REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITE AKLI MOHAND OULHADJ-BOUIRA

Faculté des Sciences et Sciences Appliquées
Département Génie électrique

Mémoire de fin d'études

En vue de l'obtention du diplôme de **Master en :**

Filière : Electronique

Option : Electronique des Systèmes Embarqués

Réalisé par :

AKLI RACHIDA **DJEMA SABRINA**

Soutenu le : 27/ 12/ 2020

Thème :

Réalisation d'un système d'identification des individus par signature électronique

Devant le jury composé de :

Dr. Kasmi Réda	MCA	UAMOB	Président
Dr. Benzaoui Amir	MCA	UAMOB	Encadreur
Mr. Ladjouzi Samir	MAA	UAMOB	Examinateur

Année Universitaire 2019/2020

Remerciements

Nous tenons tout d'abord à remercier ALLAH le tout-puissant de nous avoir donné le courage et la patience pour mener bien ce modeste travail, qu'il soit béni et glorifié

Nous adressons également nos remerciements au Dr. Amir Benzaoui, pour avoir accepté d'être notre encadreur. Nous le remercions aussi pour ses conseils, ses corrections et ses orientations.

Nous tenons aussi à exprimer nos remerciements les plus respectueux aux membres du jury.

Merci

Dédicace

.

Je dédie ce modeste travail à mes parents qui m'ont donné la vie, qui s'est sacrifié pour mon bonheur et ma réussite

A *mes sœurs, mes frères, et ma grande famille paternelle et maternelle.*

A *mon amie et mon binôme Rachida.*

A *mes amis ainsi qu'à toutes les personnes que j'ai connus, qui m'ont aidé, soutenu et encouragé.*

Sabrina

Dédicace

Je dédie ce modeste travail avant tout à ma mère qui a sacrifié pour mon bien et qui a éclairé ma route par sa compréhension et son soutien.

A

- Mes chers frères et mes chères sœurs qui m'ont soutenu et encouragé pendant la réalisation de mon travail

-Mon binôme Djema Sabrina.

-A tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible.

Rachida

Table des matières

Chapitre I:Notions de base sur la biométrie

Chapitre II: Reconnaissance de la signature manuscrite

Chapitre III: Etude expérimentale & résultats

Liste des figures

Chapitre I : Notions de base sur la biométrie

Chapitre II: Reconnaissance de la signature manuscrite

Chapitre III: Etude expérimentale & résultats

Liste des tableaux

Liste des abréviations

ADN: Acide Désoxyribonucléique

PIN: Personal Identification Number

FRR: False Rejection Rate

FAR: False **A**ccept **R**ate

EER: Equal Error Rate

PDA: Personal Digital Assistant

ACP: Analyse en Composantes Principales

ADL: Analyse Discriminante Linéaire

LBP: local Binary Pattern

SVM: Support Vector Machine

AAM: Active Appearance Models

EGM: Elastic Graph Matching

EBGM: Elastic Bunch Graph Matching

LG-PCA: Algorithme Log Gabor PCA

K-NN: Nearest Neighbors

MCYT: Ministerio de Ciencia y Technologia

Introduction générale

Introduction générale

La sécurité est devenue aujourd'hui une préoccupation majeure au niveau international et elle fait l'objet d'une attention particulière; la nécessité de la protection civile et la lutte contre les fraudes d'une part et l'explosion de l'informatique et la croissance des moyens de communication d'autre part. L'identification des personnes constitue un élément-clé dans les systèmes de sécurité, l'avantage de cette identification est que chaque individu à ses propres caractéristiques physiques qui ne peuvent n'être ni changer, ni perdues, ni volées, face à cette sollicitation grandissante, plusieurs méthodes de la *biométrie* et de *reconnaissance biométriques* ont été proposées.

La biométrie est la science permettant l'identification des individus à partir de leurs caractéristiques physiologiques et /ou comportementale qui est spécifique pour chaque personne telle que la signature manuscrite, les empreintes digitales, la géométrie de la main ou de sa paume, la numérisation de l'iris, la reconnaissance faciale et la reconnaissance de la voix.

Un système de contrôle biométrique est un système automatique de mesure basé sur la reconnaissance des caractéristiques propres à l'individu et peut utiliser des capteurs appropriés pour acquérir des données biométriques et les représenter sous forme numérique. En effet, ce système peut fonctionner en mode identification ou en mode vérification. En matière d'identification, les données capturées sont comparées à chaque information stockée dans la base de données. Autrement, dans le cas d'une vérification le système compare les données obtenues à partir de l'information entrée avec la donnée enregistrée [1].

Dans notre travail, nous nous intéressons à l'emploi de la signature manuscrite comme modalité biométrique pour l'identification qui permet d'inclure des signatures scannées ou numérisées. Selon la méthode d'acquisition de la signature, un système peut être classé en hors ligne ou en ligne. Là hors ligne est récupérée à partir des documents par numérisation alors que la en ligne est écrite directement sur un dispositif par un stylo dédié.

Dans notre projet, nous allons réaliser un système d'identification biométrique, à savoir la signature manuscrite hors ligne, cette dernière est l'une des caractéristiques biométriques les plus efficaces, populaires et les plus anciennes pour identifier les individus et les documents. L'objectif de notre travail consiste à augmenter le taux de reconnaissance ou bien

le taux d'identification et pour réaliser ce but nous avons utilisé la méthode (LBP) pour extraire les caractéristiques, et les raisons qui nous ont poussées à l'appliquer sont dues à sa grande performance dans la reconnaissance des signatures, l'efficacité et la simplicité des calculs, et elle est bien adaptée aux tâches exigeantes d'analyse d'image.

Ce mémoire est organisé en trois grands chapitres:

Dans le premier chapitre, nous présenterons les notions de bases de la biométrie ainsi que ses caractéristiques principales. Nous aborderons aussi les principes généraux de fonctionnement des systèmes biométriques, les différentes modalités biométriques, et l'évaluation des performances.

Dans le second chapitre, nous définissons l'état de l'art de la reconnaissance par signature manuscrite hors ligne et son mode de fonctionnement (Acquisition, prétraitement, et extraction des caractéristiques), par la suite l'apprentissage et classification, et finalement la décision.

Le dernier chapitre est consacré à la présentation de notre travail. Nous détaillons le système proposé en mettant en évidence nos contributions. Ce chapitre se compose de deux parties. Dans la première partie, nous présentons le processus général du système de reconnaissance ainsi que la base de données utilisées (MCYT_75) et le protocole d'évaluation implémenté dans le cadre de ce travail. Dans la deuxième partie, nous discutons sur les résultats expérimentaux obtenus dans chaque expérimentation par l'analyse de sa performance.

Nous clôturons ce mémoire par une conclusion générale et la présentation de quelques perspectives.

Chapitre I

I.1. Introduction

Depuis quelques années, les dispositifs connectés occupent une place de plus en plus importante dans notre quotidien. L'utilisation massive de ces objets pose en évidence un problème inédit, celui de la protection des données. C'est avec l'apparition de ce nouvel enjeu de sécurité que les systèmes biométriques ont connu un grand essor [1].

La biométrie est considérée comme un moyen efficace pour l'identification des individus, elle est utilisée dans un nombre important de domaines, allant de nos smartphones à nos papiers d'identité. Cette identification peut se faire de différentes manières :

- L'empreinte digitale.
- L'iris.
- L'ADN.
- La reconnaissance vocale.
- La géométrie de la main.
- La dynamique de frappe au clavier.

Dans ce chapitre, nous commencerons par voir différentes notions et définitions de base liées à la biométrie. Nous analyserons ensuite l'architecture de ses systèmes ainsi que les outils utilisés pour mesurer leurs performances. Nous nous concentrerons plus spécifiquement sur certains domaines d'application. Enfin, nous terminerons avec une comparaison et une conclusion sur ce vaste domaine (biométrie).

I.2. Définition

Le mot ***biométrie*** signifie littéralement « mesure du vivant » et désigne l'étude qualitative des êtres vivants. On utilise cette notion de biométrie pour identifier un individu grâce à ses caractéristiques morphologiques. Pour être efficace, ses caractéristiques doivent répondre à différents critères : Elles doivent être universelles (mesurables chez tous les individus), uniques (permettre de différencier un individu par rapport à un autre), permanentes (même si elles peuvent varier dans le temps), et enfin facile à modéliser [2].

Les lecteurs biométriques sont parmi les dispositifs de sécurité les plus fiables qui existent. En diminuant grandement les risques d'oubli de code, de vol ou de perte qu'on retrouve habituellement sur les systèmes de sécurité classiques, ex : Clé, badge d'accès, carte bancaire… Grâce à ces techniques, on peut s'identifier de manière plus fiable et ainsi mieux contrôler l'accès à certains lieux ou services.

I.3. Les systèmes biométriques

Un système biométrique est un système de reconnaissance qui permet de capter les données biométriques d'un individu, de les extraire et finalement d'en comparer les caractéristiques avec celles déjà mémorisées dans la base de données [3], ce type de système est composé de quatre principaux modules :

I.3.1. Le module de capture

Il correspond à la lecture de certaines caractéristiques morphologiques, comportementales, ou biologiques d'une personne, au moyen d'un terminal de capture biométrique (un lecteur d'empreintes, un scanner, un appareil photo ou tout autre module de capture).

I.3.2. Le module d'extraction

Il prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente à comparer avec les données déjà acquises.

I.3.3. Le module de correspondance

Appelé aussi le module de comparaison, il extrait et compare les caractéristiques biométriques d'une personne soumise au contrôle avec informations stockées dans la base de données. Cette comparaison permet de vérifier « la signature » et détermine le degré de similitude entre la donnée testée et celle déjà existant dans la base de données. Cette comparaison peut se faire de deux manières, soit par ***vérification*** pour une identité proclamée par la personne testée soit par ***identification*** pour retrouver l'identité recherchée.

I.3.4. Le module de décision

Généralement, il vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et les modèles stockés (bases de données) qui permettent au système de prendre la décision appropriée selon les exigences de l'application [3].

I.4. Architecture des systèmes biométriques

Un système biométrique est un système de reconnaissance des formes qui utilise les données biométriques d'un individu, ils peuvent fournir *trois modes de fonctionnement*, à savoir : le module d'apprentissage appelé aussi module d'enregistrement ou d'enrôlement, et celui de reconnaissance (identification ou vérification), et enfin le module d'adaptation.

I.4.1. Module d'apprentissage

C'est la première phase de tout système biométrique, elle s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données (ex, nom, numéro d'identification personnelle (PIN), adresse, etc…) [4].

Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signature), et enfin stockées dans la base de données (**figure.I.1)**.

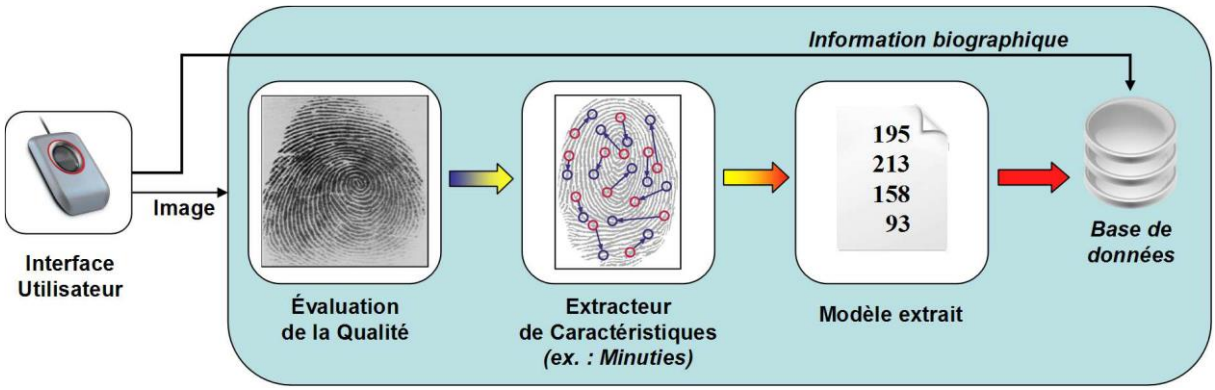


Figure.I.1: Le mode d'apprentissage

I.4.2. Module de reconnaissance (vérification ou identification)

Un système biométrique peut fonctionner en mode ***vérification*** ou en mode ***identification***.

En mode **vérification**, le système effectuera une comparaison de type **un-contre-un** (1:1). En général, lorsque nous parlons de vérification, nous supposons que le problème est *ouvert* puisque nous supposons qu'un individu qui n'a pas de modèle dans la base de données (*Imposteur*) peut chercher à être reconnu. Et en résumé, le système doit alors répondre à la question suivante: « Suis-je bien la personne que je prétends être ? » [4].

En mode **identification**, le système doit déduire l'identité de la personne. En d'autres termes, il répond à une question de type : « Qui suis-je ?». Il s'agit d'une comparaison entre le signal mesurée et les différents modèles contenus dans la base de données, c'est une comparaison de type **un-contre-N**.

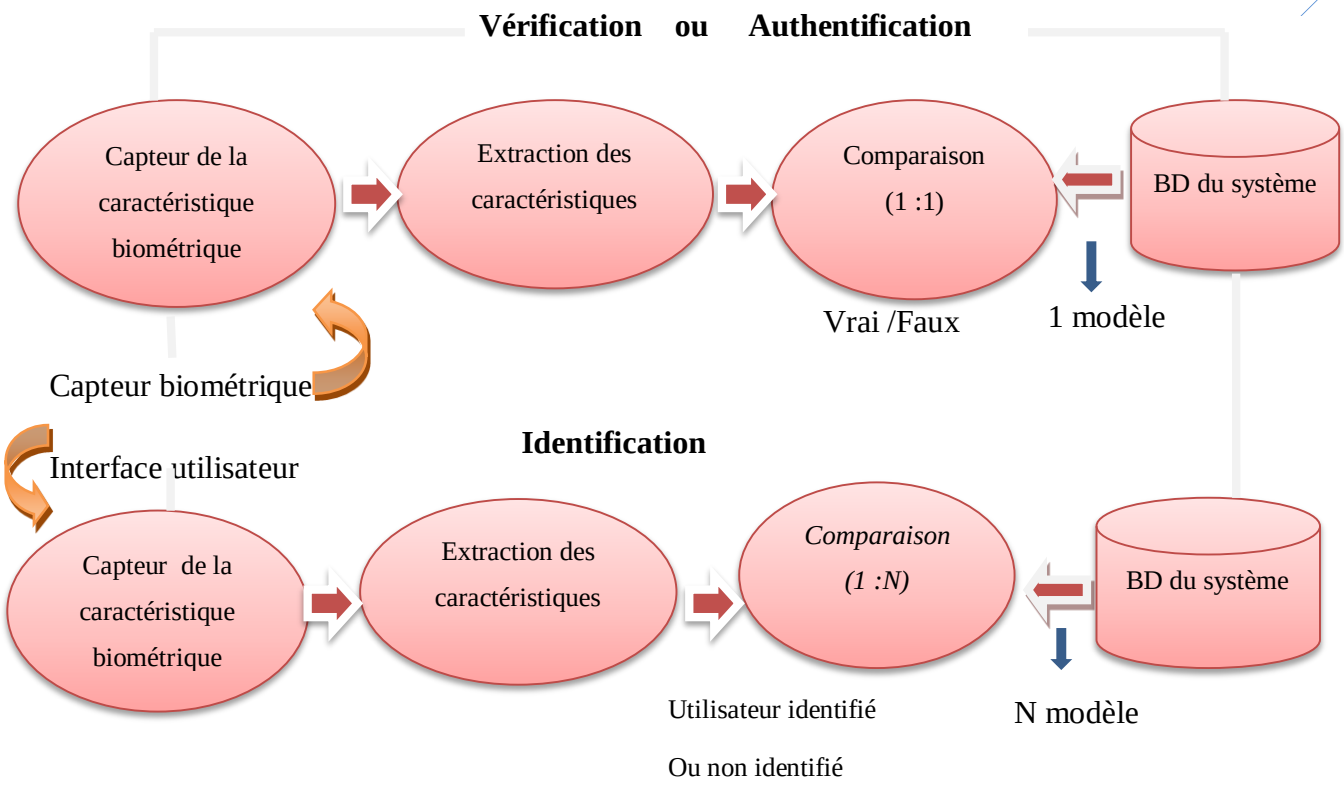


Figure.I.2: Architecture d'un système de reconnaissance biométrique (ou vérification).

I.4.3. Module d'adaptation

Dans la phase d'apprentissage, les systèmes biométriques ne capturent généralement que quelques instances du même attribut pour limiter l'inconfort de l'utilisateur. Il est difficile d'établir un modèle général qui peut décrire toutes les modifications possibles de cet attribut. De plus, les caractéristiques de cette modalité biométrique et ses conditions d'acquisition peuvent être différentes. Par conséquent, des ajustements doivent être faits pour maintenir et améliorer les performances du système après utilisation. L'adaptation peut se faire en mode supervisé ou non supervisée mais le deuxième modèle est en fait le plus utile à l'heure actuelle. Si un utilisateur est reconnu par le module de reconnaissance, les paramètres extraits du signal seront utilisés pour ré-estimer son modèle. Fondamentalement, le facteur d'adaptation dépend de la confiance du module de reconnaissance d'identité de l'utilisateur. Bien sûr, l'adaptation sans supervision peut poser un problème en cas d'erreurs du module de reconnaissance [4].

I.5. Evaluation des performances

Quasiment aucun système biométrique ne peut être totalement fiable; il est indispensable alors de prévoir différentes métriques pour évaluer les performances des différentes modalités biométriques. On rencontre rarement deux modèles biométriques du

même utilisateur avec le même vecteur de caractéristiques en raison de mauvaises conditions : changements dans la biométrie des utilisateurs, changements dans les conditions environnementales et interaction de l'utilisateur avec le capteur. La performance du système peut être mesurée principalement sur la base de trois critères : sa précision, sa performance (vitesse d'exécution), et la quantité de données qui doit être stockée pour chaque utilisateur. Nous nous intéresserons plus particulièrement aux critères de l'identification et la vérification [5].

I.5.1. Evaluation de l'identification

Le taux d'évaluation est l'une des mesures la plus utilisée couramment, mais elle peut s'avérer insuffisante, en effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les N premiers. On trace alors le score cumulé qui représente la probabilité que le bon choix se trouve parmi les N premiers.

Dans le cas où il existe plusieurs modèles pour chaque individu dans la base de données, les mesures classiques des systèmes de recherche dans une base de données peuvent être utilisées. Les performances de ce système sont mesurées à l'aide du taux d'identification :

$$\textbf{Taux d'identification}(\%) = \frac{nbre\ de\ tests\ ayant\ amenés\ à\ une\ identification\ correcte}{nbre\ total\ de\ tests} \qquad (I.1)$$

Ce paramètre dépend du nombre de personnes contenues dans la base de données. En effet, plus le nombre de tests est important, plus le taux d'erreurs risque d'être grand.

Les performances d'un système biométrique pour une application donnée sont principalement basées sur le taux d'erreur et le taux d'échec discutés ci-dessus. Les autres facteurs incluent: le coût du système, l'acceptabilité pour chaque utilisateur, la facilité d'utilisation, la fiabilité des capteurs,…peuvent également déterminer la pertinence d'un système biométrique pour une application spécifique.

I.5.2. Evaluation de la vérification

Lorsqu'un système fonctionne en mode vérification, celui-ci peut faire deux types d'erreurs. Il peut rejeter un utilisateur ***légitime*** et dans ce premier cas on parle de *faux rejet* (false rejection). Il peut aussi accepter un ***imposteur*** et on parle dans ce second cas de *fausse acceptation* (false acceptation). La performance d'un système se mesure donc à son *taux de faux rejet* (False Rejection Rate ou FRR).

Le test de vérification est formulé mathématiquement de la manière suivante:

- Soit *Xq* le vecteur de caractéristiques de la personne proclamée I.
- Soit *Xt* le vecteur de caractéristiques de la personne I stocké dans la base de données.
- Soit *S(Xq,Xt)* une fonction de similarité entre les deux vecteurs *Xq* et *Xt.*
- La fonction *S* retourne un score de similarité entre les mesures biométriques de la personne enrôlée et la personne proclamée.
- Le test de vérification est défini par la fonction *(I, Xq)* tel que :

$$(I, Xq)=\begin{cases} W1 & Si\ \ S(Xq,Xt) \leq \theta \\ W2 & Sinon \end{cases} \qquad \text{(I.2)}$$

- Où *W1* indique que la personne proclamée est *authentique* et *W2* qu'elle est *imposteur.*
- θ est la valeur de seuil de décision.

L'évaluation du système biométrique en mode vérification nécessite d'établir une distribution des scores de similitude pour les utilisateurs authentiques grâce à une comparaison *intra-classe* ainsi, d'établir une distribution des scores de similarités des utilisateurs imposteurs par des comparaisons *inter-classes*. Avec ces deux distributions, nous pouvons distinguer deux types d'erreurs de vérification liées à de mauvaises décisions.

- **Le taux de faux rejet** ("**F**alse **R**eject **R**ate" ou **FRR**) : Il peut rejeter un utilisateur légitime.

Ce taux représente le pourcentage de personnes censées être reconnues, mais qui sont rejetées par le système, il est défini par :

$$\text{FRR}(\%)=\frac{nbr\ de\ faux\ rejets}{nbr\ de\ clients\ présentés} \qquad \text{(I.3)}$$

- **Le taux de fausse acceptation** ("**F**alse **A**ccept **R**ate" ou **FAR**) : Il peut aussi accepter un imposteur.

Ce taux représente le pourcentage de personnes censées à ne pas être reconnues, mais qui sont tout de même acceptées par le système, il est défini par :

$$\text{FAR}(\%)=\frac{nbr\ de\ fausses\ acceptations}{nbr\ de\ clients\ présentés} \qquad \text{(I.4)}$$

La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptance Rate ou FAR).

- Le taux d'égalité des erreurs ("Equal Error Rate" ou EER)

Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courante. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

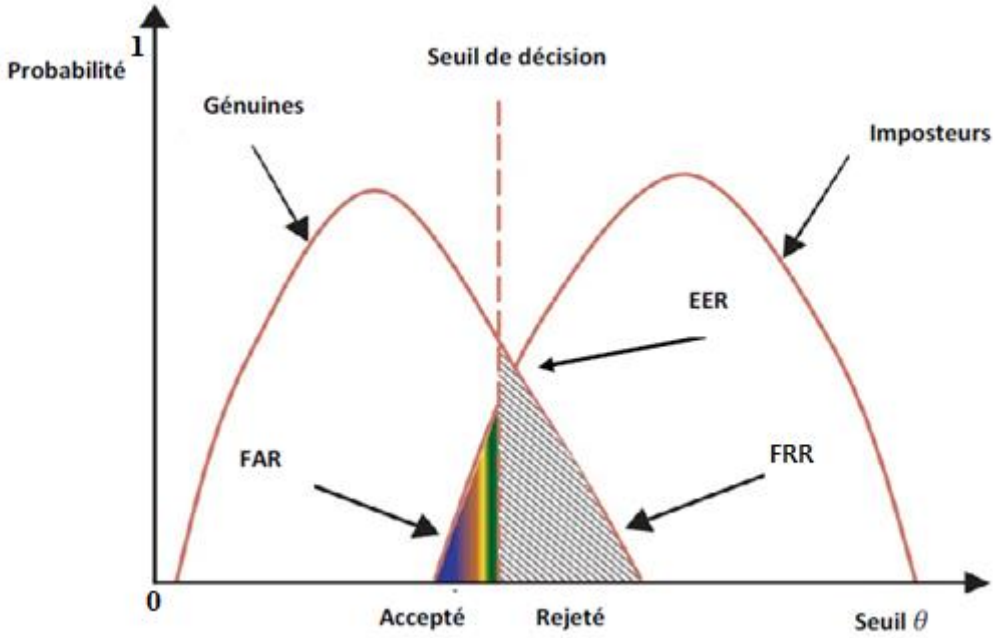


Figure.I.3: Distributions des imposteurs et authentiques en mode de vérification, et le point d'équivalence des systèmes biométriques**.**

I.6. Applications de la biométrie

De nos jours, on retrouve la reconnaissance biométrique dans différents domaines et pour différents buts. On peut citer les applications bancaires, la gestion de l'identité, et le contrôle d'accès dans certains bâtiments.

Ainsi, la biométrie offre un large éventail de techniques pour diverses applications. Les domaines où la biométrie se développe peuvent être divisés en trois grandes catégories :

I.6.1. Applications commerciales

Tels que les coffres-forts avec serrure électronique, accès à un réseau informatique, la sécurité des données électroniques, commerce en ligne, la carte de crédit, le smartphone, tous les logiciels utilisant un mode passe, le contrôle d'accès, la gestion des dossiers médicaux, etc…

I.6.2. Applications gouvernementales

Telles que le permis de conduite, le passeport, la carte d'identité nationale, la sécurité sociale, le contrôle des frontières, la gestion des droits d'accès dans les établissements correctionnels et prisons, les peines d'assignation à résidences, les enquêtes judiciaires, l'identification et l'authentification des criminels avec une grande précision, etc…

I.6.3. Applications légales

Telles que l'identification de corps humains, les enquêtes criminelles, les tests de parentalités, la recherche d'enfants disparus, etc…

La polymorphe des applications situent ci-dessus, explique la polyvalence et la large gamme de facilité d'utilisation des systèmes biométriques qui permet d'accroître la sécurité et réduire l'obligation de garder les clés, de se souvenir des mots de passe, etc [6].

I.7. Panorama de différentes modalités biométriques

À l'heure actuelle, il existe une gamme assez large de modalités biométriques et elle s'élargit de plus en plus. Chacune possède ses avantages et inconvénients selon le cadre d'utilisation. Certaines peuvent être fiables mais très contraignantes (coût élevé et collaboration des personnes indispensables dans la plupart des cas). Tandis que d'autres sont plus ergonomiques mais moins efficaces. Certaines méthodes ont déjà été déployées à grande échelle. Et pour bien déterminer la convenance des modalités physiques ou comportementales, nous allons parcourir sept critères qui vont nous permettre de juger de la pertinence d'une solution par rapport à une autre :

- **Universalité :** existe chez tous les individus.
- **Unicité :** possibilité de différencier un individu par rapport à un autre.
- **La permanence :** le trait biométrique ne varie pas ou cours du temps.
- **Mesurabilité :** les données biométriques peuvent être acquises et numérisées simplement.
- **La performance :** l'authentification doit être fiable.
- **La robustesse :** résilience face aux facteurs extérieurs.
- **Acceptabilité :** les utilisateurs doivent accepter le partage des traits biométriques.
- **Circonvention :** combien il est facile d'imiter le facteur biométrique.

Toutes les modalités utilisées dans les systèmes biométriques répondent à ces critères mais à des degrés différents. Selon les besoins de l'application, un compromis doit être trouvé dans le choix de la méthode à adopter [7].

Nous définirons quelques modalités biométriques dans les paragraphes suivants pour essayer de mettre en évidence la performance et la fiabilité de chaque technique.

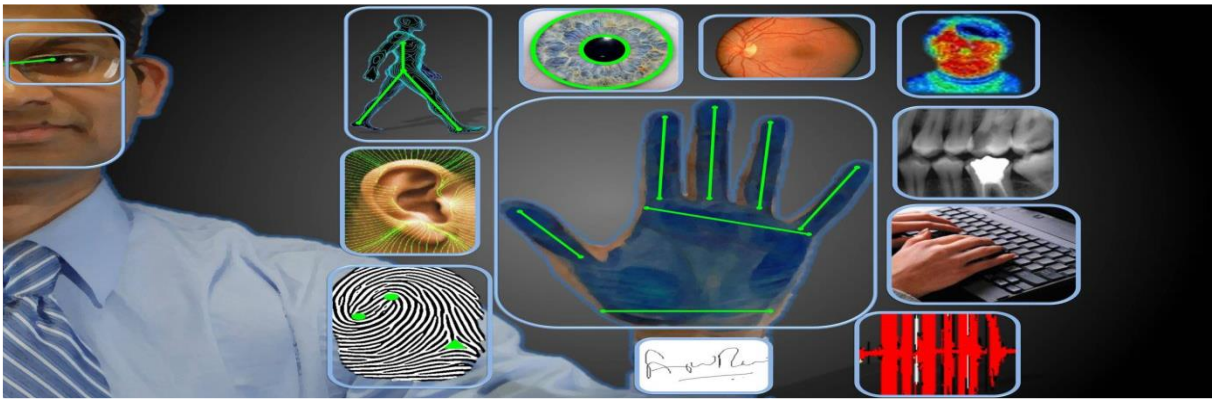


Figure.I.4: Quelques modalités biométriques.

I.7.1. Les empreintes digitales

L'empreinte digitale est le dessin formé par les lignes de la peau des doigts, des creux et des bosses **(figure.I.5)**. Ses caractéristiques sont uniques pour chaque individu. Une fois les empreintes formées, elles ne changent plus et deviennent donc immuables. Ses caractéristiques offrent un moyen de reconnaissance très fiable [8]. De nos jours, la reconnaissance des empreintes digitales est la méthode biométrique la plus répandue. En effet, l'intégration des lecteurs d'empreintes digitales sur des micro-ordinateurs ou des téléphones portables permet d'en sécuriser son utilisation. Cette méthode est très populaire car elle est très simple à employer. L'utilisation de multiples empreintes digitales pour une même personne fournit des informations supplémentaires permettant une identification plus précise. Mais à grande échelle, elle implique la création d'un grand nombre d'identités [9]. Par conséquent, on peut observer deux inconvénients à cette méthode ; la collaboration nécessaire des individus ainsi que la mobilisation de ressources informatiques importantes. Avec une moindre probabilité, un autre point faible serait la possibilité de la détérioration des empreintes suite à un traumatisme physique.

Figure.I.5: Système biométrique basée sur les empreintes digitales.

I.7.2. La géométrie de la main

La biométrie par la géométrie de la main est également une méthode assez populaire. Elle consiste en la prise d'un certain nombre de mesures des caractéristiques osseuses de la main, comme la forme des articulations, la longueur et la largeur des doigts. Cette technique est très simple à utiliser, d'un coût abordable et facilement acceptable par l'utilisateur. En comparaison avec d'autres systèmes de biométrie, la géométrie de la main est légèrement déficiente. En effet, les caractéristiques géométriques de la main ne sont pas totalement fiables. Elles peuvent changer au cours du temps, elles ne deviennent immuables qu'à l'âge adulte. De plus, ces dispositifs utilisant la main peuvent être trompés en utilisant une main factice qui reproduit les caractéristiques de la main d'un individu autorisé. Comme la montre la **figure.I.6**, la taille des dispositifs utilisant cette technique est imposante, il est donc difficile de les imaginer son intégration dans des équipements de la vie courante (téléphone, ordinateurs portables) [10].

Figure.I.6: Système biométrique basé sur la géométrie de la main.

I.7.3. Le visage

La reconnaissance faciale est une modalité biométrique qui se présente comme étant une alternative intéressante car elle est non invasive et facile à utiliser. L'intérêt pour cette méthode est grandissant aussi bien dans le secteur privé que le public. Techniquement, les données sont générées à partir de certains traits caractéristiques du visage: les yeux, la bouche, le nez, les sourcils, les lèvres, les oreilles, etc. Cependant, la difficulté avec cette méthode réside dans la captation des données, elle exige des conditions idéales pour les acquérir. En effet, le système peut être sensible à plusieurs aléas environnementaux, comme la lumière ou l'expression du visage. Dans la pratique, les systèmes de reconnaissance faciale doivent pouvoir identifier des visages présents à partir d'une photo ou vidéo et ce de manière automatisée. Le module d'acquisition, doit d'abord détecter le visage parmi une multitude de détails. Ensuite, le module de reconnaissance va l'examiner pour extraire une signature du visage. Pour finir, on compare la signature avec celles stockées en base de données [11].

Figure.I.7: La reconnaissance de visage.

I.7.4. L'iris

La technique d'identification par l'iris est considérée l'un des techniques répondantes le mieux à ce besoin. En exploitant un grand nombre de paramètres, elle offre l'avantage de pouvoir gérer l'identification ainsi que l'authentification. L'iris est la zone colorée entourant la pupille. L'aspect et la forme générale de l'iris se forment dès le stade embryonnaire chez les individus. Le dessin formé par l'iris ne varie que très peu durant la vie d'un individu (stable après les deux années premières). Ce dessin complexe est unique pour chaque personne, chaque œil, même chez les jumeaux. La caractéristique qui varie de plus est le diamètre de la pupille qui est sensible à l'éclairage environnant, qui peut être un obstacle pour son exploitation la plus précise [12].

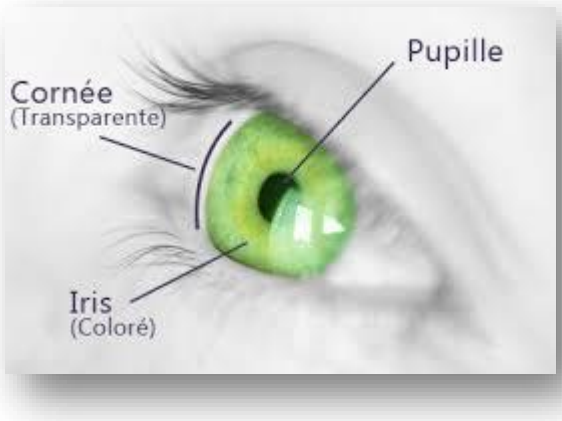


Figure.I.8: Système biométrique basé sur l'iris**.**

I.7.5. La signature électronique

La signature électronique est devenue une nécessité avec l'avènement des systèmes informatiques et la dématérialisation. En effet, elle est le moyen le plus utilisé pour authentifier et signer des documents. L'un des grands avantages de cette méthode est qu'elle ne nécessite aucun apport technologique ou d'équipement, ce qui la rend très facile à mettre en œuvre.

La signature électronique est une façon d'authentification, elle permet de vérifier l'identité d'un individu et l'intégrité d'un document électronique de type mail, pdf…Par comparaison avec la signature manuscrite, il s'agit d'un mécanisme d'engagement fiable faisant appel à des techniques cryptographiques. Elle est très utilisée par les entreprises et les administrations pour gagner du temps dans leurs échanges de documents, réduire les impressions papier et gagner du temps [13].

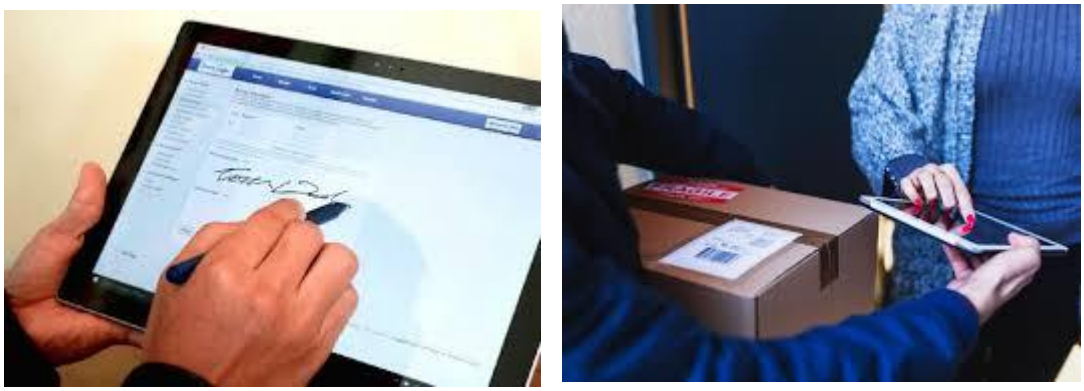


Figure.I.9: Système biométrique basé sur la signature électronique.

I.7.5. La voix

La biométrie de la voix vise à reconnaitre et analyser les caractéristiques de la voix humaine. Elle peut être constituée de composantes physiologiques et/ou comportementales. En effet, plusieurs caractéristiques de cette technique sont déterminées par le conduit vocal, la bouche, les lèvres, les cavités buccales et nasales. Toutes ses caractéristiques physiologiques sont uniques pour chaque individu, mais d'un point de vue comportemental, la parole évolue au cours du temps et de l'âge. L'état de santé ou émotivité du locuteur est également un facteur de variation. Cette modalité n'est pas intrusive, ne demande aucun contact physique avec le système et il est facile à produire. Il existe plusieurs manières de mettre en œuvre cette reconnaissance, l'individu peut être amené à dire un texte fixe (un mot ou une phrase), un texte prompt (une ou plusieurs phrases à répéter), dans certains cas le locuteur peut parler librement. Malgré tous ses avantages, la biométrie de la voix rencontre des difficultés à cause de la possibilité d'utiliser un enregistrement pour tromper le système, la sensibilité aux bruits environnant lors d'acquisitions, la variabilité due à l'état du locuteur [14].

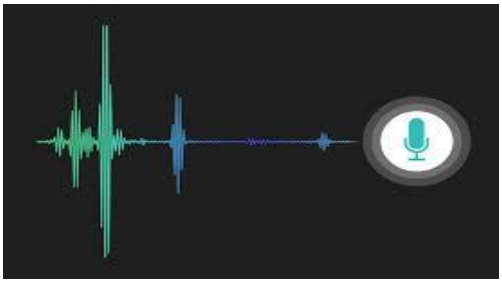


Figure.I.10: Système biométrique basé sur la voix.

I.7.6. La dynamique de frappe au clavier

La biométrie comportementale peut, chez un individu, analyser les caractéristiques de certaine de leurs comportements comme la dynamique de frappe au clavier. Cette technique peut apporter l'authentification d'un individu selon sa manière de taper au clavier. Cette technique n'est pas coûteuse car le matériel d'acquisition ne demande qu'un clavier et un ordinateur et elle est facilement acceptée par les usagers. Les performances de cette modalité sont moindres comparées à d'autres modalités à cause de la forte variabilité des données biométriques, elles peuvent être dues à l'état émotionnel de l'individu ou à une modification volontaire de la manière d'utiliser le clavier [15].

Figure.I.11: Système biométrique basé sur la dynamique de frappe au clavier.

I.7.7. La façon de marcher

La marche ou plutôt la façon de marcher est un moyen fiable pour la reconnaissance des individus et la sécurité des systèmes. En effet, l'entrainement possible de la reconnaissance de démarche réside dans la capacité de reconnaitre (identifier) un individu à distance. Cette modalité comportementale est attentivement associée à la musculature naturelle de l'homme tel que : la vitesse, l'accélération, le mouvement du corps de l'être humain, c'est ce que la rend personnel. Tous ces éléments sont obtenus avec une caméra de surveillance afin de les transmettre à un ordinateur pour l'analyser. Les inconvénients de ce système résident dans sa sensibilité au changement des habitudes, des chausseurs…Et n'est pas permanent (âge, maladie...) [16].

Figure.I.12: Système biométrique basé sur la façon de marcher.

I.8. Pourquoi la signature électronique

De nos jours et de plus en plus des services sont accessibles en ligne (banque, assurance, commerce, etc.)**.** Par conséquent, on retrouve de plus en plus des documents au format numérique. Pour faciliter cet usage, la signature électronique a été mise en place. Elle permet aux usagers d'acquérir et signer ses différents contrats en ligne de manière simple et sécurisée. L'utilisation de la signature électronique biométrique permet d'économiser les coûts en matière d'émission, de gestion et de stockage des documents. Ainsi, peu de temps après la mise en œuvre de cette technique, l'investissement peut être amorti. En effet, grâce à

l'utilisation de la signature électronique, les coûts liés à l'impression, l'archivage et l'acheminement des documents seront considérablement diminués. Elle permet à la fois de rendre certains services plus accessibles et permet aux entreprises et institutions de réaliser des économies d'échelle : le tout dans un cadre où la sécurité est renforcée.

Grace à ces avantages, nous disons que ce sujet revêtant d'une importance capitale qui a attiré notre attention car : il nous permet de connaitre et de comprendre explicitement le fonctionnement d'un système de reconnaissance biométrique en général, et celui de reconnaissance des signatures électroniques en particulier, tout en proposant la sécurité de certains documents de trafic pour minimiser la fraude.

I.9. Comparaison

Une question qui se pose souvent dans ce domaine est la suivante : « Quelle est la meilleure technique biométrique à utiliser ?»

La réponse logique pour cette question est qu'il n'y a aucune meilleure technique biométrique en termes absolus, tout dépond à la précision et à la raison d'exécution de l'application. Le tableau et la **figure.I.13**, illustrent la comparaison entre ces techniques biométriques [17].

Tableau.I.1: Comparaison de différentes modalités biométriques.

les caractéristiques biométriques / Modalité	Universalité	Unicité	Performance	Stabilité	Acceptabilité	Mesurabilité	Circonvention
Empreinte Digital	M	E	M	M	M	E	E
Géométrie de la main	M	M	M	M	M	F	M
Visage	E	E	M	E	E	E	F
Iris	M	E	M	F	F	E	F
Signature électronique	F	E	M	M	M	E	E
frappe sur le clavier	M	M	M	M	E	M	M
Façon de marche	E	M	M	E	E	M	F

(M=Moyen, E=Elevée, F=Faible)

Les systèmes d'identification unimodale ne rassurent pas la reconnaissance des individus avec une précision très élevée, alors que la biométrie multimodale consiste à faire ça et aussi atténuer les limites observées dans ces systèmes, tels que le manque d'individualité, la vulnérabilité aux attaques et la fraude intentionnelle. Ainsi que, la biométrie multimodale se base sur la combinaison de diverses informations de différents sources biométriques, ces sources peuvent être différentes instances de la même modalité comme: plusieurs algorithmes (ex., identification par l'iris à base de deux algorithmes d'appariement), plusieurs captures (ex., capture infra-rouge pour la reconnaissance des visages), plusieurs échantillonnages (ex., reconnaissance du visage en se basant sur les images du visage de face et selon les profils droit et gauche afin de prendre en compte les variations de la pose faciale), plusieurs traits (ex., voix, oreilles), plusieurs unités (ex., l'empreinte de l'index droit et gauche) dans le but

d'améliorer les résultats. Ces avantages apportés par la multimodalité des systèmes biométriques sont obtenus en fusionnant plusieurs systèmes biométriques [18].

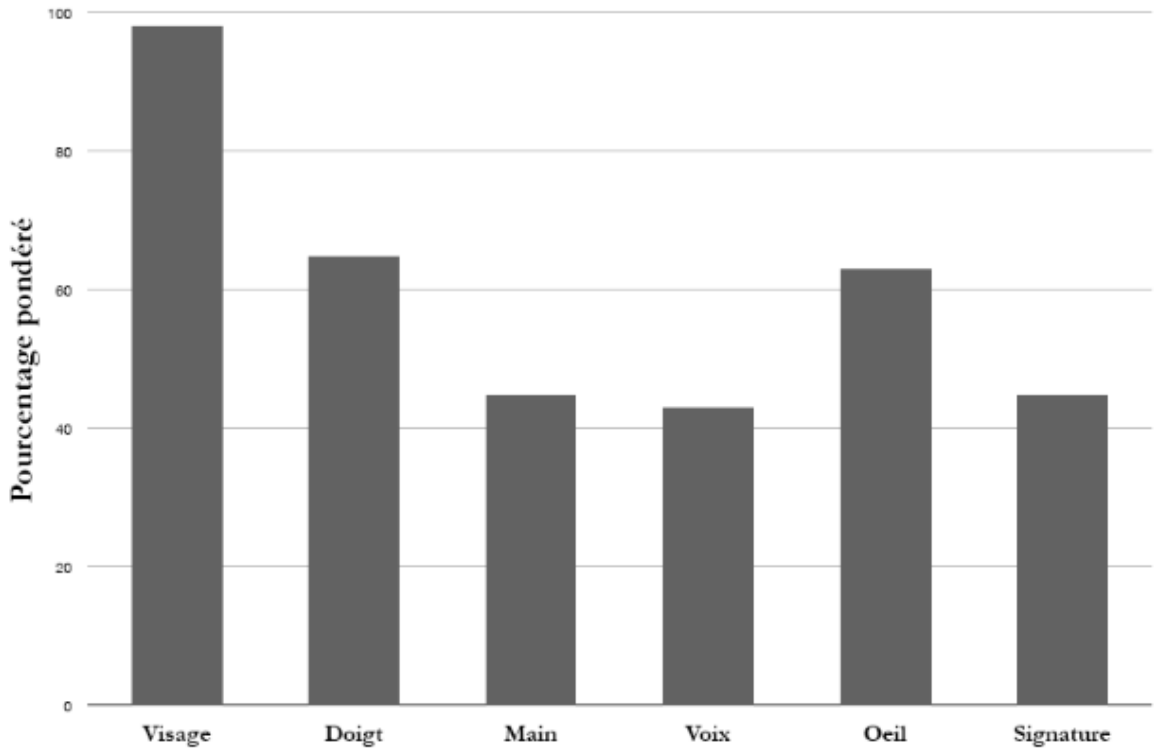


Figure.I.13: Scores de compatibilité pour différentes technologies biométriques dans un système biométrique.

I.10. Conclusion

Dans ce chapitre, nous avons présenté une brève présentation des techniques de la biométrie. Nous avons également établi un aperçu de l'architecture de ses systèmes et de leurs performances. Enfin, nous avons mis en évidence les applications et un panorama des différentes modalités d'usage. Dans le chapitre suivant, nous présentons en détails le principe de fonctionnement des systèmes de reconnaissance biométriques basés sur la signature électronique

Chapitre II

II.1. Introduction

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu. Aujourd'hui, la signature est une pratique réputée dans la vie quotidienne; nous signons pour la validation des contrats, des documents administratifs, des chèques, etc. Dans le domaine de la biométrie, à l'instar des autres techniques biométriques, la signature est utilisée soit pour identifier une personne, soit pour vérifier son identité[19].

Les approches de la vérification de signature se devisent en deux catégories selon l'acquisition des données: en ligne et hors ligne. La différence fondamentale entre eux réside dans l'utilisation de la source à des fins d'identification.

Aujourd'hui, ce thème de recherche reste ouvert afin d'améliorer les systèmes proposés ou d'innover des nouvelles techniques plus efficaces. Dans ce chapitre, nous allons étudier la reconnaissance de signature à partir de la représentation de son processus en détaillant ses étapes: acquisition, prétraitement, extraction de caractéristiques (méthodes globales, locales, et hybrides), par la suite l'apprentissage, la classification, et la décision, et en finissant avec une conclusion.

II.2. Mode de fonctionnement d'un système de reconnaissance de signature

La signature est une caractéristique biométrique comportementale qui permet l'identification ou l'authentification de son propriétaire. Il existe deux types de signature: en ligne et hors ligne [19].

- **La signature hors ligne (statique)**: offline (en anglais), ce modèle de signature ne fournit que sa forme, elle est capturée à l'aide d'un scanner optique pour extraire des caractéristiques statiques qui existent sur l'image numérisée. En effet, il existe deux approches pour la vérification de signature hors ligne: l'approche statique: elle associé des mesures géométriques et l'approche pseudo-dynamique: elle essaie d'apprécier les informations dynamiques à partir de l'image statique.
- **La signature en ligne (dynamique)**: Online (en anglais), différents dispositifs, disponibles sur le marché: les tablettes graphiques, les tablettes PC, les écrans tactiles, et les PDA (Personal Digital Assistant) qui fournit plus à sa forme des propriétés dynamiques telles que la vitesse, la pression, l'accélération, et l'inclinaison de stylo pour chaque point de signature, cela conduit à une meilleure précision.

Un système de reconnaissance par signature comporte plusieurs modules et espaces de travail, tels que le système de reconnaissance de signature hors ligne qui est défini par une suite d'opérations et des étapes illustrées dans la figure suivante. Dans ce qui suit, nous détaillons chacune de ces étapes qu'on va les appliquer sur la base de données MCYT.

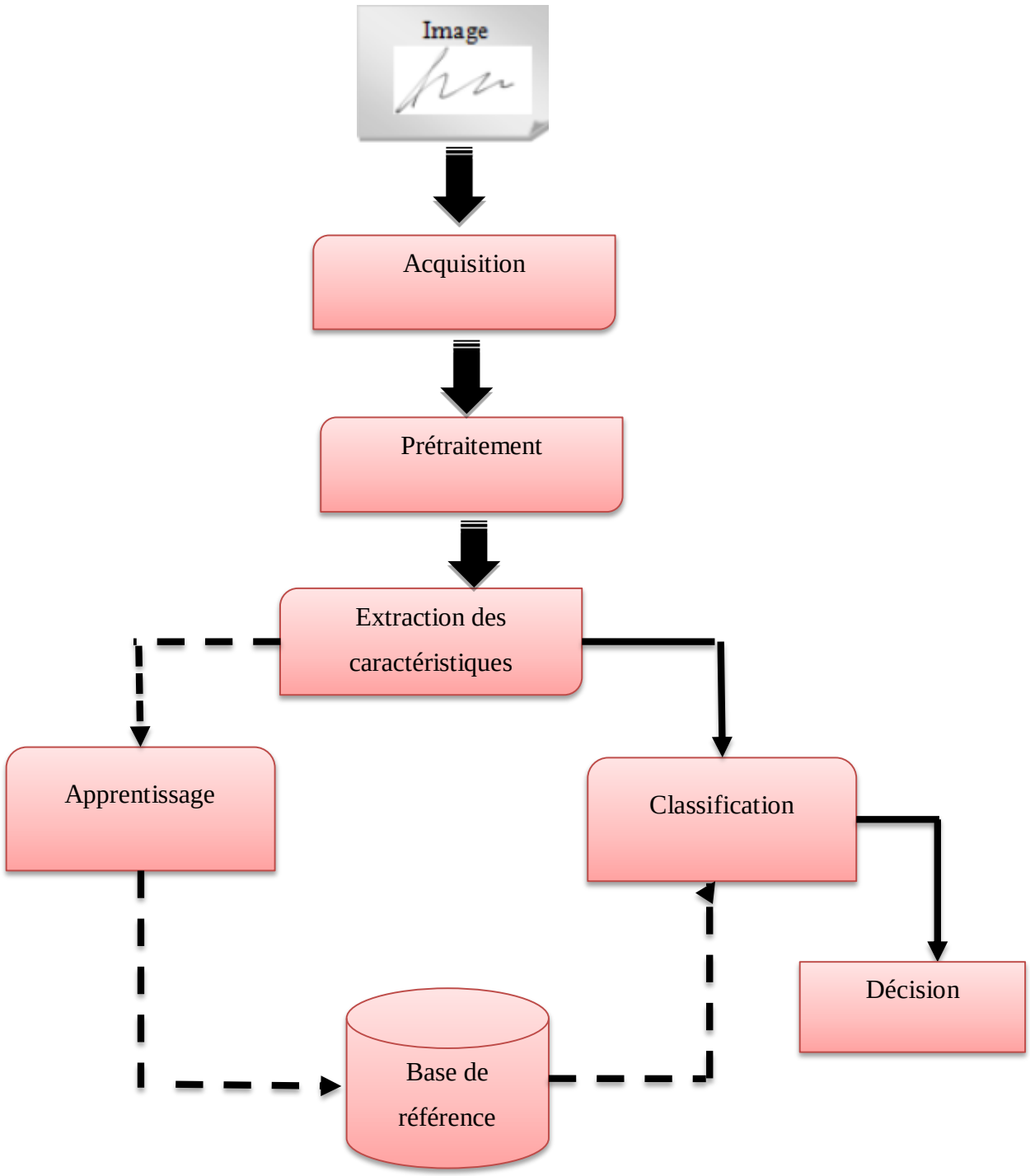


Figure.II.1: Organigramme général d'un système de reconnaissance de signature.

II.2.1. Acquisition d'image

L'acquisition des signatures s'effectue sur un tablet PC, une tablette graphique, ou un PDA. La signature est échantillonnée par le capteur à une fréquence fixe. À chaque point d'échantillonnage, différentes informations sont enregistrées. Ces informations dépendent du type de périphérique d'acquisition de la signature. Pour les PDA et les écrans tactiles, seules les coordonnées x et y, le long de la trajectoire du stylet, et le temps d'acquisition sont fournies. En plus du fitness, les tablettes et tablettes graphiques peuvent également nous offrir la taille de la signature, la pression de chaque point de la signature, et l'angle d'inclinaison du stylo à chaque point de signature (la hauteur et l'azimut du stylo). Ces signaux représentent la personne qui signe numériquement et la signature peut donc être traitée différemment [20].

PDA ANOTO Tablet PC Tablette graphique

Figure.II.2 : Les dispositifs d'acquisition de signature

II.2.2. Prétraitement

L'application d'un prétraitement est conditionnée par le choix des méthodes d'analyse utilisées. Pour faciliter la comparaison, un ré-échantillonnage peut être effectué en utilisant le même nombre de points pour toutes les signatures, quelle que soit leur taille.

Le but de cette méthode est d'éliminer les informations inutiles et améliorer la qualité du signal représentant la signature, améliorant ainsi les performances du système. Le prétraitement est essentiel car il rend le signal indépendant du processus d'acquisition, ne conserve que l'information intéressante pour une analyse plus approfondie. En cas de signature dynamique, plusieurs types de prétraitement ont été appliqués à différentes tâches de recherche. Nous avons trouvé le filtrage (transformée de Fourier), l'élimination du bruit (math), le lissage (filtre gaussien), et la normalisation [20].

Le filtrage: le processus d'acquisition introduit du bruit sur les signaux de la signature. Afin d'éliminer ce bruit, des filtres sont appliqués aux signaux acquis qui permettent d'éliminer les oscillations involontaires dans la signature.

Le ré-échantillonnage: permets d'améliorer la représentation de la forme de la signature. Cependant, le ré-échantillonnage de la signature cause la perte de quelques informations temporelles selon la vitesse de la signature ainsi que certains systèmes reposent sur des points critiques (comme les points de début, les points de fin de signature, et les points de lever du stylo). Pour éviter ces problèmes, les paramètres temporels (vitesse) et les points critiques de la signature sont extraits avant de ré-échantillonner la signature.

La normalisation: consiste à standardiser la signature dans un domaine comme la taille, la position, ou la durée. Certaines méthodes de normalisation en position réalisent une transformation sur les signatures de telle manière que le point de départ de la signature soit le même. D'autres alignent les centres des signatures. D'après l'étude de l'influence de ces deux normalisations en position et constate que la deuxième donne le meilleur résultat [21].

II.2.3. Extraction des caractéristiques

Cette étape est très importante dans le système de reconnaissance, elle permet d'extraire des attributs ou des caractéristiques d'une image donnée qui seront sauvegardés en mémoire pour être utilisées, dans le but d'effectuer des détails utiles et ordonnés sous la forme de l'information d'observation. En effet, le test de classe d'une signature se base exclusivement sur ses caractéristiques et la précision de la vérification, donc ils assurent une meilleure exploitation de données. Après cette étape, le processus suivant dépend seulement de données portées alors que la signature ne sera plus représentée par une suite de points mais par un vecteur constitué de valeurs de chacune des caractéristiques choisies [22].

Les méthodes d'extraction des caractéristiques peuvent être séparées en trois grandes familles, les **méthodes globales** (ou **statistiques**), les **méthodes locales (**ou **géométriques),** et les **méthodes hybrides.**

II.2.3.1 Méthodes globales

La méthode globale c'est l'utilisation directe des valeurs d'intensité des pixels de l'image entière de la signature sur laquelle la décision de reconnaissance sera fondée. Autrement dit, le résumé de l'ensemble visuel de l'image qui prend généralement la forme d'un seul vecteur basée sur l'analyse statistique d'image pixel par pixel. Une fois les caractéristiques globales de la signature: le temps total de processus de signer, le rapport

hauteur /largeur, la vitesse moyenne pour signer,...sont calculées, la signature soit représentée par un vecteur de même longueur dans l'espace des paramètres. L'avantage principal de cette méthode est que les calculs de base ne sont pas compliqués et relativement rapide à mettre en œuvre. En revanche, elle contient peu d'informations et elle n'est pas très discriminante. Pour cela l'approche globale doit extraire plus de paramètre globeux, de l'ordre de 50 à 100, pour atteindre des informations acceptables. Ses caractéristiques sont moins sensibles aux variations de signature et au bruit en tant que telles, elles conviendraient pour des contrefaçons aléatoires mais ne donneront pas une précision élevée pour les contrefaçons qualifiées [23].

Parmi les méthodes globales largement citées, nous pouvons mentionner :

- **L'Analyse en Composantes Principales (ACP) :**

C'est l'algorithme le plus connu qui s'appuie sur des propriétés statistiques bien connues, il utilise l'algèbre linéaire. Elle a été proposée par **M.A. Turk et M.P. Pentland.** Son idée principale et d'utiliser des vecteurs et des valeurs propres, telle que c'est vecteur contenant des informations indépendantes d'un vecteur à l'autre. Donc ces nouvelles informations sont extraites de manière plus adaptée à la reconnaissance de signature. Il existe plusieurs méthodes qui basent sur la technique PCA, nommée aussi « eigenface » [24].

- **L'Analyse Discriminante Linéaire (ADL) :**

L'algorithme ADL connu sous le nom de 'fisherfaces' a été découvert par Belhumeur et al. De Yale university (USA) en 1997 [25]. ADL effectue une véritable séparation de classes, réversiblement à l'algorithme PCA. Pour utiliser cette méthode, il faut au préalable organiser la base d'apprentissage en plusieurs classes: plusieurs images par classe et une classe par personne. Alors que, pour maximiser les variations entre les images d'individus différents et minimiser les variations entre les images d'un même individu, l'ADL va analyser et traiter les vecteurs propres de la matrice de dispersion des données. Mais parfois, il y a des difficultés pour appliquer ADL lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, dans laquelle elle faisait apparaitre des matrices de dispersions singulières [26].

II.2.3.2. Méthodes locales

La méthode locale consiste à effectuer des transformations en des tâches spécifiques de l'image, plus précisément c'est l'extraction de plusieurs paramètres en chaque point ou en chaque partie de la signature. Alors que, une partie peut être délimitée par des min ou max de

la vitesse, de l'ordonne, ou de l'accélérateur …En fin de compte, la signature est représentée par une suite de vecteurs de grandes dimensions. Contrairement à la méthode globale ou une signature est représentée par un vecteur de même langueur fixe. Dans la méthode locale, la signature est représentée par une suite de vecteurs et de longueur variable. Les informations concernant la dynamique (la vitesse, l'accélération..) et la forme (le rayon de courbe, l'angle entre le vecteur de vitesse et l'axe des abscisses…) sont souvent exploitées au niveau local.

Bien que son temps de calcul soit élevé, mais elle est plus précise que les caractéristiques globales. Parmi les approches de cette méthode: les approches Bayésiennes (comme la méthode BIC), les machines à vecteurs de support (SVM), la méthode des modèles actifs d'apparence (AAM), ou encore la méthode « local Binary Pattern » (LBP) [27].

II.2.3.3. Méthodes hybrides

La méthode hybride permettant d'associer l'utilité des méthodes globales et locales en combinant l'extraction des caractéristiques d'aspects locales et les caractéristiques structurales afin d'améliorer la stabilité des performances de reconnaissance de signature. Elle se base sur plusieurs algorithmes comme [28]:

- l'Elastic Graph Matching (EGM).
- l'Elastic Bunch Graph Matching (EBGM).
- l'algorithme Log Gabor PCA (LG-PCA).

La figure suivante illustre la classification des méthodes d'extraction de caractéristiques utilisées dans le domaine de la reconnaissance des signatures électroniques.

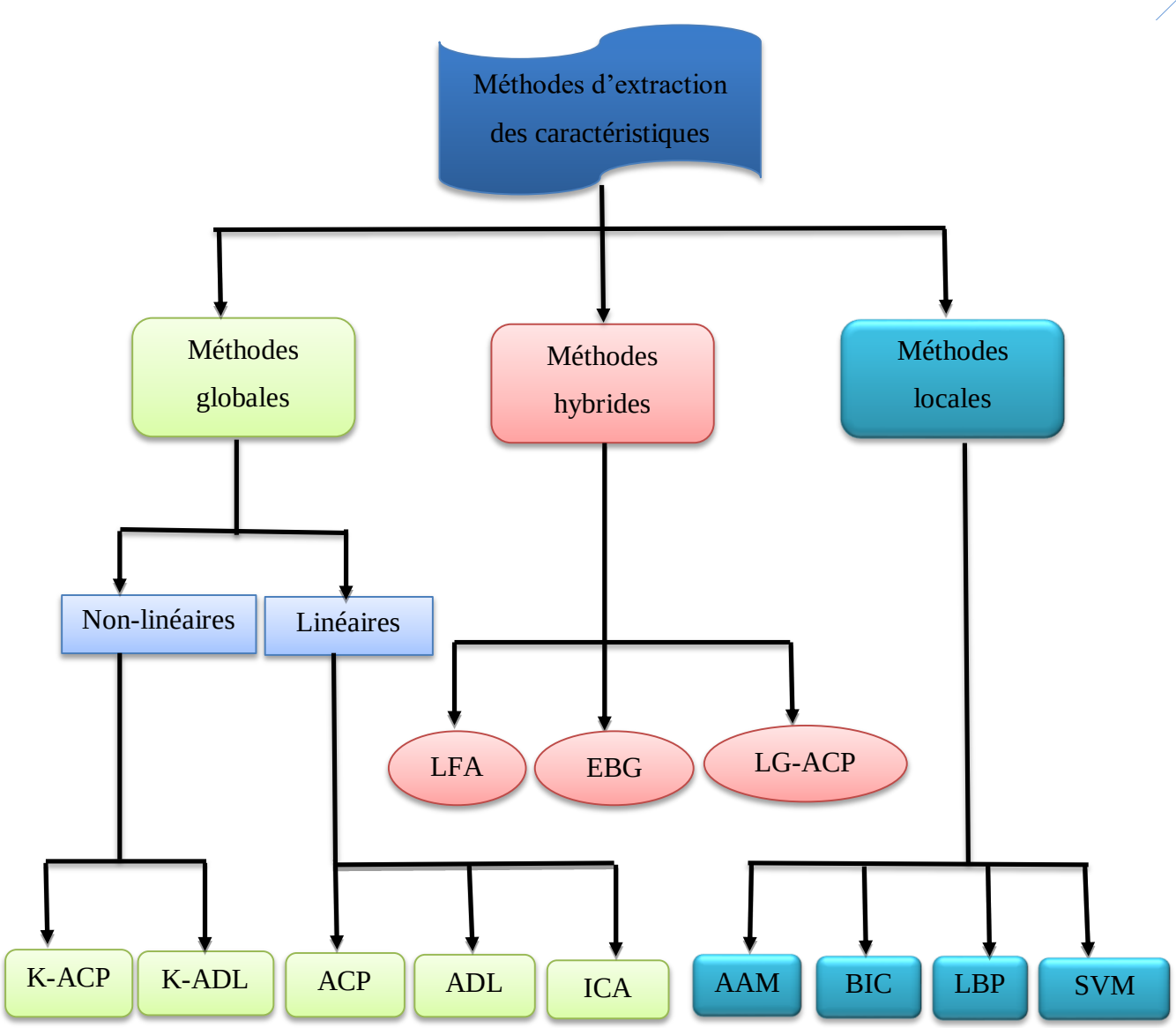


Figure.II.3: Schéma représentatif d'une classification des algorithmes principaux utilisés dans la reconnaissance des signatures.

L'extraction des caractéristiques à partir d'une image dans laquelle en extrayant des informations importantes, dont ces informations sont des attributs de texture de la signature qui est apparue comme une phase très importante pour faire un système de reconnaissance prospère. L'analyse de ces textures représente comme une approche intéressante pour caractériser l'écriture personale pour des procédures améliorées de vérification de signature, telle que: la texture considérée comme la variation spatiale d'intensités de pixels. Pour cela, nous avons choisi l'algorithme (motifs binaires locaux (LBP)) qui est très utilisé et donne des résultats utiles.

II.2.4. Motifs binaires locaux (LBP)

Les descripteurs de textures basés sur LBP (local binary patterns) ont été au début proposé par Ojala en 1996 [29], pour le but de caractériser les textures présentes dans des images aux niveaux de gris. Son principe général est d'assigner à chaque pixel *p* de l'image *I(i,j)*, une valeur à distinguant le motif local à propos de ce pixel. Tel que ces valeurs sont calculées en comparant les niveaux de gris de pixel *p* central avec les valeurs des niveaux de gris des pixels voisins [30].

Pour calculer un code LBP dans un voisinage de P pixels, dans un rayon R. Tel que, le paramètre P vérifie la quantification de l'espace angulaire et R prélève la résolution spatiale de l'opérateur. On calcule les occurrences de niveaux de gris gp plus grands ou égaux a la valeur centrale avec la formule suivante :

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

Où V(..) est la fonction signée, où g_i et g_c sont respectivement les niveaux de gris d'un pixel voisin et du pixel central.

$$V(x) = \begin{cases} 1 & si\ x \geq 0 \\ 0 & si\ non \end{cases} \qquad \text{(II.2)}$$

Le calcul du code binaire est associé à une opération de corrélation lors de l'application d'un filtre sur une image numérique. Pour cela, il est adéquat d'étudier chaque pixel de l'image en prend en considération les huit pixels de son voisinage immédiat (tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement **(figure.II.4)**. En effet, ce code représente la texture locale d'une région et il est calculé par seuillage d'un voisinage avec le niveau de gris de pixel.

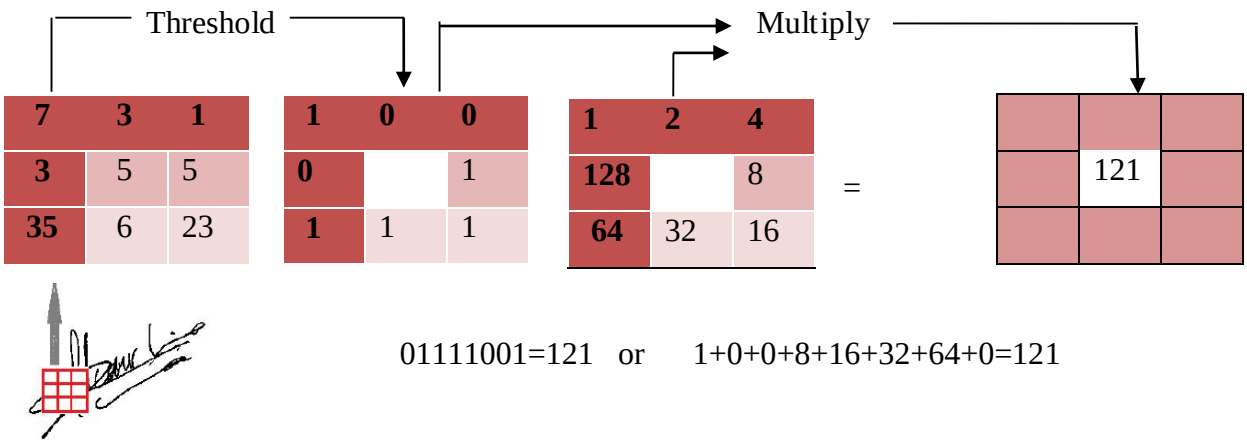


Figure.II.4: Construction d'un forme binaire et calcul du code LBP pour un pixel central.

L'opérateur LBP a été expansé dans le but d'utiliser des voisinages de différentes tailles. Pour chaque pixel de niveau de gris de pixel central g_c d'une image, on déduit la diffusion de niveaux de gris du voisinage circulaire $Tg_c = (g_c, g_0 \ldots\ldots, g_{p-1})$ où p est le nombre de points du voisinage, et g_p avec (p=0,…..p-1) , correspondant au niveau du gris de P pixels espacés uniformément sur un cercle de rayon R. Sachant que g_c et g_p sont calculés avec l'équation suivante [31] :

$$x_g = x_c + R.\cos\left(2.\pi.\frac{p}{P}\right) \qquad y_g = y_c - R.\sin\left(2.\pi.\frac{p}{P}\right) \qquad \text{(II.3)}$$

La **figure.II.5** illustre différents voisinages de la notion (P, R) qui consiste à obtenir des p points échantillonnés dans les voisinages pour tout rayon R.

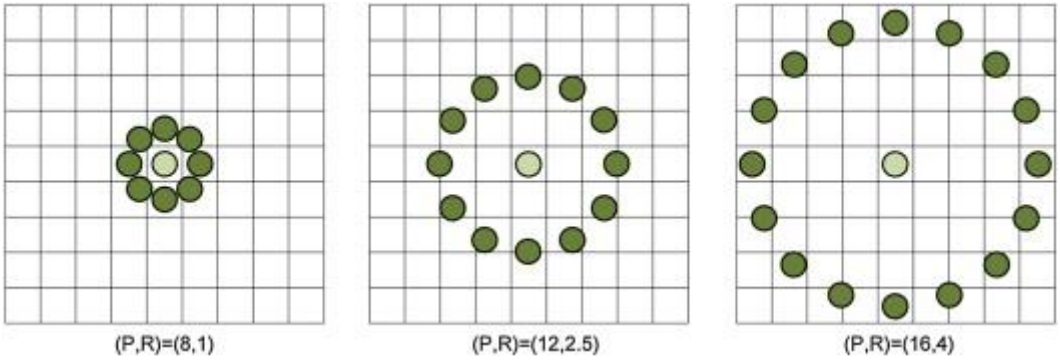
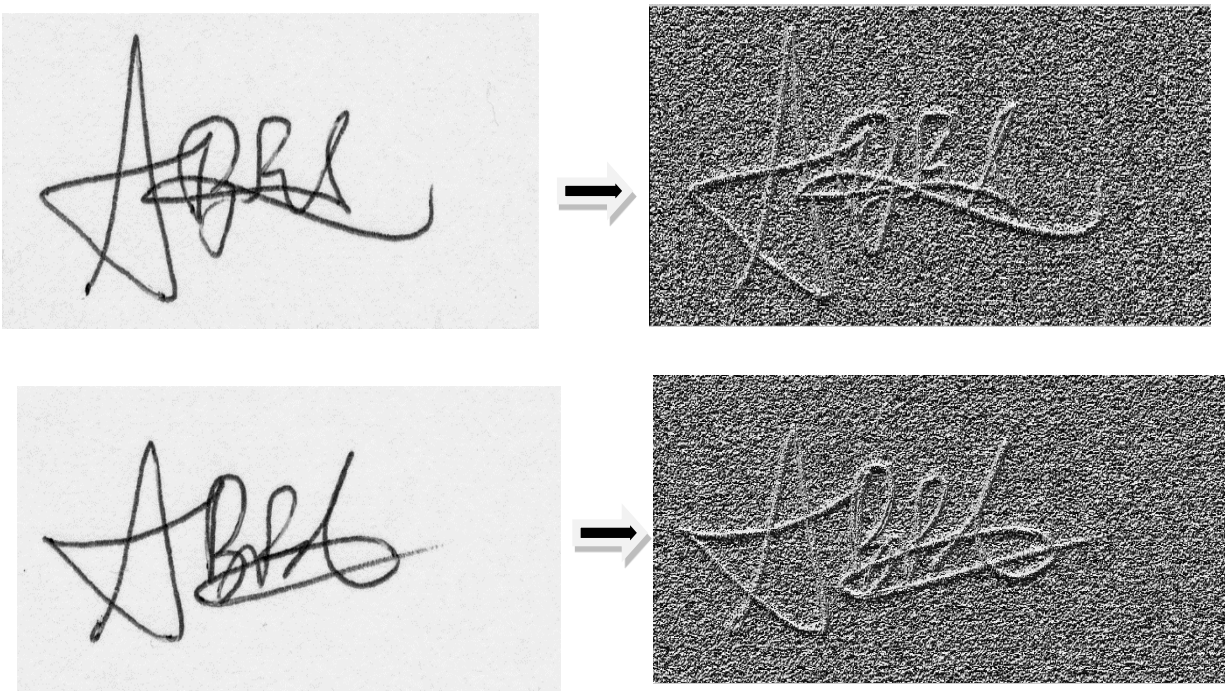


Figure.II.5: LBP multi-échelle. Exemples de voisinages obtenus pour différentes valeurs de (P,R).



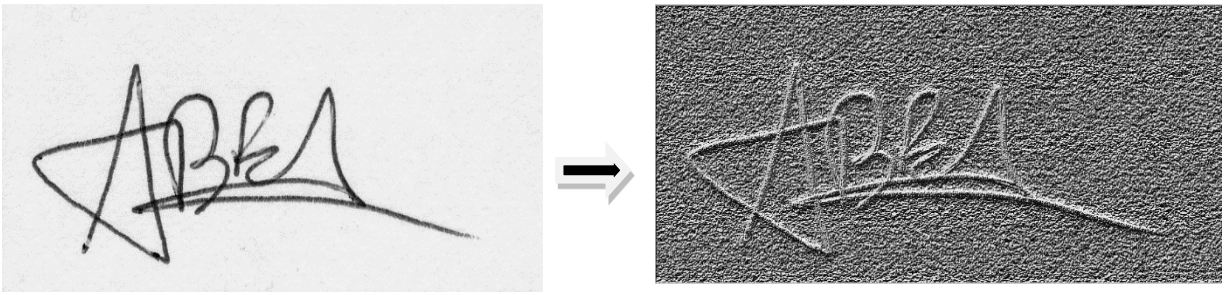


Figure.II.6 : Des images de signatures est ses nouvelles représentations après l'application du descripteur LBP.

II.2.5. Apprentissage

Comme tout système biométrique, avant qu'un modèle de décision ne soit combiné dans un système de reconnaissance de signature, il faut avoir procédé préalablement à l'étape d'apprentissage qui permette au système de s'adapter graduellement aux caractéristiques propres à un scripteur en analysant un nombre limité de ses signatures qui seront appelées des références. Autrement, c'est l'obtention de connaissances et compétences permettant la compilation d'information et caractérisant les classes de forme ou modèle de référence afin d'identifier les nouvelles formes par rapport à elles. Il existe deux types d'apprentissage qui sont ***supervisé*** et ***non-supervisé*** [32]:

- **Apprentissage supervisé**: l'apprentissage est dit supervisé si le système connut l'ensemble des familles des formes à préalable à partir d'une base de données. Tel que, la base de données est en règle d'un ensemble de couples entrées/sorties {(x, y)}. Par objet d'apprendre à prévoir pour toute nouvelle entrée x, la sortie y [32]. Il existe plusieurs algorithmes et techniques utilisés pour la classification supervisée des signatures comme les réseaux de neurones, *K-Plus Proches Voisins* (KPPV)…
- **Apprentissage non supervisé**: par contre, l'apprentissage non supervisé traite le cas où on dispose seulement des entrées {X} sans avoir au préalable les sorties. Donc, on dispose seulement d'exemples sans aucune étiquette de classe. Il permet de partitionner des données en différents ensembles homogènes (clusters). Tel que, les clusters qui contiennent des mêmes classes, il s'agit des caractéristiques communes qui sont définies grâce à des algorithmes comme K-means ou l'Isodata.

II.2.6. Classification

La classification de signature est une étape très importante dans le système d'identification, elle consiste à donner un ensemble de vecteurs de caractéristiques extraits à partir des signatures présentées au système, à des classes spécifiques.

Au cours de ce travail, nous parlerons d'une classification supervisée basée sur l'approche de k-les plus proches voisins (K-NN) passant par la comparaison de distance entre différents vecteurs.

Parmi les méthodes de classification supervisée largement utilisées dans ce domaine, nous pouvons citer:

II.2.6.1. Mesures de distances

Quand nous discutons d'une comparaison des objets, nous devons comprendre le processus de calcul de distance entre les projections vectorielles. Il semble logique que les images sauvegardées dans la base de données aient une petite valeur de distance signifie que les deux projections sont similaires, et une grande valeur de distance signifie que les deux projections sont différentes [33].

La première catégorie de distance est constituée de distances Euclidiennes et sont définies à partir de la *distance de Minkowski d'ordre* p dans un espace euclidien R^N où **N** détermine la dimension de l'espace Euclidien**.** Considérons deux vecteurs X considérer (x_1,x_2, …….x_N), et Y = ($y_1, y_2, \dots \dots y_N$), la distance de Minkowski d'ordre ***p*** (valeurs positives) notée **L*p*** est définie par:

$$\mathbf{Lp}=\left(\sum_{i=1}^{N} |\boldsymbol{x_{i-}}\, \boldsymbol{y_i}|^{p}\right)^{1/p} \qquad \text{(II.4)}$$

C'est à partir de cette formule générique que vont être définies des distances couramment utilisées dans les algorithmes de reconnaissance de signature :

- Pour ***p* = 1**, nous obtenons **la distance City-Block:**

$$L_1=\sum_{i=1}^{N}|X_i - Y_i| \qquad \text{(II.5)}$$

- Pour ***p* = 2**, nous obtenons **la distance Euclidienne**:

$$L_2 = \sqrt{\sum_{i=1}^{N} |X_i - Y_i|^2} \qquad \text{(II.6)}$$

- **La distance de Hamming** :

La distance d'Hamming permet de quantifier la différence entre deux projections et elle fait des calculs avec un nombre de bits différents et valides pour les deux signatures entre le code A et le code B. Plus la distance de *Hamming* est faible, plus les deux codes se ressemblent. Une distance 0 correspond à une parfaite correspondance entre les deux images alors que deux images de personnes différentes auront une distance de *Hamming* proche de 0.5.

La distance de *Hamming* est donnée par la formule suivante :

$$HD = \frac{1}{B}\sum_{i=1}^{B} X_i \otimes Y_i \qquad \text{(II.7)}$$

Ou Xi et Yi représentent i ème bit dans les séquences X et Y, respectivement, $\otimes$ désigne le OR exclusif (XOR) et c'est l'opérateur booléen connu qui donne un binaire 1 si les bits de position i dans X et Y sont différents et 0 s'ils sont similaires, B est le nombre total de bits dans chaque séquence [34].

II.2.6.2. K-plus proche voisin

La méthode des k plus proches voisins (KPPV) est une méthode d'apprentissage supervisé. En abrégé k-NN ou KNN (en anglais *k-nearest neighbors)*. Elle consiste à prendre en compte les échantillons d'apprentissage dont l'entrée est la plus proche de la nouvelle entrée x, selon une distance à définir. Telle que, il doit classer l'entrée dans la catégorie à laquelle appartiennent les k plus proches voisins dans l'espace de caractéristiques identifiées par apprentissage. Cette technique donne des bons résultats dans des cas simples et est facile à mettre en œuvre car elle est non paramétrique.

- **Si k=1 :**

Soit **x** un point de l'espace de représentation **R=R^d** et soit **Xi** le plus proche voisin de **x** dans cet espace, appartenant à l'ensemble d'apprentissage **E** muni de la distance **d** :

$$\forall\, X_j \in E \; d(X, X_i) \leq d(X, X_j). \qquad \text{(II.8)}$$

La règle de décision consiste à attribuer au vecteur **X** de classe inconnue, la classe du vecteur X_i

- **k-PPV (k > 1) :**

La règle de décision basée sur les **K-NN** consiste à examiner les k plus proches voisins de **X** : les vecteursX_1, X_2, X_3…X_k de **E** indicés en fonction de leur distance au point **X**. La règle de décision consiste à attribuer au vecteur x la classe w_i majoritairement représentée parmi les **k** voisins.

Elle permet aussi de traiter des nuages des points non linéairement séparables. Nous utilisons cette méthode pour chercher et associer les points correspondants. Chaque point associé ne pouvant être associé qu'à un seul voisin [34].

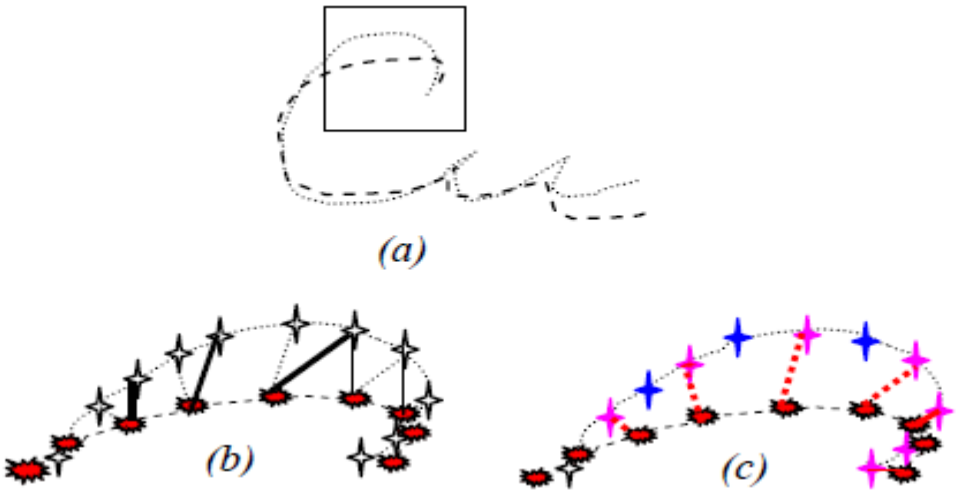


Figure.II.7: Fonctionnement de l'algorithme d'association des points. (a) Deux graphes à associer, (b) Calcul des distances entre points et recherche des voisins, et (c) Association des points des deux graphes.

II.2.7. Décision

C'est la dernière étape dans le processus du système de reconnaissance de signature, elle attribue une signature à vérifier selon le score de comparaison à l'une des deux classes client ou imposteur. Tel que, cette décision est prise selon le degré de similitude entre les caractéristiques extraites et celle des modèles stockés. En effet, la décision est comptée sur trois concepts importants : la distance, k plus proche voisin, et classification.

II.3. Conclusion

Dans ce chapitre, nous avons présenté la technique biométrique de la reconnaissance générale de signature, et un aperçu sur les différentes méthodes de reconnaissance existantes. Tel que les trois méthodes d'extraction des caractéristiques et les différents types de

classification. Ainsi, dans cette étude, nous avons détaillé la méthode LBP et la méthode de la distance, les plus connues au stade de cette recherche.

Le chapitre suivant va présenter notre système de reconnaissance biométrique proposé ainsi qu'une étude expérimentale.

Chapitre III

III.1. Introduction

Comme nous avons vu précédemment, la signature est l'une des tâches les plus personnelles et les plus uniques que l'être humain peut l'accomplir. Nous avons présenté dans le chapitre précédant la technique dite ‘’*Motif Binaire Local (LBP) ‘’* qui est largement utilisée en caractérisation des images texturées, ainsi que ses extensions les plus populaires en analyse de texture [36].

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

III.2. Système proposé

Dans le système d'identification de signatures manuscrites hors ligne proposée, on extrait les signatures de chaque utilisateur et les mettre sous la forme d'un vecteur de caractéristiques. Ces derniers sont associés et stockés dans une base de données afin de les employer dans la phase d'apprentissage. Puis, quand un utilisateur, prétendant être un client particulier du système, présente sa signature pour l'identification, elle sera comparée avec toutes les signatures référentielles stockées dans la base de données du système. Après cette comparaison, des scores mesurant la similitude entre la signature proclamée et les signatures référentielles sont fournis. À la fin, le système attribue à la signature proclamée l'identité de la signature la plus proche, qui a le plus petit score de similarité.

Le diagramme de notre système proposé est illustré dans la **figure.III.1**. Notre système est séparé en deux blocs: un bloc d'apprentissage et un bloc de test. On doit noter que les opérations de prétraitement des signatures sont identiques pour les deux blocs considérés. Les phases principales composant notre système sont décrites dans ce que suit:

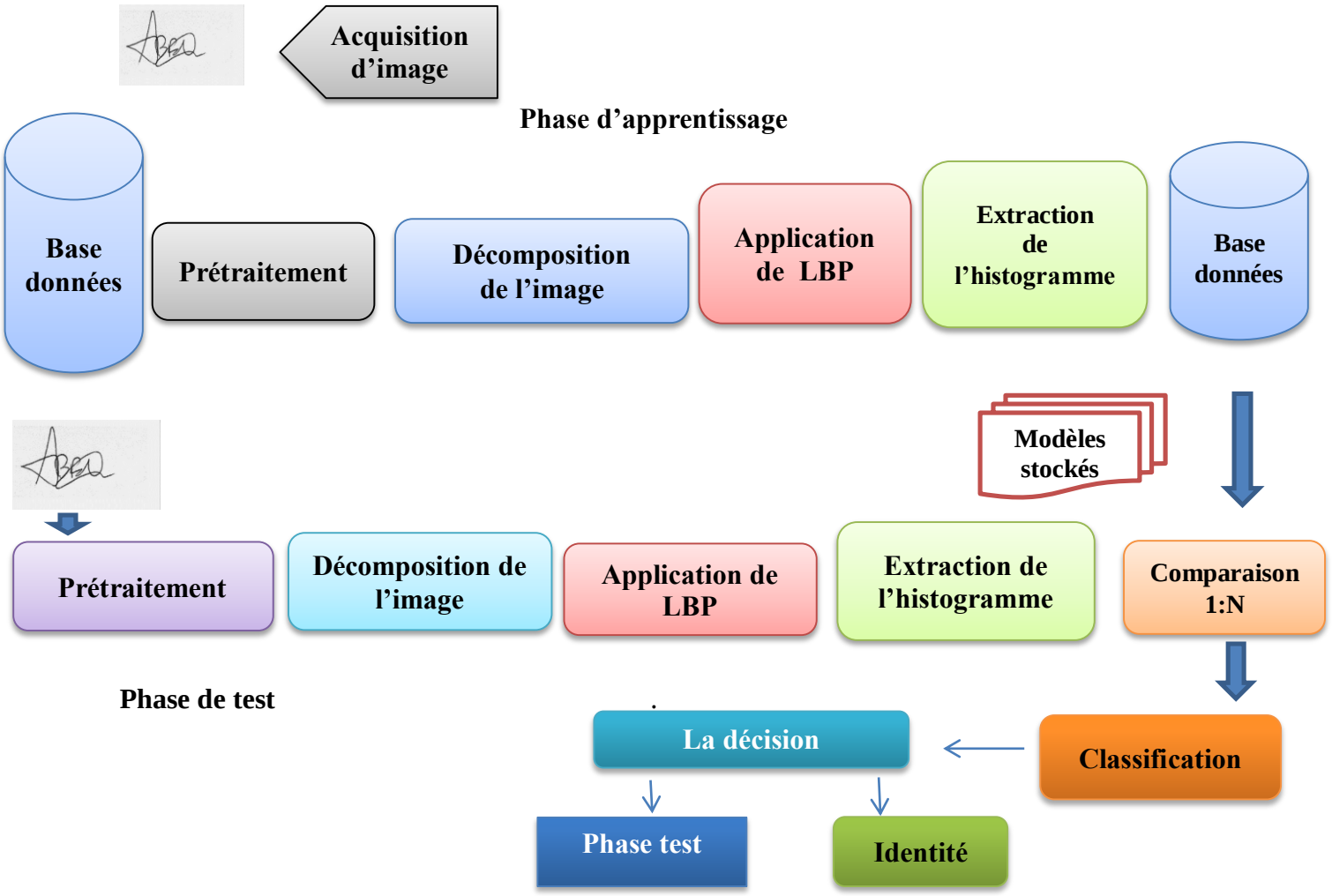


Figure.III.1: Schéma général de notre système d'identification de signatures hors ligne proposé

III.2.1. Prétraitement

L'étape de prétraitement a été appliquée dans les phases d'apprentissage et de test. L'objectif de cette phase est d'éliminer le bruit introduit lors de l'acquisition ainsi que la redondance de l'information pour que la signature soit prête pour l'extraction de caractéristiques et aussi pour améliorer les performances de la reconnaissance.

Les images utilisées dans notre système sont numérisées aux niveaux de gris avec un arrière-plan trop contrasté. Pour résoudre ce problème, nous avons utilisé la procédure de postérisation définie dans l'article présenté dans la référence [36] :

$$Ip(x, y)=[round\ [round\left[\ \frac{I(x,y)*nL}{255}\right]\frac{255}{nL}\ ].\ ] \qquad (III.1)$$

Ip : Image postérisée

Round : Arrondit les éléments aux entiers les plus proches.

I(x, y) : Image originale de signature de la base de données MCYT à 256 niveaux de gris.

nL : nous avons sélectionné nL = 3 pour que la signature sera conservée et l'arrière-plan apparaît presque propre, moins de cette valeur la signature sera à moitié effacée.

La **figure.III.2** montre le résultat de l'application de la procédure de postérisation sur une image de la base de données MCYT.

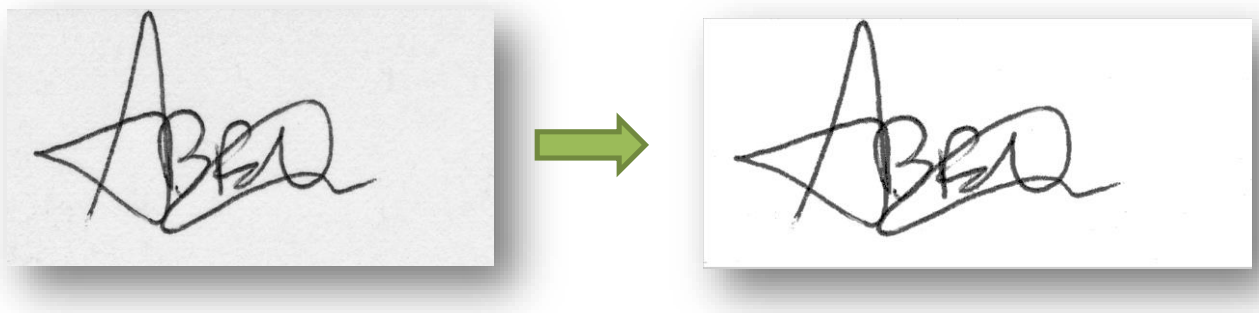


Figure.III.2: Une image originale et sa représentation après l'application de la fonction Ip.

Dans l'image postérisée, nous avons obtenu des signatures apparaissent plus foncées avec un arrière-plan blanc. Pour obtenir une image binarisée (noir et blanc), nous avons appliqué un seuillage comme suite :

$$Ibw(x, y) = \begin{cases} 255 & si \quad Ip(x,y)=255 \\ 0 & \text{sinon} \end{cases} \qquad \text{(III.2)}$$

La figure suivante montre le résultat de l'application de la fonction Ibw sur l'image Ip:

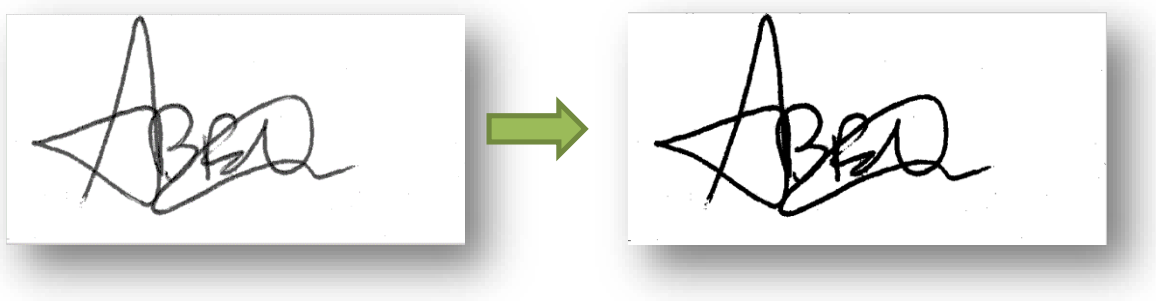


Figure.III.3: Une image postérisée et le résultat après l'application de Ibw.

L'image obtenue (Ibw) est utilisée comme un masque pour segmenter la signature originale et indiquer quels est les pixels de l'image qui appartiennent à la texture de la signature, afin de supprimer les informations bruyantes dans les étapes ultérieures avec l'opération suivante :

$$Is(x, y) = \begin{cases} 255 & si \quad Ibw(x,y)=255 \\ I(x,y) & \text{sinon} \end{cases} \qquad \text{(III.3)}$$

La figure suivante montre le résultat de l'application de la fonction Is sur les deux images I et Ip:

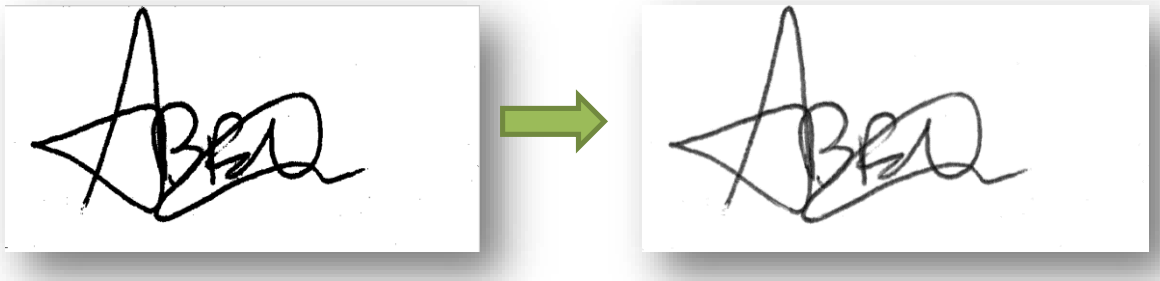


Figure.III.4: Une image binaire et sa représentation après l'application de Is.

Vers la fin, nous utilisons le déplacement de l'histogramme pour réduire l'influence des différents stylos à encre d'écriture sur la signature segmentée. Nous atteignons ceci en déplaçant l'histogramme dans lequel on force tous les niveaux de gris de l'image à être équiprobables (les pixels de signature vers zéro), en gardant l'arrière-plan blanc avec un niveau de gris égal à 255. En assurant que la valeur de niveau de gris du pixel de signature le plus sombre est toujours égale à 0. Cela peut être réalisé en soustrayant la valeur de niveau de gris minimum dans l'image à partir des pixels de signature:

$$Ig(x, y) = \begin{cases} Is(x,y) & si \quad Is(x,y)=255 \\ Is - \min\{Is(x,y)\} & \text{sinon} \end{cases} \qquad \text{(III.4)}$$

La figure suivante montre le résultat de l'application de la fonction Ig sur l'image Is.

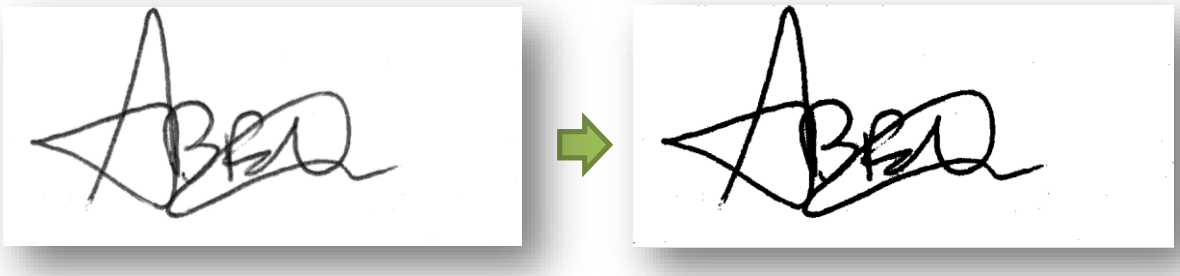


Figure.III.5 : Une image binaire et l'image après le traitement de Ig. .

III.2.1. Extraction des caractéristiques

L'extraction des caractéristiques est une méthode de réduction dimensionnelle. Le but de cette méthode est d'améliorer l'invariance d'échelle, représenter les informations intéressantes, ainsi que garder la texture de l'encre aussi invariante que possible.

Nous avons utilisé pour cette tâche l'extracteur de caractéristiques LBP (Local Binary Pattern), qui est appliqué sur les images aux niveaux de gris et ses statistiques sont résumées par un histogramme. Cette phase est la plus importante car les performances du système sont dépendantes à la méthode utilisée en extraction, en termes de résultats, robustesses et de temps d'exécution.

Le principe de la méthode LBP et ses variantes sont expliqués en détails dans le chapitre II.

III.2.2. Classification

Dans cette dernière étape, nous cherchons, parmi les modèles d'apprentissage représentés en paramètres descriptifs ceux où'ils sont les plus proches en calculant des distances entre le vecteur de l'image de test et chaque vecteur de la base de données (apprentissage).

- **La méthode des K plus proches voisins** :

Les 'k plus proches voisins sont une méthode non paramétrique dans laquelle le modèle mémorise les observations de l'ensemble d'apprentissage pour la classification des données de l'ensemble de tests.

En effet, cet algorithme est qualifié comme paresseux (Lazy Learning) car il n'apprend rien pendant la phase d'entraînement. Pour prédire la classe d'une nouvelle donnée d'entrée, il va chercher ses K voisins les plus proches (en utilisant la distance euclidienne, ou autres) et choisira la classe des voisins majoritaires, comme expliqué en détail dans le chapitre précédent.

Dans notre travail, nous intéressons à trois distances, qui sont : Euclidienne, City block et Hamming.

III.3. Base de données et protocole d'évaluation

III.3.1. Base de données

La base de données MCYT (Ministerio de Cienca y Technologia) [37], est une partie de la base biométrique multimodale (empreinte digitale et signature).

L'acquisition des données de signatures a été faite avec le même stylo encreur et les mêmes modèles de papier, sur une tablette à stylet similaire. Les modèles de papier ont été numérisés à 600 dpi. Cette base de données comprendre 75 signataires de quatre sites espagnols différents. Pour chaque signataire, nous disposons 15 signatures authentiques (image du type génuine) et 15 signatures fausses expérimentées (image du type imposteur).

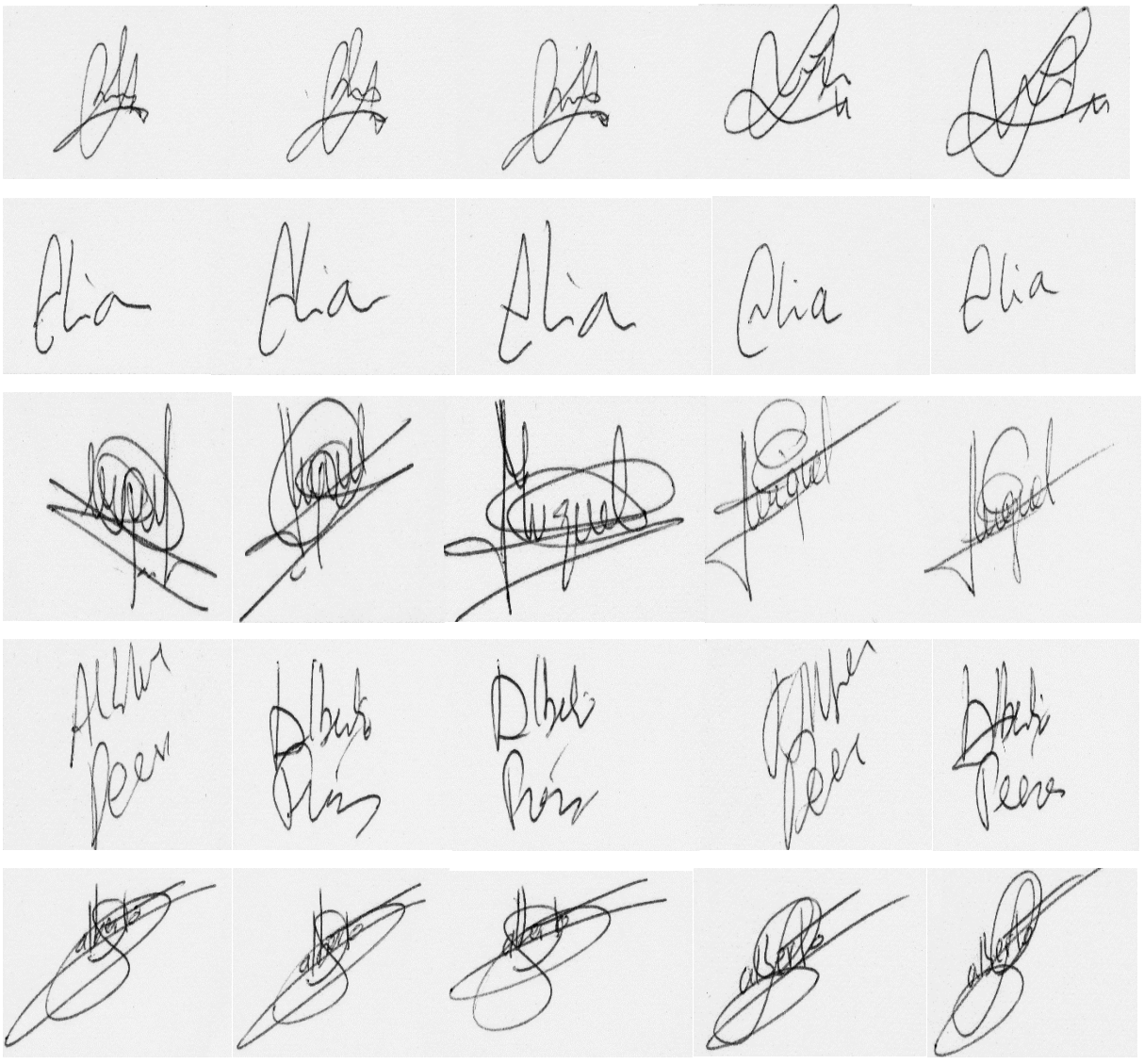


Figure.III.6: Des images de base de données MCYT.

III.3.2. Protocole d'évaluation

À partir du système de reconnaissance déjà présenté en (**figure.III.1)**, différents tests ont été effectués en fonction de différents nombres de vecteurs de caractéristiques. Afin de développer une application de reconnaissance de signature électronique, il est nécessaire de scinder la base d'images MCYT-75 en deux bases: l'une pour effectuer l'apprentissage et l'autre pour tester le système et déterminer ses performances,

Dans le but d'évaluer le taux de reconnaissance, nous avons suivi ce protocole:

- ***Phase d'apprentissage*** : les **10** premières images du type génuine servent pour la phase d'apprentissage, ce qui implique que 750 images sont dédiées à cette phase.
- ***Phase de test :*** les **5** dernières images du type génuine de chaque individu ont été servies pour la réalisation de différents tests. Ce qui nous fait un sous- ensemble de 375 images consacrées pour les tests.

$$\textit{Taux de reconnaissance}\ (\%) = \frac{\text{nombre d'images de test correctement reconnues}}{\text{nombre total des images de test}} \qquad \text{(III.5)}$$

Tableau.III.1: Distribution d'images entre l'apprentissage / test.

Base de données	MCYT-75
Nombres des personnes	75
Nombres des images de type génuine	1125
Images utilisées dans l'apprentissage	750
Images utilisées dans le test	375

III.4. Expérimentations & Résultats

III.4.1. Expérimentation #1 (Effet des variantes du descripteur LBP)

Dans cette première expérimentation, nous avons testé les performances de notre système en testant plusieurs variantes du descripteur de texture LBP, à savoir: LBP(8,1), LBP(8,2), LBP(8,3), LBP(8,4) sur la base de données MCYT-75.

Les résultats obtenus sont mis dans le tableau suivant :

Tableau.III.2: Performances du système proposé avec plusieurs variations du descripteur LBP.

Base de données	LBP (8,1)	LBP (8,2)	LBP (8,3)	LBP (8,4)
Taux de Reconnaissance(%)	**63.52**	**65.73**	**71.73**	**78.46**

D'après les résultats mentionnés dans le **tableau.III.2**, Nous remarquons une amélioration des résultats; nous avons obtenu un taux de reconnaissance pour LBP(8,4) de **78,46%.** Ceci implique que le choix de la variante LBP est très important dans un système de reconnaissance de signature et la variante LBP(8,4) est la meilleure par rapport aux autres configurations.

III.4.2. Expérimentation #2 (Effet des distances)

À partir des meilleurs paramètres obtenus dans l'expérimentation précédente, nous avons testé plusieurs distances: Hamming, Euclidienne, et City block (détaillées dans le chapitre II). Les résultats correspondants sont rassemblés dans le tableau suivant :

Tableau.III.3: Résultats montrant l'effet des distances sur taux de reconnaissance.

Distance	Hamming	Euclidienne	City block
Taux de reconnaissance(%)	**11,33**	**78,46**	**88.53**

Nous remarquons une amélioration des résultats, avec la distance de **City block,** nous avons obtenu un taux de reconnaissance de **88 ,53%.** Par contre, le taux de reconnaissance

avec l'utilisation de la distance Hamming a été largement diminué vers **11,33%**, donc cette distance est inappropriée pour ce type de reconnaissance. Ceci implique que le choix de la distance est très important dans un système de reconnaissance d'une signature.

III.4.3. Expérimentation #3 (Effet de décomposition de l'image en plusieurs blocs)

À partir des meilleurs paramètres obtenus dans les expérimentations précédentes (LBP(8,4) & distance de city block), nous avons divisé l'image en sous-blocs de la même taille, ensuite nous avons appliqué le descripteur LBP sur chaque sous-bloc, et à la fin les histogrammes extraits sont concaténés dans un seul histogramme global qui représente le vecteur de caractéristiques de l'image. Cette méthode est appelée LBP multi-blocs, son principe est illustré dans la figure suivante:

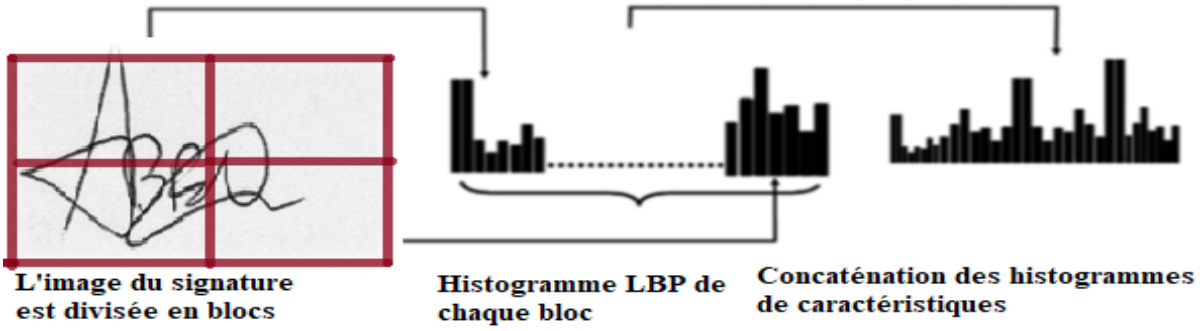


Figure.III.7 : Exemple de décomposition d'image en plusieurs blocs (2x2).

Les résultats obtenus sont mis dans le tableau suivant :

Tableau III.4: Effet de la décomposition de l'image en plusieurs blocs.

	LBP multi-blocs		
n blocs	1 bloc	4 blocs	8blocs
Taux de reconnaissance (%)	**88.53**	**92.00**	**95.00**

Comme le montre le **tableau III.4**, le LBP multi-blocs a un effet très important, telle que: à chaque fois le nombre de blocs soit supérieur, les performances du système de

reconnaissance vont être augmentées. Dans notre cas, l'optimisation a touché le 6,44%. Le taux de reconnaissance a été amélioré de **88 ,53%** à **95%.**

III.5. Conclusion

Dans ce chapitre, nous avons présenté les tests effectués et les résultats obtenus par notre système d'identification biométrique unimodale basé sur la reconnaissance de signature manuscrite hors ligne. Nous avons commencé par présenter le système proposé ainsi que la base de données MCYT_75 et le protocole d'évaluation. Ce système est testé dans le but d'améliorer le taux d'identification de cette modalité.

La méthodologie proposée améliore l'évaluation de la performance finale du module d'identification.

Conclusion générale et perspective

Conclusion générale

La biométrie est une technique en plein essor. Elle est de plus en plus utilisée dans les applications en lien avec la sécurité vu les avantages qu'elle offre contrairement aux anciennes méthodes.

Dans ce mémoire, nous avons étudié un système biométrique d'identification de l'identité d'une personne à partir de sa signature manuscrite puisqu'elle fournisse une identification efficace, simple, très acceptable par le public et surtout pas chère.

Notre projet de fin d'études s'intéresse à la reconnaissance de signature manuscrite hors ligne. En effet, nous avons conçu et réalisé ce système de reconnaissance dans le mode d'identification basé sur l'extraction des caractéristiques, en utilisant une texture locale LBP (Local Binary Pattern, en anglais). Pour connaître la performance de notre système, nous l'avons testé sur la base de données MCYT_75 (Ministry of Science and Technology, en anglais) qui est connue comme une base de données appropriée pour les tests des systèmes de la reconnaissance de signature.

Les expériences réalisées dans cette étude sont effectuées sur plusieurs facteurs qui pouvant améliorer la performance du système, telles que, le prétraitement des images qui est très important pour obtenir des résultats adéquats pour améliorer la précision de reconnaissance de signature. La première expérimentation concerne uniquement l'utilisation des descripteurs LBP dans le système proposé, l'expérience préliminaire montre que le descripteur LBP(8,4) a donné de meilleur résultat. La deuxième expérimentation, nous nous sommes concentrés sur la recherche de meilleurs paramètres entre plusieurs distances (Euclidienne, city block, Hamming) et nous avons déterminé que la distance City block est la brillante dans la reconnaissance de signature.

Vers la fin, nous avons fait une dernière expérimentation qui consiste à décomposer l'image en plusieurs blocs (1 bloc, 4 blocs, et 8 blocs) et appliquer sur chaque bloc indépendamment le descripteur LBP(8,4), ce qu'on appelle « LBP en multi-blocs ». Ensuite, nous concaténons les vecteurs de caractéristiques obtenus de chaque bloc pour former un vecteur final. Cette expérience a apporté des taux de reconnaissance très élevés et remarquables pour optimiser les performances du système de reconnaissance par signature manuscrite hors ligne.

Perspectives

Par ailleurs, nous voyons les perspectives suivantes :

- Nous pouvant envisager une association avec une autre modalité, ce qu'on appelle "La biométrie Multimodale" (ex : identification faciale, les empreintes digitales, etc.) afin d'avoir un système plus complet et répondant aux exigences actuelles dans le domaine de la sécurité.
- Utilisation des autres descripteurs de caractéristiques telle que l'ACP (analyse en composantes principales) ou ADL (Analyse Discriminante Linéaire).
- Nous essayons au futur d'implémenter notre système après l'amélioration de résultat sur un circuit logique programmable du type FPGA.

Enfin, si la recherche traditionnelle sur la signature biométrique a mis l'accent sur plusieurs performances, ce domaine reste ouvert et de nouvelles problématiques vont être émergées. Citons par exemple, la proposition de nouveaux algorithmes de comparaison de signatures, la protection des signatures de référence, l'interopérabilité des dispositifs, la génération synthétique des signatures, etc. Cela nous ouvre la possibilité de continuer nos travaux dans ce domaine.

Références Bibliographiques

[1] H. Nabil **: "** ***Méthode hybride en biométrie: Application à la paume de la main & l'Oreille".*** Thèse de Doctorat, Université 08 Mai 1945 – Guelma, 2017.

[2] S. Chantaf: " ***Biométrie par signaux physiologiques***". Thèse de Doctorat, l'université de Paris (UPEC) de sciences et de technologie (France), 2011.

[3] M. El Abed: " ***Evolution de système biométrique*** ". Thèse de Doctorat, l'université E Caen /Basse-Normandie (France), 2017.

[4] S. Liu, M. Silverman: "***A practical Guide to Biometric Security Technology***". IEEE Computer Society, IT Pro-Security, January-February, 2001.

[5] www.biometrie-online.net Consulté le 10/07/2020.

[6] A. Berrzdjem: "***La reconnaissance des individus par leur empreinte des articulations des doigts***". Thèse de Doctorat, Université 8 Mai 1945 – Guelma (Algérie), 2019.

[7] H. Guesmi:" ***Identification de personne par fusion de différentes modalités biométriques*** " .Thèse de Doctorat. Sous le sceau de l'université européenne de Bretagne, 2014.

[8] H. Benalioche: "***Multimodalité Biométrique dans le cadre d'une application d'authentification***". Thèse de Doctorat, université Ferhat Abbas Sétif 1 (Algérie), 2016.

[9] S. AKROUF:" ***Une Approche Multimodale pour l'Identification du Locuteur*** ". Thèse de Doctorat, université Ferhat Abbas Sétif (Algérie), 2011.

[10] Y. kabbara:" ***Caractérisation des images à Rayon-X de la main par des modèles mathématiques : application à la biométrie***". Thèse de Doctorat, université Paris-Est (France), 2015.

[11] S. GUERFI ABABSA: "***Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D***". Thèse de Doctorat, université D'Evry Val D'Essonne (France), Octobre 2008.

[12] M. E. Krichen: "***Reconnaissance des personnes par l'iris en mode dégradé*** ". Thèse de Doctorat, université d'Evry-Val d'Essonne (France), 2007.

[13] E. A. Caprioli: "***De l'authentification à la signature électronique : quel cadre juridique pour la confiance dans les communications électroniques internationales***". Revue Générale de Droit International Public, 1996-2, p.321.

[14] P. Florent, D. Jean-Luc: "***Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo*** ". Rapport, Institue Eurocom, Traitement du Signal, Vol 19 – n°4, pp.259, 2002.

[15] S.Z .S. Idrus, E. Cherrier, And C. Rosenberger: " ***Fusion et biométrie douce pour la dynamique de frappe au clavier*** ". Article, university Malaisia Perlis (Malaisie), décembre 2016.

[16] H.T. Betaouaf: "***identification biométrique des individus par l'analyse des caractéristiques de la rétine***", Thèse de Doctorat, université Abou-Bekr Belkaid –Tlemcen (Algérie), janvier 2018.

[17] M. CHAA: "***Système de reconnaissance de personne par des techniques biométriques***". Thèse de Doctorat, université Ferhat Abbas –Sétif**,** novembre 2017**.**

[18] E. Cherrat, R.Alaoui, H.Bouzahir « ***système d'identification biométrique par fusion multimodale*** ». Conférence, Ecole nationale des sciences appliquées Agrad (Maroc), 2019.

[19] S. Hans: "***Algorithm For Signature Verification System***''. Conference Paper, Thapar Institute of Engineering and Technology. April 2012.

[20] S. Bengio, J .Mariéthoz: "***A Statistical Significance Test for Person Authentication***".

Article, The Speaker and Language Recognition Workshop, ODYSSEY, Toledo, Spain, May 31 - June 3, 2004.

[21] J.J. Igarza, L. Gomez, I. Hernaez, I. Goirizelaia: "***Searching for an optimal reference system for on-line signature verification based on (x, y) alignment***". First International Conference on Biometric Authentication (ICBA'04), Hong-Kong (Chine), pp. 519-525, 2004.

[22] Saba. M, A.H. Mir: "***Signature Verification: A Study***". International Conference on Computer and Communication Technology (ICCCT), septembre 2013.

[23] B. Ly Van : " ***Réalisation d'un Système de Vérification de Signature Manuscrite En ligne Indépendant de la Plateforme d'Acquisition***". Thèse doctorat, l'Institut National des Télécommunications en partenariat avec l'Université de Technologie de Troyes (France), Décembre 2005.

[24] M. Bengherabi, L. Mezai1, F. Harizi1, A. Guessoum, M. Cheriet : " ***Fusion de la DCT-PCA et la DCT-RLDA pour la Reconnaissance de Visages***". Article, université Saad Dahlab de Blida, 2016.

[25] M. Belahcen: "***Chapitre 3 méthode de réduction et classification*** ". Articles associés, universite de Bisekra, 2013.

[26] K. Etemad, R. Chellappa: "***Discriminant Analysis for Recognition of Human Face images***". Journal of the Optical Society of America A, Vol. 14, No. 8, August 1997, pp. 1724-1733.

[27] F. Leclerc, R. Plamondon: "***Automatic Signature Verification: The State of the Art - 1989-1993***". International Journal of Pattern Recognition and Artificial Intelligence, june 1994.

[28] N. Morizet : " ***Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris***". Thèse doctorat, l'Ecole Nationale Supérieure des Télécommunications et électronique, Paris, 18 Mars 2009.

[29] S. Kumar Roy, B. Chanda, B. B. Chaudhuri, D. Kumar. Ghosh, S .Ram Dubey: "***Local Jet Pattern: A Robust Descriptor for Texture classification***". Journal, preprint: Accepted in multimedia tools and applications, 4 December 2018.

[30] S. Marcel, Y. Rodriguez, G. Heusch: "***On the recent use of local binary patterns for face authentication***". International Journal on Image and Video Processing, Special Issue on Facial Image Processing, 2007.

[31] T. Ojala, M. Pietikainen, T. Maenpaa: "***Multiresolution gray-scale and rotation invariant texture classification with local binary patterns***". IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002.

[32] A. Bohut: "***Etude de propriétés d'apprentissage supervise et non supervise par des méthodes de physique statique***". Thèse de doctorat, université Grenoble I, 30 mars 1992.

[33] N. Morizet, T. EA, F. Rossant, F. Amiel, A. Amara : "***Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie*** ". Article, Institut Supérieur d'Electronique de Paris (ISEP), Département d'Electronique, 2013.

[34] N. Larbi: "***Identification biométrique par fusion multimodale***". Thèse de doctorat, Université Djilali Liabes de Sidi bel Abess, 2017.

[35] L. Likforman-Sulem, E. b. Smith: " ***Reconnaissance des formes* ".** Livre, Ellipses Edition Marketing S.A., ISBN9782-7298-80675. Volume (227 pages). 2013.

[36] J. F. Varga, M. A. Ferrer, C. M. Travieso and J. BAlonso: "***Off-line signature verification based on grey level information using texture feuters***''. Journal. Pattern Recognition, vol. 44, No.2, pp.375-385.

[37] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V.Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero and Q. I. Moro, "***MCYT baseline corpus: a bimodal biometric database***". Article, IEEE Proceeding Vision, Image and Signal Processing, vol. 150, no. 6, 2003.

Annexe A: Généralités sur le Traitement d'Images

1. Généralités sur le traitement d'images

1.1. Définition de l'image

L'image est une représentation planaire d'une scène ou d'un objet situé en général dans un espace tridimensionnel, elle est issue du contact des rayons lumineux provenant des objets formants la scène avec un capteur.

On désigne par traitement d'images numériques l'ensemble des techniques permettant de modifier une image numérique (transformant une image en une autre image, ou en une autre primitive formelle) afin d'améliorer ou d'en extraire des informations qu'on va les utiliser dans différentes applications, par exemple: la reconnaissance, la classification,…etc.

1.2. Types d'images

1.2.1. Image binaire

Une image binaire est une image de taille M *N où chaque point peut prendre uniquement la valeur 0 ou 1. Les pixels sont noirs (0) ou blancs (1).

1.2.2. Image au niveau de gris

Le niveau de gris est la valeur de l'intensité lumineuse en un point. La couleur du pixel peut prendre des valeurs allant du noir au blanc en passant par un nombre fini de niveaux intermédiaires. Donc pour représenter les images à niveaux de gris, on peut attribuer à chaque pixel de l'image une valeur correspondant à la quantité de lumière renvoyée.

1.2.3. Images en couleurs (Polychromes) :

Elle est obtenue par la combinaison de trois couleurs dites primaires : rouge, vert et bleu (RVB), et chaque couleur est codée comme une image à niveaux de gris.

1.3. Caractéristiques de l'image

L'image est un ensemble structuré d'informations caractérisé par les paramètres suivants:

1.3.1. Pixel

Le pixel (abréviation venant de l'anglais : Picture élément) est le plus petit élément qui peut être manipulé par le matériel et les logiciels d'affichage et d'impression.

1.3.2. Résolution

La résolution est le nombre de bits associés à chaque couleur primaire d'un pixel.

1.3.3. Luminance

C'est le degré de luminosité des points de l'image. Elle est définie aussi comme étant le quotient de l'intensité lumineuse d'une surface par l'aire apparente de cette surface, pour un observateur lointain, le mot luminance est substitué au mot brillance, qui correspond l'éclat d'un objet.

1.3.4. Contraste

C'est l'opposition marque entre deux régions d'une image, plus précisément entre les régions sombres et les régions claires de l'image.

1.3.5. Bruit

Un bruit dans une image est considéré comme un phénomène de brusque variation de l'intensité d'un pixel par rapport à ses voisins.

1.3.6. Histogramme

L'histogramme des niveaux de gris ou des couleurs d'une image est une fonction qui donne la fréquence d'apparition de chaque niveau de gris (couleur) dans l'image

1.4. Prétraitement

1.4.1. Filtre Médian : C'est un filtre non linéaire. Les filtres non linéaires sont destinés pour:

- Eliminer le bruit impulsionnel.
- L'intégrité des frontières: on souhaiterait éliminer le bruit sans rendre floues les frontières des objets.

Pour effectuer ce type de traitement sur Matlab nous utilisons la fonction ***«imfilt2 ».***

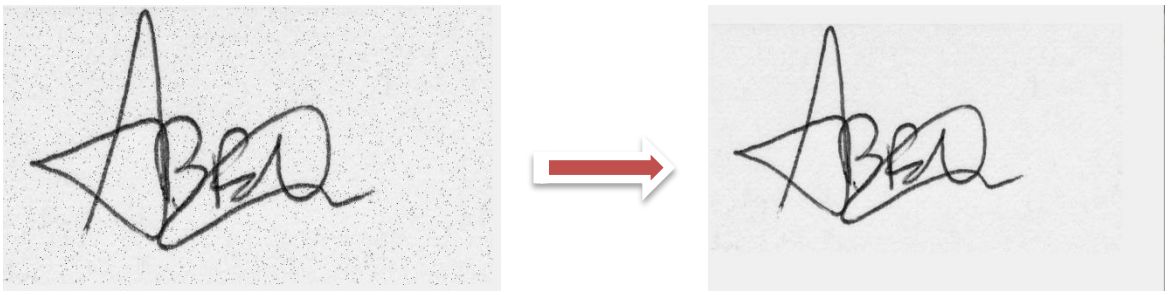


Figure 2: Application de filtrage médian sur une signature.

1.4.2. Egalisation d'histogramme

C'est un traitement à base d'histogramme. L'égalisation d'histogramme est une transformation des niveaux de gris dont le principe est d'équilibrer le mieux possible la distribution des pixels dans la dynamique (Idéalement, on cherche à obtenir un histogramme plat). Pour effectuer ce type de traitement sur Matlab, nous utilisons la fonction ***« imhist ».***

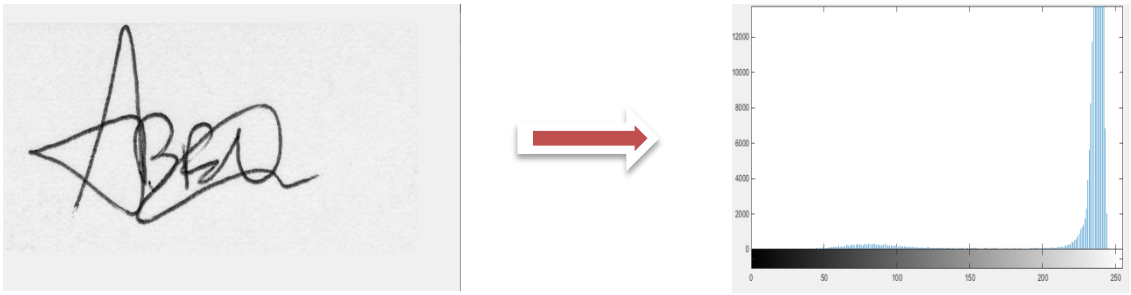


Figure.1 : Exemple d'histogramme d'une image

2. Environnement du travail

Dans cette section, nous présentons les environnements matériel et logiciel de notre travail:

Nous avons implémenté notre système de reconnaissance de signature dans l'environnement de programmation **Matlab R2014b** qui offre une grande simplicité de manipulation des images.

➢ **Pourquoi utiliser Matlab ?**

Matlab est un langage de haut niveau qui permet l'exécution de tâches nécessitant une grande puissance de calcul et dont la mise en œuvre sera bien simple et rapide. Ce langage possède des avantages très intéressants pour les applications sur l'image telle que:

- Il est facile d'accéder et visualiser nos données sur Matlab.
- Facilité de manipulation des matrices ce qui est un point fort et important dans le cas de notre application.
- Utile au traitement et à l'analyse des images.
- Il existe beaucoup d'algorithmes pour l'extraction des caractéristiques et l'apprentissage automatique.

Résumé

La biométrie est une mesure de caractéristique biologique pour l'identification et l'authentification d'un individu à partir de certaines de ses caractéristiques (physiologiques, chimiques, ou comportementales). Dans notre travail, nous nous sommes intéressés à la reconnaissance de signature comme modalité d'identification. La signature manuscrite est l'une des caractéristiques biométriques les plus anciennes et aussi une technique très efficace qui est utilisée dans de nombreuses applications liées à la sécurité. L'objectif visé dans ce travail est d'améliorer les performances de ce système (identification de signature manuscrite hors ligne). Deux contributions principales de notre part ont permis d'atteindre l'objectif cité auparavant. Premièrement, nous avons utilisé le motif local binaire (Local Binary Pattern (LBP)) pour le but d'extraire les caractéristiques statistiques de l'image et évaluer la fiabilité de cette méthode. Des expériences ont été réalisées à l'aide de la base de données MCYT-75. En deuxième lieu, nous avons utilisé la méthode de k-plus proches voisins comme classificateur associé à une mesure de distance, les performances de reconnaissance atteignent respectivement des valeurs de 88,53% et 78,46% pour les distances city block et euclidienne. En troisième lieu, pour but d'extraire le plus grand nombre possible d'informations et améliorer le taux de reconnaissance, nous avons utilisé une autre méthode qui est le LBP en multi-blocs; cette méthode a donné des résultats impressionnants et de meilleurs résultats.

Mots clés : Biométrie, reconnaissance de signature manuscrite, identification de signature, motif local binaire (LBP), k-plus proches voisins (KNN), classificateur, LBP multi-blocs.

Abstract

Biometrics are a measure of a biological characteristic for the identification and authentication of an individual based on some of these characteristics (physiological, chemical, or behavioral). In our work, we have been interested in signature recognition as a method of identification. Handwritten signature is one of the oldest biometric features and also a very effective technology which is used in several securities related applications. The objective of this work is to improve the performance of this system (offline handwritten signature identification). Two main contributions were made from for us to achieve the stated objective. First, we used the Local Binary Pattern (LBP) for the purpose of extracting statistical image characteristics and to assess the reliability of this method. Several experiments were carried out using the MCYT-75 database. In the second, we used the k-nearest neighbor method associated with a metric distance as a classifier, the recognition performances reach the values of 88.53% and 78,46% for city block and Euclidean respectively. Third, in order to extract as much information as possible and improve the recognition rate, we used another method which is a multi-block LBP, which conducted that this method gives interesting and better results.

Keywords: Biometrics, handwritten signature recognition, signature identification, binary local pattern (LBP), k-nearest neighbors (KNN), classifier, multi-block LBP.

ملخص

القياسات الحيوية هي مقياس لخاصية بيولوجية لتحديد ومصادقة الفرد بناءً على بعض هذه الخصائص (الفسيولوجية والكيميائية أو السلوكية). في عملنا، كنا مهتمين بالتعرف على التوقيع كوسيلة لتحديد الهوية. يعد التوقيع بخط اليد أحد أقدم ميزات المقاييس الحيوية وأيضًا تقنية فعالة للغاية تُستخدم في العديد من التطبيقات المتعلقة بالأمان. الهدف من هذا العمل هو تحسين أداء هذا النظام (تحديد التوقيع بخط اليد دون اتصال الجهاز). مساهمتان رئيسيتان جعلتا من الممكن تحقيق الهدف المعلن من قبل. أولاً، استخدمنا النمط الثنائي المحلي LBP لغرض استخراج خصائص الصورة الثابتة. ولتقييم مصداقية هذه الطريقة، أجريت تجارب باستخدام قاعدة بيانات MCYT-75. ثانيًا، استخدمنا طريقة k-الأقرب كمصنف، ووصل أداء التعرف إلى قيم 88,53٪ و 78,46٪ لي city bloc و euclidienne على التوالي. ثالثًا، لاستخراج أكبر عدد ممكن من المعلومات وتحسين معدل التعرف، استخدمنا طريقة أخرى وهي LBP متعددة الكتل، واستنتجنا أن هذه الطريقة تعطي نتائج رائعة.

الكلمات الرئيسية: القياسات الحيوية, التعرف على التوقيع بخط اليد, تحديد التوقيع النمط الثنائي المحلي (LBP), ك أقرب الجيران (KNN), مصنف متعدد الكتل LBP.