IV.1)}$$

Où : g_c est le niveau de gris du pixel central de coordonnées (x_c, y_c).

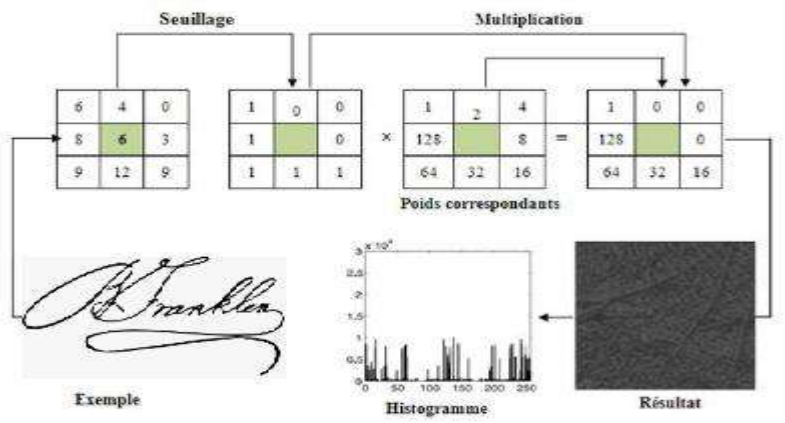
(p = 0,1,...,7) est le niveau de gris de chaque pixel voisin.

Avec : S(x) une fonction définie comme suit :

$$S(x) = \begin{cases} 1 & si\ x \geq 0 \\ 0 & si\ x < 0 \end{cases} \qquad \text{(IV.2)}$$

IV.5.2.Histogramme

Souvent la distribution des codes LBP sur l'image est utilisée pour décrire la texture sous forme d'histogramme. Une fois le code LBP est calculé pour tous les pixels de l'image, on calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image. En réalité, afin d'incorporer plus d'informations spatiales au vecteur représentant l'image, on divise tout d'abord cette image codée par l'opérateur LBP en petites régions et l'histogramme sera construit pour chaque région. Finalement, on concatène tous les histogrammes des régions afin de former un grand histogramme représentant l'image (voir la figure ci-après). L'efficacité du code LBP s'explique par le fait que le LBP permet de caractériser les détails fins d'unesignature.



Le motif =11111000 LBP code =1+16+32+64+128=241

Figure (IV.5) : Exemple d'un histogramme LBP d'une image signature.

L'histogramme LBP est connu sous cette forme :

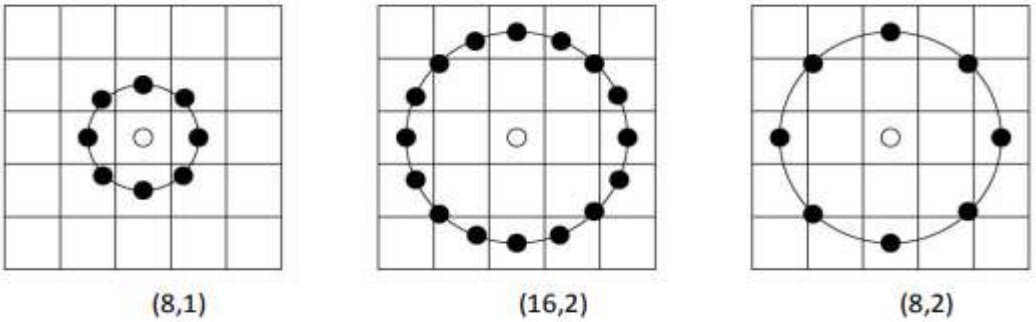
$$h(i) = \sum_{x,y} B(LBP(x,y) = i) \qquad \text{(IV.3)}$$

$$\text{Avec : } i \in [0, \dots, 2^p - 1] \quad \text{et} \quad B(v) = \begin{cases} 1, & \textit{lorsque } v \textit{ est vraie} \\ 0, & \textit{autrement} \end{cases}$$

IV.5.3. Le LBP_{PR}

A l'origine, les codes de LBP ont été proposés seulement pour des régions 3 x 3. Ils ont été limités à de petites régions et ne peuvent capturer que des micro-textures locales. Ainsi, le LBP a été étendu à LBP (P, R) et cela en utilisant des voisinages de taille différente. Dans ce cas, un cercle de rayon R autour du pixel central est choisi. Les valeurs des P points échantillonnés sur le bord de ce cercle sont prises et comparées avec la valeur du pixel central. Pour obtenir les valeurs des P points échantillonnés dans le voisinage pour tout rayon R, une interpolation est nécessaire.

Dans ce qui suit, la notation (P, R) définie le voisinage de P points sur un rayon R d'un pixel (Figure IV.6).



Figure(IV.6) : Exemples de voisinages avec différentes valeurs de (P, R).

Pour calculer un LBP dans un voisinage de P pixels, dans un rayon R, on compte simplement les occurrences de niveaux de gris plus grands que la valeur centrale.

$$LBP_{P,R} = \sum_{p=0}^{P-1} S(g_p - g_C)\, 2^p \qquad \text{(IV.4)}$$

Où (x)est la fonction signe :

$$s(x) = \begin{cases} 1 \; si \; x \geq 0 \\ 0 \; sinon \end{cases} \qquad \text{(IV.5)}$$

$g_p$et$g_C$sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

On peut illustrer la méthode calculant le $LBP_{P,R}$ par la figure suivante :

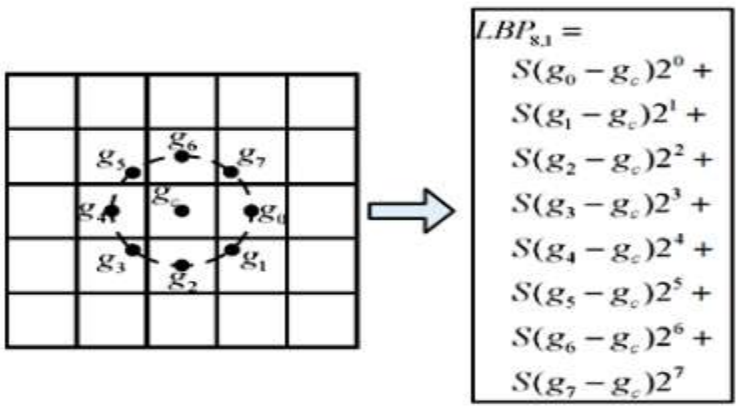


Figure (IV.7) : Calcul d'un $LBP_{P,R}$ (P=8, R=1).

IV.5.4. Local Phase Quantization (LPQ)

Le descripteur de texture Quantification de Phase Locale (ou Local Phase Quantization : LPQ) a été introduit pour la première fois par Ojansivuet[33].Il permet d'améliorer la classification de textures tout en étant robuste aux artéfacts générés par différentes formes de flou présents dans une image. Pour cela, le descripteur est construit de façon à ne retenir dans une image que l'information locale invariante à un certain type de flou.Une fois les conditions sur le flou définies, une transformée de Fourier à fenêtre glissante est calculée pour plusieurs fréquences u choisies pour respecter les critères de la fonction d'étalement. Les coefficients ainsi obtenus sont quantifiés afin d'obtenir un mot de 8 bits [33].

L'information de LPQ peut être extraite en utilisant la transformée discrète de Fourier à fenêtre à deux dimensions (2DWFT).

$$F_u(x) = \sum_{m \varepsilon Nx} h(m-x) f(m) e^{-j2\pi u^T m} = E_u^T f_x \qquad \text{(IV.6)}$$

Où E_u, de taille = 1 ×M2, est un vecteur de base de 2DWFT avec la fréquence u, et fx, taille = MT× N, est un vecteur contenant les valeurs des pixels d'image dans Nx à chaque position x. La fonction fenêtre, h (x) est une fonction rectangulaire. La transformation est calculée à quatre valeurs de la fréquence, u = [u_0, u_1, u_2, u_3] où u_0 = [a, 0]T, u_1 = [0, a]T, u_2 = [a, a]T et u_3 = [a,-a]T. La valeur a est la plus haute fréquence scalaire pour laquelle Hui> 0. Ainsi, seuls quatre fonctions complexes comme un banc de filtres sont nécessaires pour produire huit images résultantes, composées de 4 images de la partie réelle et 4 images de la partie imaginaire de la transformée. Chaque pixel de l'image complexe résultant peut être codé en une valeur binaire représentée dans l'équation (IV.7) en appliquant (the quadrant bit coding)[33].

$$B_{ui}^{\mathrm{Re}} = \begin{cases} 1 si\left(F_{ui}^{\mathrm{Re}}(x) \quad 0\right) \\ 0 si\left(F_{ui}^{\mathrm{Re}}(x) \le 0\right) \end{cases} B_{ui}^{\mathrm{Re}}(x) = \begin{cases} 1 si\left(F_{ui}^{Im}(x) \quad 0\right) \\ 0 si\left(F_{ui}^{\mathrm{Im}}(x) \le 0\right) \end{cases} \qquad \text{(IV.7)}$$

Ce procédé de codage attribue deux bits pour chaque pixel pour représenter le quadrant dans lequel se trouve l'angle de phase. En fait, il fournit également la quantification de la fonction de phase de Fourier. En général, LPQ est une chaîne binaire, présentée dans l'expression (IV.8), obtenue pour chaque pixel par la concaténation des codes quadrant bits réelles et imaginaires des huit coefficients de Fourier.

$$LPQ(x)=\left[B_{u0}^{\mathrm{Re}}(x),B_{u0}^{Im}(x),...,B_{u3}^{\mathrm{Re}}(x),B_{u3}^{Im}(x)\right] \quad \text{(IV.8)}$$

La chaîne binaire est convertie en nombre décimal par l'expression (IV.9) pour produire une étiquette de LPQ. La Figure IV.8 résumel'ensemble de ces étapes.

$$LPQ(x)=\left[B_{u0}^{\mathrm{Re}}(x)+B_{u0}^{Im}(x)\times 2^{1}+...+B_{u3}^{\mathrm{Re}}(x)\times 2^{k-1}+B_{u3}^{Im}(x)\times 2^{k}\right] \quad \text{(IV.9)}$$

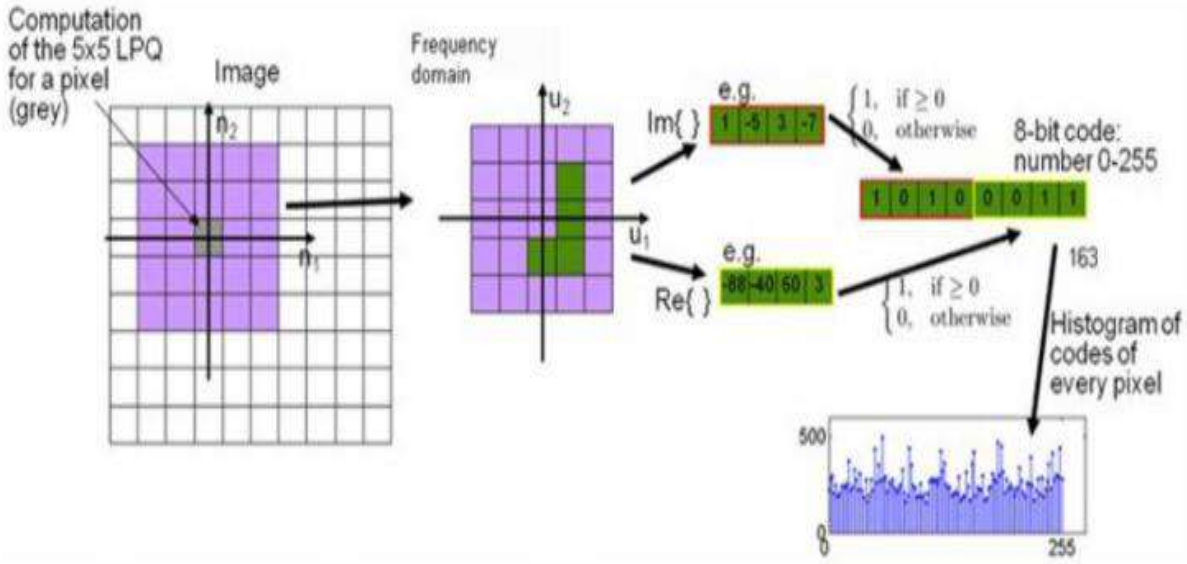


Figure IV.8 : Organigramme de l'ensemble des étapes nécessaire à la construction du descripteur LPQ.

IV.6.Base des donnés

Dans ce chapitre, 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. «Le descripteur de texture Quantification de Phase Locale (ou Local Phase Quantization : LPQ)»".

Nous allons tester et comparer ces descripteurs de texture récents sur des images de données biométriques, à savoir: GPDS-100 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 à la fin de ce chapitre.

IV.7. Méthodologie

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.

Notre système biométrique [34], 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 phase 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 (IV.9).

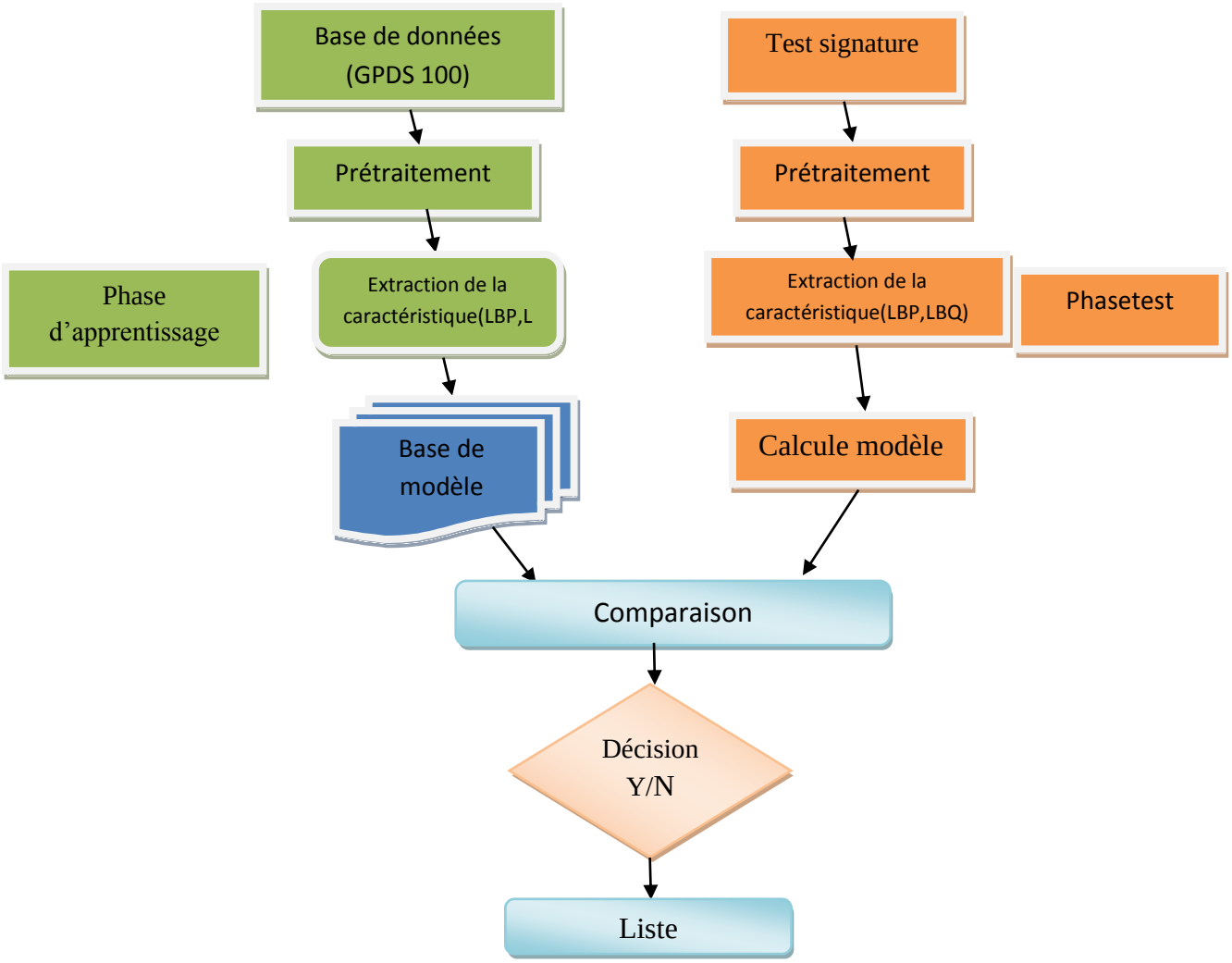


Figure. IV.9. Schéma synoptique de notre système d'identification de signature hors ligne proposé

L'opérateur LBP (ou LPQ) est appliqué à l'image de la signature. Pour chaque bloc, les statistiques de LBP (ou LPQ) sont résumées par histogramme. Le descripteur de signature final est obtenu en concaténant les histogrammes de différents blocs.

IV.8.Résultats expérimentaux et discussion

IV.8.1. Bases de données

Nous avons utilisé la base des données GPDS 100. Elle estnumérisée à 600 dpi, ce qui garantit une représentation suffisante de la texture grise. Dans la base de données GPDS 100, tous les utilisateurs ont signé avec leurs propres stylos sur différentes surfaces. Le corpus de signature GPDS-100 contient 24 signatures authentiques et 30 contrefaçons de 100 individus. Donc, il y a 100 x 24 donnantes 2400 signatures authentiques et 100 x 30 donnantes 3000 contrefaçons [35]. 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.

IV.8.2. Résultats d'identification de signature

Dans ce travail, nous avons testé les résultats de divers descripteurs de texture récents: LBP et LPQ sur la base de données 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 la base de donnée en tant qu'ensemble d'apprentissage et les autres images manuscrites de la même personne«authentique» ont été utilisées comme ensemble de test, sont présentées dans les*Tableaux*(IV.1) et (IV.2).

Différents paramètres de LBP	Extractions des paramètres
LBP (8,1)	92.37
LBP (8.2)	95.85
LBP (8.3)	97.56
LBP (8.4)	98.03
LBP (8.5)	98.30
LBP (8.6)	98.52
LBP (8.7)	98.76
LBP (12,3)	98.86
LBP (16.1)	97.96
LBP (16.2)	98.56
LBP (16.3)	98.86

Tableaux (IV.1) : Résultat de la base GPDS-100, descripteur LBP.

Différents paramètres de LPQ	Extractions des paramètres
LPQ*M*=1	89.64
LPQ*M*=2	94,72
LPQ*M*=3	95.20
LPQ*M*=4	95.97
LPQ*M*=5	96.97
LPQ*M*=6	98.82
LPQ*M*=3	99.10
LPQ*M*=12	99.32

Table IV.2 : Résultat de LPQ descripteur

Lesrésultats des tableaux (IV.1 et IV.2) présentent simultanément la performance de la base GPDS100 avec les deux descripteurs (LBP et LPQ).

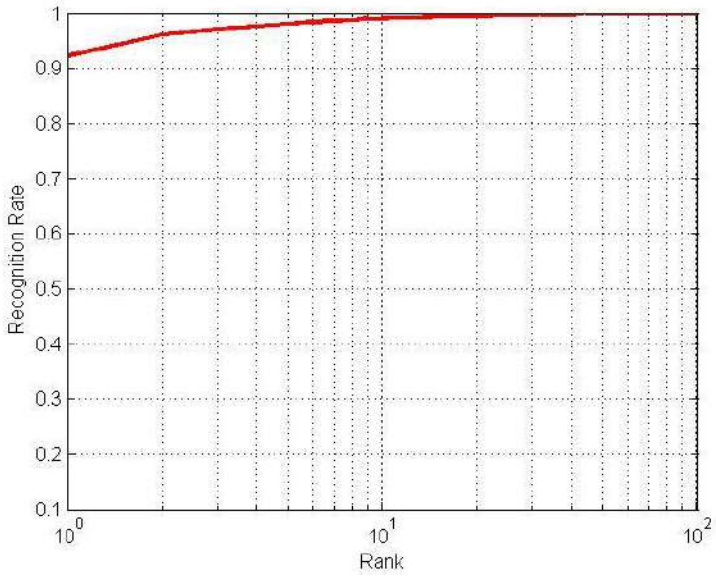


Figure IV.10: Courbe CMC pour LBP Méthode (R=1 et N = 8)

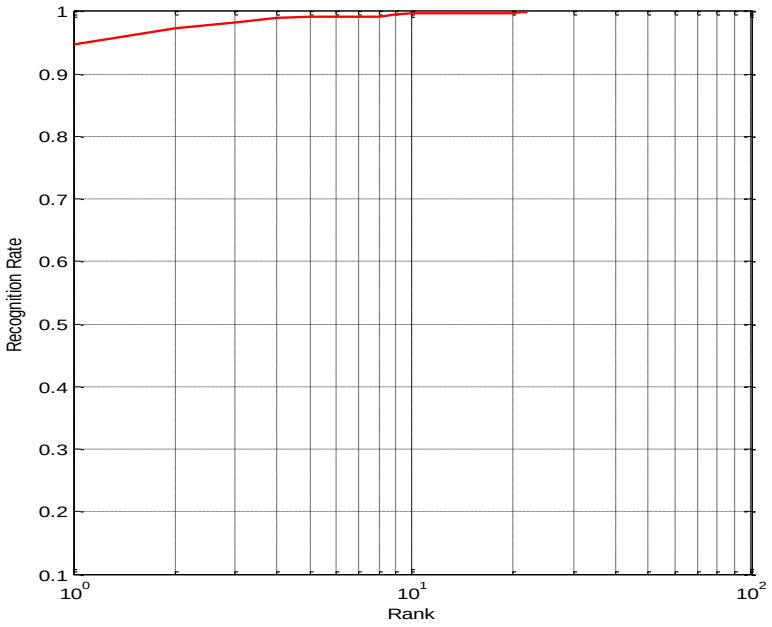


Figure IV.11: Courbe CMC pour LBP Méthode (R=2 et N = 8).

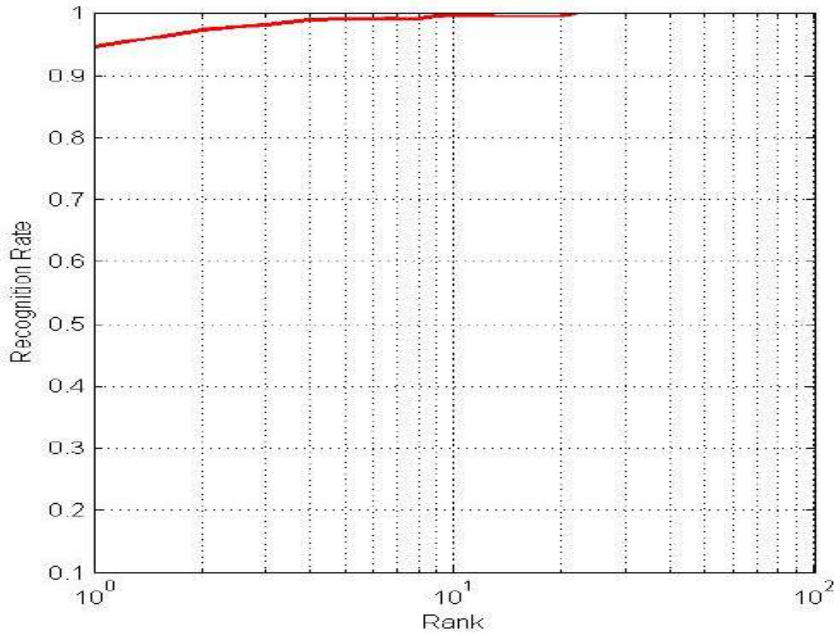


Figure IV.12:Courbe CMC pour $LPQ_{M=2}$Méthode.

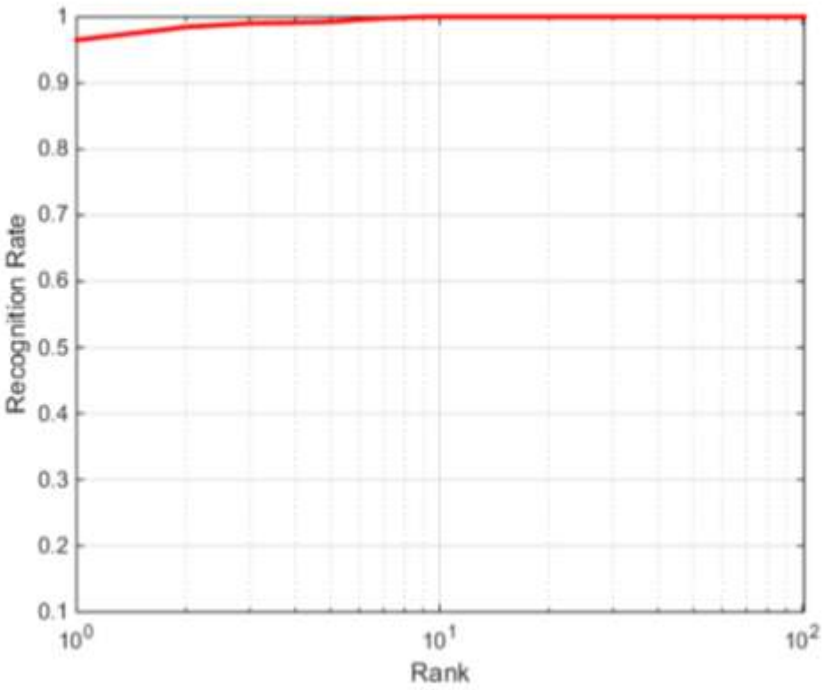


Figure IV.13: Courbe CMC pour $LPQ_{M=6}$ Méthode.

Les figures ci-dessus présentent l'évaluation des résultats de descripteur LBP et LPQ de la base GPDS100.

- **Discussions des résultats expérimentaux**

Selon les tableaux (IV.1 et IV.2), le descripteur LBP donne des résultats impressionnants, suivie par le descripteur LPQ. Parconséquent, la meilleure valeur obtenue par le descripteur LBP est de 98.86% avec LBP (12,3) et (16,3). Et la meilleure valeur obtenue par le descripteur LPQ est de 99.32% avec $LPQ_{M=12}$.

Les critères de comparaison sont le taux d'identification et le temps de calcul. Le but est de sélectionner la meilleure méthode pour concevoir un système d'identification : Et d'après lestableaux précédent (Tableau IV.1 et IV.2) on peut en conclure les résultats, Le temps de calcule du système basé sur la méthode LPQ, est moins grand par rapport au système basé sur la méthode LBP, donc LPQ a donné de bon résultat par rapport LBP (taux d'identification et temps de calcule). D'après ces résultats, le système d'identification est un système fiable.

IV.9. Conclusion

Dans ce chapitre, les résultats expérimentaux présentés ont mené à l'élaboration d'un système d'identification des signatures manuscrites hors ligne. Nous avons expérimentés la base de donnéesGPDS 100. Dans ce système utilisé dans le but d'améliorer et évaluer le taux d'identification et le temps de calcul.Le but est de sélectionner la meilleure méthode pour concevoir un système d'identification. Après, Les résultats sont pris et discutés.

Conclusion générale

La biométrie est un domaine en expansion dont le nombre de recherches est en croissance continue dont le but est d'aboutir à un moyen efficace, fiable et rapide pour identifier les personnes. Elle utilise, des outils mathématiques souvent très développés, pour identifier et reconnaître des individus.

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu. Elle est 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, 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.

Notre travail consiste à la mise au point d'un programme destiné à reconnaître un individu par signatures manuscrites hors ligne. Nous avons expérimentés la base de données GPDS 100. Nous utilisant la méthode «LBQ et LBP», qui se base sur une analyse des informations acquise dans la méthode de prétraitement, ensuite l'extraction des caractéristiques biométriques et puis calculer le taux de reconnaissance en utilisant le logiciel Matlab pour visualiser les résultats à vouloir obtenir. Après, Les résultats sont pris et discutés.
Les critères de comparaison sont le taux d'identification et le temps de calcul. Le but est de sélectionner la meilleure méthode pour concevoir un système d'identification. Et d'après les résultats obtenus on peut en conclu que le temps de calcule du système basé sur la méthode LPQ, est moins grand par rapport au système basé sur la méthode LBP, donc LPQ a donné de bon résultat par rapport LBP (taux d'identification et temps de calcule). D'après ces résultats, le système d'identification est un système fiable et les résultats de reconnaissance sont encourageants.

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

Références Bibliographiques

[1] F. PERONNIN et J. DUGELAY, “Introduction à la biométrie, authentification des individus par traitement audio et vidéo”. Revue Traitement du Signal, Vol.19, No.04, 2002.

[2] S. AKROUF, ”Une Approche Multimodale pour l’Identification du Locuteur”, thèse de doctorat, Université Ferhat Abbas- Sétif , 2011.

[3] S. BOUDJELAL, ”Détection et identification de personne par méthode biométrique ”, Mémoire de magister en électronique, Université de Tizi Ouzo, 2014.

[4] L. ALLANO, ‘La Biométrie multimodale : stratégies de fusion de scores et mesures de dépendance appliquées aux bases de personnes virtuelles’, thèse de doctorat, Université D’Avery Val D’Essonne, 2009.

[5] S. GUERFI ABABSA, ”Authentification d’individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D”, thèse de doctorat, Université D’Avery Val D’Essonne ,2008.

[6] T. AMELLAL, K. BENAKLI, ”Système de reconnaissance de visage basé sur les GMM ”, mémoire fin d’étude d’ingéniera en informatique, Institut National de formation en Informatique (I.N.I) Oued-Smar Alger, 2007.

[7] F. LOUIBA et R. HADJ, ” Système de contrôle d’accès physique basé sur le visage et la Java Card”, mémoire fin d’étude d’ingéniera en informatique, Institut National de formation en Informatique (I.N.I), 2010.

[8] L. MENSSOURA, ‘identification des visages humains par réseaux de nuerons’, mémoire de magister, université de Batna, 2013.

[9] A. BENAGGA et L. TELIB, ” Reconnaissance des personnes basée sur l’empreinte de l’articulation de doigt”, Mémoire de master académique, université KasdiMerbah Ouargla, 2016.

[10] F. DAVOINE, B. ABBOUD et V. MO DANG,’ Face and facial expression analysisbased on an active apparence model ‘, Traitement du signal, Vol.21, No.3, 2004.

[11] CHAA, Mr. Mourad. *Système de reconnaissance de personne par des techniques*
Biométriques. Setif : Université Ferhat Abbas – Sétif-1 -, 2017.

[12] "Molecular Expressions Microscopy Primer: Digital Image Processing – Difference of Gaussians Edge Enhancement Algorithm", Olympus America Inc., and Florida State University Michael W. Davidson, Mortimer Abramowitz

[13] NAVAZ, AS Syed, DHEVISRI, T, et MAZUMDER, Pratap. Face recognition using principal component analysis and neural networks. *March-2013, International Journal of Computer Networking, Wireless and Mobile Communications. Vol*, 2013, no 3, p. 245- 256.

[14] LOUIBA Fadia et HADJ ALI Ryma "Système de contrôle d'accès physique Basé sur le visage" .pp.19 ; 2010.

[15] MORIZET, Nicolas, THOMAS, E. A, ROSSANT, Florence, *et al*. Revue des algorithmes PCA LDA et EBGM utilises en reconnaissance 2D du visage pour la biométrie. *P1-11. Institut Supérieur d'" Electronique de Paris (ISEP), département d'" Electronique*, 2006.

[16] ETEMAD, Kamran et CHELLAPPA, Rama. Discriminant analysis for recognition of humane face images. *Josa à*, 1997, vol. 14, no 8, p. 1724-1733.

[17] YU, Pengfei, YU, Pengcheng, et XU, Dan. Comparaison of PCA, LDA and GDA for palmprint vérification. In : *2010 International Conférence on Information, Networking and Automation (ICINA)*. IEEE, 2010. p. V1-148-V1-152

[18] BELHUMEUR, Peter N, HESPANHA, João P, et KRIEGMAN, David J. Eigen faces vs. fisherfaces: Recognition using class spécifie linear projection. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, 1997, no 7, p. 711-720.

[19] YANG, Ming-Hsuan. Kernel Eigen faces vs. Kernel Fisher faces: Face Recognition Using Kernel Méthodes. In : *Fgr*. 2002. p. 215.

[20] SWATI, M. R. et RAVISHANKAR, M. Finger Knuckle Print recognition based on Gabor feature and KPCA+ LDA. In : *2013 International Conference on Emerging Trends in Communication, Control, Signal Processing and Computing Applications (C2SPCA)*. IEEE, 2013. p. 1-5.

[21] CHOMBOON, Kittipong, CHUJAI, Pasapitch, TEERARASSAMEE, Pongsakorn, *et al*. An empirical study of distance metrics for k-nearest neighbor algorithme. In : *Proceedings of the 3rd International Conference on Industrial Application Engineering*.
2015. p. 1-6.

[22] J. Carbonnier, "Droit Civil, Introduction", PUF, collection Thémis, 25ème édition,198 p., 1997.

[23] Commission Nationale de l'Informatique et des libertés (CNIL), http://www.cnil.fr

[24] O. Iteanu, "Biométrie, une technologie sous surveillance?", http://solutions.journaldunet.com/0502/050209_juridique.shtml, 2005.

[25] CNIL, délibération 04-018 du 8 avril 2004.

[26] 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.
[27] R. Sabourin, G. Genest et F. J. Prêtreux, "Off-Line Signature Vérification by Local
Granulométrique Size Distribution", IEEE Transactions on Pattern Analysais and Machine
Intelligence, vol. 19, no. 9, pp. 976-988, 1997.

[28] C. Santos, E.J.R. Justino, F. Bortoluzzi 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.

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

[30] Razafimanantsoa herilanja todisoa. ‘ Reconnaissance de la signature manuscrite a base des réseaux de neurones feed-forward couplée avec la méthode d'Otsu par traitement d'image’ université d'Antananarivo, mémoire master 2015].

[31] THÈSE Présentée en vue de l’obtention du diplôme en Electronique Doctorat 3ème Cycle en LMD, Présentée par : Hedjaz HEZIL. THÈSE dirigée par : Rafik DJEMILI Professeur des Universités Skikda

[32] Ojala, T., Pietikäinen, M., Mäenpää, T.: Multi résolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Transe. Pattern Anal. Mach.Intell. 24(7), 971–987 (2002)].

[33] V. Ojansivu and J. Heikkilä, "Blur Insensitive Texture Classification Using Local Phase Quantization," in Image and Signal Processing. vol. 5099, A. Elmoataz, O. Lezoray, F. Nouboud, and D. Mammass, Eds., ed: Springer Berlin Heidelberg, 2008, pp. 236-243.

[34] L. BOUCERREDJ.al. ‘’Etude de la fiabilité d’un système biométrique dédie à la reconnaissance de signatures manuscrites’’. Séminaire international sur l’industrie et la technologie en ligne (webinaire),12 et 13 Mars 2021, Oran, Algerie

[35]. 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.