République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur Et de La Recherche Scientifique

Université de Ghardaïa

N° d'ordre :
N° de série :

Faculté des Sciences et Technologies
Département des Sciences et Technologies

Mémoire présenté en vue de l'obtention du diplôme de

MASTER

Domaine : *Sciences et Technologies*
Filière : *Automatique*
Spécialité : *Automatique*

Par : SEBROU ABDELAZIZ

Thème

Reconnaissance Automatique Des Signatures Manuscrites Hors-lignes

Soutenu publiquement le :26/05/2015

Devant le jury :

M. BITEUR KADA	Maître Assistant A	Univ. Ghardaïa	**Président**
M. LADJAL BOUMEDIENE	Maître Assistant A	Univ. Ghardaïa	**Examinateur**
M. KIFOUCHE ABDESSALAM	Maître Assistant A	Univ. Ghardaïa	**Examinateur**
M. ARIF MOHAMMED	Maître Assistant A	Univ. Ghardaïa	**Encadreur**

Année universitaire 2014/2015

DEDICACES

Je dédie ce travail à mes parents, qui ont employés tous leurs moyens et efforts, pour m'élever, pour me former, et pour me faire arriver à ce niveau. A tous les professeurs qui ont contribués à ma formation du primaire à l'université.

Je dédie aussi ce travail à mon frère et mes sœurs, A tous ceux que j'aime et qui m'aiment, A ma famille et à mes amis.

REMERCIMENTS

J'aimerais en premier lieu remercier mon dieu Allah qui m'a donné la volonté et le courage pour la réalisation de ce travail.

Je tiens à remercier tout d'abord mon encadreur **M^r^. ARIF MOHAMMED**, pour son aide et disponibilité tout au long de ce projet.

j'adresse mes sincère remerciements à mes parents, mon frère, mes sœurs, et a tous mes amis.

Je tiens à remercier toute personne ayant contribué de près ou de loin a l'aboutissement de mon effort.

Merci à mes professeurs et formateurs du primaire à l'université.

TABLE DES MATIERES

Chapitre III

Approche de vérification

Chapitre IV

Résultats, Analyses et Discussions

Liste des Figures

Chapitre I

Chapitre II

Chapitre III

Chapitre IV

Liste des tableaux

Introduction générale

La biométrie est la technologie d'authentification et d'identification des individus la plus utilisée de nos jours. Elle remplace de plus en plus les anciennes techniques d'identification qui sont basées sur la possession ou la connaissance d'identifiant externe (badge, code, clé…) susceptible d'être perdu, oublié ou encore volé. Elle s'appuie sur la prise en compte des caractéristiques physiologiques, et comportementales propres et uniques à chaque individu.

La vérification de la signature manuscrite est parmi les axes les plus importants de la vérification biométrique de l'identité. En effet, la signature a toujours été le moyen le plus accepté socialement et légalement pour l'identification et l'authentification de tout document officiel. Elle est facile à acquérir, elle résulte d'un geste spontané et propre à chaque individu. En outre, la mise en place d'un système de vérification de signatures est moins coûteuse et plus que celle des systèmes biométriques d'identification basés, par exemple, sur l'iris ou le visage.

Le travail décrit dans ce mémoire propose une contribution à la Vérification Hors-ligne de la Signature Manuscrite. Ainsi, nous allons observer ce geste spontané avec une technique de Modèles de Markov Caché.

A cette fin, nous avons présenté les paramètres d'un HMM, les principaux problèmes dans le calcul du HMM, et donné la méthode de calcul multi-variables, qui nous avons utilisé.
Le plan du mémoire est organisé comme suit :

Chapitre I : Généralités sur les systèmes de reconnaissance biométrique :

Dans le chapitre 1, nous présentons un survol des techniques pour l'identification et l'authentification automatiques de personnes ainsi que des notions sur la biométrie.

Chapitre II : Techniques de Vérification des Signatures Manuscrites :

Ce chapitre sera consacré à l'état de l'art des différentes approches de vérification de signature manuscrite.

Chapitre III: Approche de vérification:

Dans le troisième chapitre, nous présentons une vue d'ensemble des HMMs (Modèles de Markov Cachés), ainsi que l'extraction des paramètres des strokes qui nous donne des résultats acceptable.

Chapitre IV: Résultats, analyses et discussions

Ce chapitre sera dédié à la Vérification Hors-ligne de la Signature Manuscrite, ainsi que les différents tests de validation effectués et la comparaison des résultats obtenus avec d'autres résultats de la même base de données.

Nous terminerons ce mémoire par une conclusion générale sur l'ensemble de cette étude et nous proposerons des perspectives à notre travail.

Chapitre I

Généralité sur Les systèmes de reconnaissance biométrique

I-1. Introduction

Une large variété de systèmes intègrent des techniques de reconnaissance des personnes fiables pour vérifier ou trouver l'identité des individus qui font appel à leurs services. Le but de ces techniques est de s'assurer que les services rendus sont uniquement exploités par des utilisateurs légitimes et n'est pas par n'importe qui. Comme exemples de ces systèmes, on cite : les systèmes de contrôle d'accès aux bâtiments (sites sensibles), les réseaux informatiques, PCs portables, les téléphones cellulaires et les distributeurs automatiques de billets. Ces systèmes sont vulnérables aux ruses d'un imposteur s'ils ne sont pas dotés des techniques de reconnaissance robuste.

Traditionnellement, les mots de passe (reliés à « quelque chose que vous connaissez ») et les cartes d'identification (reliées à « quelque chose que vous possédez ») ont été utilisés pour restreindre l'accès à ces systèmes[l]. Néanmoins, la sécurité de ces systèmes peut facilement être rompue quand un mot de passe est divulgué à un utilisateur non autorisé ou si une carte d'identification est volée par un imposteur : de plus, les mots de passe simples sont faciles à deviner (par un imposteur) et les mots de passe difficiles peuvent être durs à se rappeler (par un utilisateur légitime). L'émergence de la biométrie a pris en charge les problèmes qui tourmentent les méthodes traditionnelles de vérification.

Dans ce chapitre nous introduirons la notion de la biométrie, des systèmes biométriques, les différentes modalités utilisées actuellement ou peut être prochainement ainsi que les diverses applications qui en découlent.

I-2. Qu'est-ce que la biométrie ?

Une ancienne définition du mot biométrie est : « Étude statistique des dimensions et de la croissance des êtres vivants » ou « Mesure des dimensions du corps humain, d'un organe ».

Une définition plus récente décrit la biométrie connue étant une « Technique permettant de contrôler l'identité de quelqu'un par la reconnaissance automatique de certaines de ses caractéristiques physiques ou comportementales préalablement enregistrées (empreintes digitales, visage, voix, etc.) » [Larousse 2015]. Ainsi, la biométrie repose sur «Technique qui permet d'associer à une identité une personne voulant procéder à une action, grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques physiques et comportementales de cette personne préalablement enregistrées (empreintes digitales, visage, voix, etc.) ».

I-3. Les systèmes de reconnaissance biométrique

Un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques physiques ou comportementales d'un individu. Ces caractéristiques doivent être universelles, uniques, permanentes, collectables et mesurables. La finalité d'un système biométrique est la vérification et l'authentification (pour l'éligibilité à un accès ou à des services), l'identification ou encore le chiffrement de données à l'aide d'une clé biométrique.

La reconnaissance biométrique est le processus décisionnel permettant de reconnaître au moyen des caractéristiques biométriques les identités des individus proclamées. Pour que la reconnaissance soit envisageable et fiable, les caractéristiques extraites des individus servent à la reconnaissance biométrique doivent au moins garantir les conditions suivantes [1], [2], [3], [4]:

- **L'unicité:** il faut qu'il n'existe pas deux individus ou plus ayant les mêmes traits biométriques;
- **La discrimination:** il faut qu'elles fournissent une variation significative inter individus et une variation minime entre les différentes instances de la même personne;
- **La persistance:** les caractéristiques biométriques ne doivent pas muter au fur et à mesure du vieillissement. En outre, il faut qu'elles ne soient pas trop dépendantes de l'état pathologique (stress, joie, …etc.) ou l'état sanitaire de l'individu ;
- **Difficile à l'usurpation:** le défi majeur des systèmes biométriques est de lutter contre la fraude et l'usurpation de l'identité. En effet, c'est cette difficulté d'usurper les caractéristiques biométriques qui distingue les systèmes biométriques par rapport aux systèmes classiques d'authentification (mot passe, carte d'accès,…etc.).

I-4. Les tâches d'un système de reconnaissance biométrique

Selon le contexte d'application, un système biométrique peut fonctionner selon deux principales tâches sont [4]:

- **L'authentification (Vérification):** le système valide l'identité d'une personne en comparant ses données biométriques prélevées avec celles qui ont été préalablement prélevées et stockées dans sa base de données. Dans un tel système, l'individu désirant être reconnu proclame son identité, généralement, via son numéro d'identification PIN (Personal Identification Number). Son nom d'utilisateur (user name) ou sa carte à puce. Ainsi, le système fait une comparaison un à un pour confirmer ou infirmer l'identité proclamée.
- **L'identification:** le système établit l'identité d'une personne en comparant ses données biométriques prélevées avec celles de toutes les personnes qui ont été préalablement prélevées et stockées dans sa base de données. Dans un tel système, l'individu désirant être

reconnu n'est pas obligé de donner son identité. Ainsi, le système fait une comparaison un à plusieurs pour établir l'identité d'une personne.

I-5. L'architecture d'un système de reconnaissance biométrique

Un système générique d'authentification biométrique fonctionne selon les étapes suivantes:

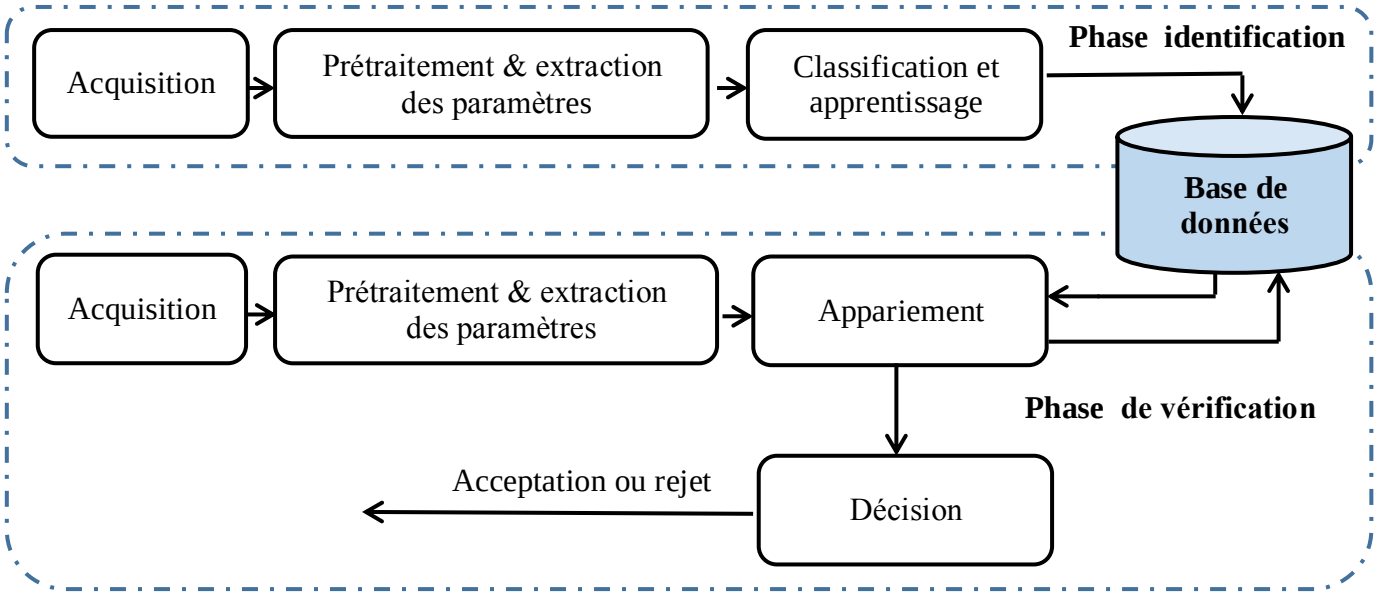


Figure I- 1: Architecture d'un système de reconnaissance biométrique automatique.

I-5-1. Acquisition

Un système d'acquisition équipé d'un capteur est utilisé pour acquérir une caractéristique spécifique de l'utilisateur, par exemple: une caméra ou un microphone dans le cas de la voix.

I-5-2. Prétraitement et extraction des paramètres

Ayant une image ou une voix en entrée, une étape de segmentation permet d'extraire la caractéristique dont le processus d'authentification a besoin. Par exemple: extraire le visage du fond d'une image dans le cas de l'identification de visage.

I-5-3. Classification et apprentissage

En examinant les modèles stockés dans la base de données, le système collecte un certain nombre de modèles qui ressemblent le plus à celui de la personne à identifier, et constitue une liste limitée de candidats. Cette classification intervient uniquement dans le cas d'identification car l'authentification ne retient qu'un seul modèle (i.e. celui de la personne proclamée).

I-5-4. L'appariement (*matching*)

Le matching consiste à évaluer le taux de similarité entre deux objets. Dans le cas de l'authentification, le score du matching est calculé entre le modèle de l'identité revendiquée, préalablement enregistré, et le vecteur des paramètres biométriques en entrée. L'identité

proclamée sera accordée si et seulement si le score du matching dépasse un certain seuil qu'on considère suffisant.

Le problème de l'identification est plus crucial car le système doit deviner l'identité de la personne à partir des données biométriques disponibles. Dans le jargon de la classification, l'authentification consiste à voir si l'exemple (vecteur de paramètres à tester) appartient à la classe modélisant l'identité proclamée ou le reste des classes.

I-5-5.Décision

Dans le cas de l'identification, il s'agit d'examiner les modèles retenus par un agent humain et donc décider. En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes: l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas. Elle est basée sur un seuil prédéfini.

Il est impossible d'obtenir ligne coïncidence absolue (100% de similitude) entre 1e fichier créé lors de l'enrôlement et le fichier créé lors de la vérification. Les éléments d'origine (une image, un son...) utilisés pour les traitements informatiques ne pouvant jamais être reproduit à l'identique. Les performances des systèmes d'authentifications biométriques s'expriment par :

• T.F.R - Taux de Faux Rejets (False Rejection Rate) : Il s'agit des gabarits biométriques rejetés par le système de vérification alors qu'il ne devrait pas l'être.

• T.F.A - Taux de Fausses Acceptations (False Acceptance Rate) : il s'agit des gabarits identifié par le système biométrique comme étant un gabarit biométrique de référence stocké dans ce système, par exemple, dans une base de données dédiée au système biométrique.

• T.E.E - Taux d'Egale Erreur (Equal Error Rate), donne un point sur lequel le T.F.A est égal au T.F.R.

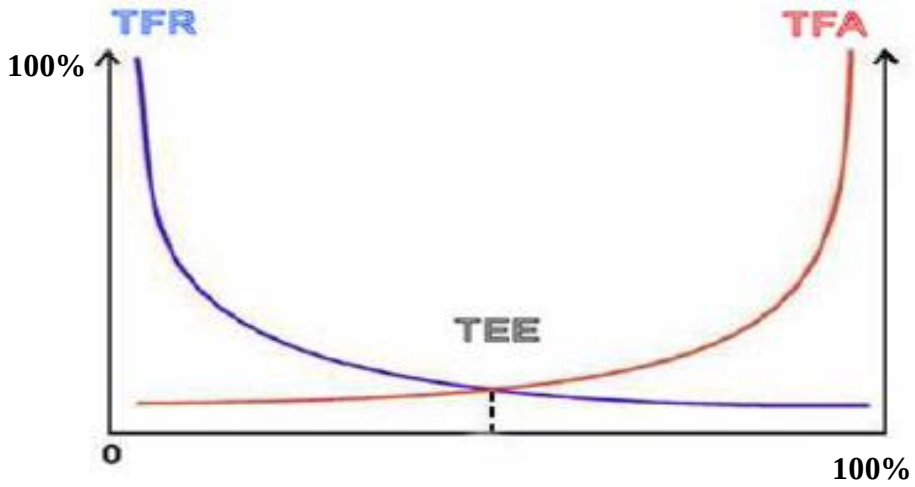


Figure I- 2:Le TFR et le TFA en fonction de la marge d'erreur autorisée

Ce graphe est purement démonstratif: A représenter la marge d'erreur autorisée par le système, variant de 0 à l'infini on voit que plus la marge d'erreur autorisée est importante, plus le taux de fausses acceptations augmente, c'est-à-dire que l'on va accepter de plus en plus de personnes qui, normalement, n'ont pas le droit d'accès (et donc la sécurité du système diminue). Par contre, on voit que le taux de rejet des personnes ayant le droit d'accès diminue également, ce qui rend le système plus fonctionnel et répond mieux aux attentes des utilisateurs. A l'autre extrémité, si l'on diminue la marge d'erreur acceptée par le procédé de mesure biométrique, les tendances des deux taux sont inversées : on va de moins en moins accepter des individus essayant de frauder mais on va aussi, par la même occasion, avoir un taux de rejet sur des personnes autorisées qui sera trop important pour être toléré dans la plupart des cas. Le compromis habituel est de prendre la jonction des courbes, c'est â dire le point où le couple (TFR, TFA) est minimal.

I-6. Différentes techniques biométriques

Actuellement, il existe plusieurs techniques biométriques différentes permettant d'identifier ou de vérifier une personne [3], [4], [5]. Celles-ci sont répertoriées dans trois catégories.

I-6-1. Techniques physiologiques (statiques)

I-6-1-1. Forme de la main ou des doigts de la main

Cette technologie se base sur la géométrie de la main dans l'espace. Nonante caractéristiques sont prises en compte comme la longueur et la largeur des doigts, la largeur et l'épaisseur des paumes, la forme des articulations, les dessins des lignes de la main,...

Figure I- 3: Identification de la forme de la main.

Avantages	*Inconvénients*
➢ Bonne acceptation des usagés ; ➢ Très simple à utiliser ; ➢ Le résultat est indépendant de l'humidité et de l'état de propreté des doigts.	➢ Risque de fausse acceptation pour des jumeaux ou des membres d'une même famille; ➢ Trop encombrant pour un usage sur le bureau ou dans une voiture.

I-6-1-2. Les veines

Cette technique est habituellement combinée à une autre, comme l'étude de la géométrie de la main. II s'agit ici d'analyser le dessin formé par le réseau des veines sur les parties du corps d'un individu (la main) pour en garder quelques points caractéristiques.

Figure I- 4: Le réseau veineux de la main

Avantage

Il n'existe aucun moyen de frauder, car on ne peut pas "photographier" les veines de la main. Le réseau vasculaire est propre à chaque individu : même les vrais jumeaux en ont un différent.

Inconvénient

La méthode est encore trop récente pour être correctement évaluée. Le scanner est relativement encombrant comparé aux capteurs d'empreintes digitales.

I-6-1-3. Empreintes digitales

Les systèmes de reconnaissance d'empreintes digitales exploitent la forme géométrique des parties (surfaces) inférieures des bouts des doigts pour effectuer la reconnaissance des personnes.

Cette technique utilisait au départ par la police scientifique, la reconnaissance par empreinte digitale est aujourd'hui la technique la plus largement utilisée [6].

Figure I- 5: Etapes du traitement d'une empreinte digitale

Avantages	*Inconvénients*
➢ Technique évoluée et éprouvée ➢ Grande précision; ➢ Peuvent être installés dans divers milieux; ➢ Dispositifs ergonomiques et faciles à utiliser; ➢ Permettent d'enrôler plusieurs empreintes (plus grande précision et fiabilité);	➢ Enrôlement impossible pour un faible pourcentage; ➢ Performance pouvant se détériorer avec le temps; ➢ Association psychologique à une enquête criminelle.

I-6-1-4. Visage

C'est la technique la plus simple et la moins contraignante. Mais elle a encore de gros progrès à faire. En mode vidéo, les résultats ne sont pour l'instant pas très probants.

Cette technologie se base sur des caractéristiques telles que l'écart entre les yeux, la forme de la bouche, le tour du visage, la position des oreilles,... En tout, plus de 60 critères fondamentaux existent.

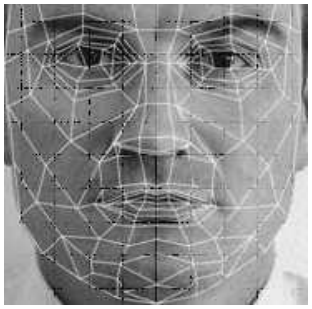


Figure I- 6: Points clés dans la reconnaissance faciale

Avantages	*Inconvénients*
➢ Peuvent s'appuyer sur l'équipement d'acquisition des images actuel; ➢ Peuvent comparer des images statiques, comme des photos de permis de conduire; ➢ Seule technique biométrique offerte sur le marché capable de fonctionner sans la collaboration du sujet.	➢ Les changements dans l'environnement d'acquisition des images (principalement la lumière et l'angle de l'appareil photo) peuvent avoir une incidence sur l'exactitude de la concordance; ➢ Les changements physiques peuvent tromper le système; ➢ Fortes préoccupations relatives au respect de la vie privée en raison de leurs Capacités d'enrôlement et d'identification sans la collaboration des sujets

I-6-1-5. Rétine

Cette technique se base sur le fait que le dessin formé par les vaisseaux sanguins de la rétine (Figure I-7), paroi interne de l'œil, est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. Mais, elle est moins bien acceptée par les utilisateurs à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques millimètres), l'image de la rétine est numérisée par un laser à faible intensité en effectuant un balayage de celle-ci.

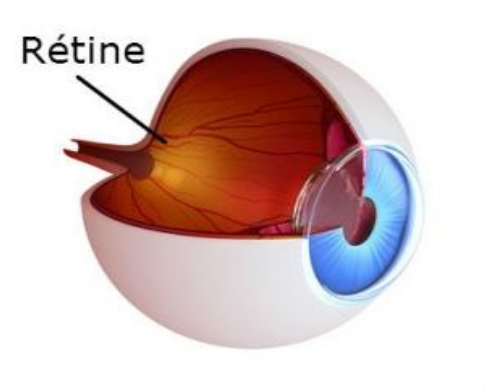


Figure I- 7: Image d'une rétine

Avantages	*Inconvénients*
➢ Extrêmement précis ➢ Très difficiles à mystifier	➢ Relativement difficiles à utiliser ➢ N'est pas largement distribués sur le marché

I-6-1-6. L'iris

En ce qui concerne l'iris (Figure I-8), l'individu se place en face du capteur (caméra) qui scanne son iris. Cette technique est relativement désagréable pour l'utilisateur car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct.

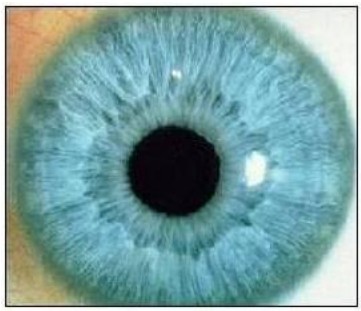


Figure I- 8: Iris d'un œil humain

Avantages	*Inconvénients*
➢ Potentiel de très grande précision ➢ Peuvent être utilisés pour l'identification et la vérification ➢ Les structures de l'iris restent stables durant toute la vie.	➢ L'acquisition des images exige une certaine formation et de la pratique. ➢ L'acquisition des images crée un certain inconfort chez l'utilisateur, ce qui peut empêcher l'enrôlement de certaines personnes. ➢ Le nombre de faux rejets est plus élevé que pour les autres techniques

I-6-2. Techniques comportementales (dynamiques)

I-6-2-1. La voix

La technologie de reconnaissance vocale se base sur les caractéristiques de la parole, constituée par une combinaison de facteurs comportementaux (vitesse, rythme,...) et physiologiques (tonalité, âge, sexe, fréquence, accent, harmonique,...)

Elle est vulnérable (utilisation d'un enregistrement, par exemple) mais peu intrusive.

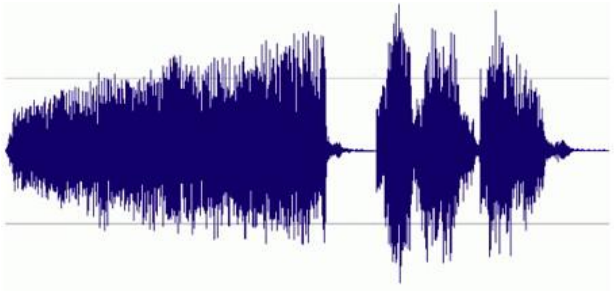


Figure I- 9: Spectre de la voix

Avantages	*Inconvénients*
➢ Peuvent exploiter la vaste infrastructure téléphonique. ➢ Se fondent bien avec la reconnaissance de la parole et les mots de passe vocaux. ➢ Aucune connotation négative, contrairement à d'autres techniques biométriques	➢ Leur conception les rend vulnérables à la fraude à l'aide d'enregistrements. ➢ Les dispositifs de capture de piètre qualité et le bruit ambiant limitent souvent leur précision. ➢ Les gabarits sont généralement très volumineux comparativement à ceux des autres techniques biométriques.

I-6-2-2. Techniques de frappe au clavier

Cette technologie correspond grosso modo à la transposition de la graphologie aux moyens électroniques. Sont pris en compte : la vitesse de frappe, la suite de lettres, la mesure des temps de frappe, la pause entre chaque mot, la reconnaissance de mots précis,...

Figure I- 10 : Dynamique de frappe au clavier.

Avantages	*Inconvénients*
➢ Exploitent le matériel existant ➢ Exploitent le processus d'authentification par mot de passe ➢ Un mot de passe peut être changé au besoin. ➢ Perçus comme non contraignants	➢ Technique récente ➢ Renforcent la sécurité, mais ne sont pas plus pratiques pour autant ➢ Conservent bien des défauts de l'authentification par mot de passe

I-6-2-3. *Reconnaissance de la signature*

La vérification de signature est le processus utilisé pour identifier les signatures manuscrites d'un individu [7]. Elle a été pratiquée pendant des siècles, et l'acte de signer un document a été longtemps accepté par presque chaque culture dans le monde en tant que son identification. De nos jours, il est généralement employé et accepté comme une manière de vérifier l'identité des personnes dans une grande variété de buts, particulièrement dans légal, les banques, le film publicitaire, et même les documents éducatifs [8].

Figure I- 11 : Exemple de signature de base de données MAUG14/15

Avantages	*Inconvénients*
➢ Résistent mieux aux imposteurs que les signatures habituelles ➢ Généralement perçus comme non Contraignants ➢ Les utilisateurs peuvent changer de signature selon l'usage.	➢ Les signatures changeantes augmentent le taux d'erreur. ➢ Les utilisateurs n'ont pas l'habitude de signer sur une tablette graphique

I-6-3. Techniques émergentes

I-6-3-1. ADN (l'acide désoxyribonucléique)

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire. L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'acide désoxyribonucléique (ADN) [9][10], Cette technique est complexe, coûteuse et lente à réaliser compte tenu des nombreuses manipulations biologiques (amplification + électrophorèse). Ceci explique ce fait qu'il n'existe toujours pas de solution technologique grand-public qui permette de réaliser automatiquement cette analyse, d'autant plus qu'elle nécessite un prélèvement d'échantillon (sang, salive, sperme, cheveux, urine, peau, dents, etc.) qui rend cette technique très intrusive.

Figure I- 12: Illustration de l'acide désoxyribonucléique « ADN »

I-6-3-2. Analyse de la démarche

La technique biométrique de reconnaissance de la démarche utilise la posture et les caractéristiques de locomotion en vue de contribuer à l'identification. Toujours au stade de la recherche, cette technique présente des éléments intéressants. Comme la reconnaissance faciale, elle permet d'identifier un sujet à distance, sans sa collaboration et à son insu. Cette technique peut être utile lors des activités de surveillance et pourrait mieux déjouer les déguisements que la reconnaissance faciale. Il reste encore beaucoup à faire avant que la reconnaissance de la démarche ne devienne une technique commerciale viable.

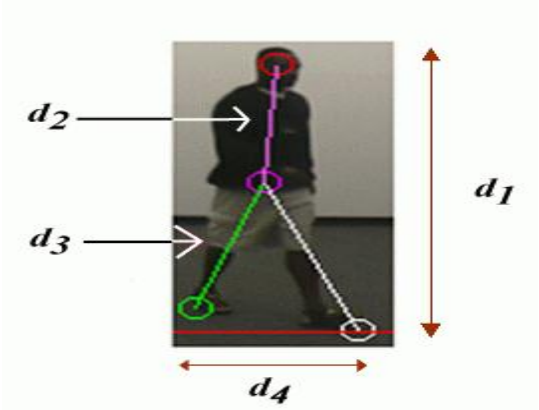


Figure I- 13: Caractéristiques de la marche

Avantages	*Inconvénients*
➢ Alternative à la reconnaissance faciale ➢ Peuvent fonctionner sans la collaboration du sujet	➢ N'est pas bien développés et pas offerts sur le marché ➢ Des changements comportementaux de la démarche peuvent tromper le système. ➢ Fortes préoccupations relatives au respect de la vie privée en raison de leurs capacités d'enrôlement et d'identification sans la collaboration des sujets

I-7. Conclusion

Au cours de ce premier chapitre de généralité sur les systèmes de reconnaissance biométrique, nous avons tout d'abord expliqué qu'est-ce que veut dire la biométrie et exposé comment authentifier et identifier automatiquement un individu ainsi que donné un aperçu des différentes technologies existantes. Alors que certaines d'entre elles sont employées depuis plus d'un siècle pour identifier des individus, d'autres technologies plus innovantes ne sont encore qu'à un stade purement expérimental. Ces technologies émergentes ne seront peut-être jamais réellement développées, car jugées incompatibles avec les spécifications imposées par un marché de masse (prix, acceptabilité, etc.). Cependant cette recherche de nouvelles techniques et d'amélioration est indispensable car aucune solution biométrique actuelle ne répond parfaitement au problème d'identification ou de vérification automatique de personnes. Trois axes d'amélioration sont principalement concernés : (i) réduire les taux d'erreurs, (ii) faciliter l'intégration des systèmes biométriques dans les objets nomades, (iii) et aussi les rendre plus accessibles vis à vis de l'utilisateur (moins intrusif et contraignant).

Pour conclure ce chapitre, nous soulignons l'impact potentiel de la biométrie sur la protection des renseignements personnels et la vie privée. La biométrie a été présentée comme un remède universel aux problèmes de sécurité (terrorisme, fraude, plus de mots de passe ou cartes qu'on égare, etc.)- Mais « bien que la plupart des techniques biométriques soient des outils de sécurité fort efficaces, elles ne brillent pas par leur innocuité en ce qui concerne la protection de la vie privée et des renseignements personnels ». Dans le chapitre suivant, nous présenterons les systèmes biométriques basés sur la signature manuscrite hors ligne.

Chapitre II

Techniques de Vérification des Signatures Manuscrites

II-1. *Introduction*

La signature manuscrite est depuis plusieurs siècles le moyen le plus répandu pour manifester sa propre volonté. Elle est aujourd'hui, et le demeurera sans doute dans le futur, le moyen biométrique d'authentification le plus utilisé pour identifier des documents et pour responsabiliser les gens face à l'engagement. Il existe actuellement plusieurs paramètres permettant l'identification d'un individu soit pour des raisons de sécurité, de confidentialité, de repérage et pour d'autres raisons. Citant par exemple : les systèmes bancaires, informatiques, juridiques et les centres de recherches avec accès limités. Il y a aussi d'autres méthodes fréquemment adoptées telle que l'utilisation des codes alphanumériques, les cartes d'accès ou les mots de passe pour l'utilisation des réseaux informatiques ou bancaires. D'autres approches sont basées sur des caractéristiques biométriques telles que la taille, le poids, la voix, les empreintes digitales, etc.

Dans ce chapitre, nous donnerons une définition de la signature manuscrite, et nous présenterons les différentes classes et types de signature manuscrite, ainsi que les différentes approches de vérification de signature manuscrite.

II-2. *Définition*

L'utilisation de la signature manuscrite repose sur l'hypothèse que ces sont plus des mouvements instinctifs que des actes conscients qui sont impliqués dans la réalisation de la signature. Ce postulat implique que certaines caractéristiques de la signature sont stables donc constantes pour un signataire. Ainsi, la signature en ligne ou hors ligne peut être considérée comme une méthode biométrique comportementale. La principale difficulté concernant l'authentification est que la signature en entrée et la (ou les) signature(s) servant de référence ne sont pas exactement les mêmes. Pour que cette reconnaissance soit exacte, il faut que la variation existant entre les signatures d'une même personne soit inférieure à la distance entre les signatures de deux personnes différentes. Il faut donc essayer d'isoler les parties ou caractéristiques de la signature qui sont pratiquement constantes, de celles qui ne le sont pas.

A cet effet, les systèmes bancaires et judiciaires ont recours lors de litiges à des experts pour l'authenticité de la signature ou documents, et malgré qu'elle fournit des résultats satisfaisants mais elle reste toujours coûteuse en temps et expertise, d'où la nécessité d'un système automatique pour la vérification et l'authentification [1].

La condition nécessaire pour la construction d'un bon système de vérification de signatures, c'est la bonne caractérisation de ces dernières. Parmi ces caractéristiques et mesures :

Mesures globales : utilisant des paramètres géométriques telles que les dimensions de la signature (sa hauteur et sa largeur), les projections (projection horizontale et verticale), la pente (l'inclinaison de la signature par rapport à l'axe horizontale) et l'enveloppe (contour convexe enveloppant la signature).

Mesures locales : C'est une approche classique qui est basée sur l'extraction de caractéristiques locales pour caractériser les signatures, ces mesures sont basées sur l'évaluation de la distribution de l'encre à différentes résolutions et de régions de forte pression. Pour une signature donnée, le squelette, le contour ainsi que les frontières suivant les directions (nord, sud, est et ouest) sont calculées et forment un vecteur dont la taille varie suivant la résolution voulue.

II-3. *L'authentification des signatures*

Le terme "authentification" couvre en fait deux sous problèmes : l'identification et la vérification. L'identification consiste à déterminer, à partir d'une base de référence, la personne dont la donnée biométrique est la plus proche de celle testée. Dans ce cas, la réponse du système sera le nom de la personne ou le rejet de la donnée biométrique si aucune des références stockées dans la base n'est assez proche de la donnée testée.

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

Le résultat net d'une signature est une entité fortement variable et sa vérification n'est pas insignifiante, même pour les experts humains [2].

II-3-1. Les classes de signatures

On distingue deux classes de signatures : la classe des signatures authentiques et la classe des fausses :

II-3-1-1. La classe authentique : la classe des signatures authentiques d'un individu est caractérisée par une grande variabilité intra-classe. De plus, la signature authentique en général possède une diversité infinie de styles. Cependant, des groupes peuvent facilement être identifiés:

a. la signature de type Nord Américain : habituellement lisible,
b. la signature de type Européen (le paraphe) : habituellement très personnalisée et caractérisée par l'absence de la forme sémantique ce qui la rend totalement illisible,
c. la signature de type Arabe : qui possède en partie les caractéristiques de l'écriture cursive propre à la culture arabe et qui peut être également lisible ou très personnalisée au même titre que le paraphe,
d. la signature de type Asiatique : qui est facilement distinguable des autres types mentionnés précédemment.

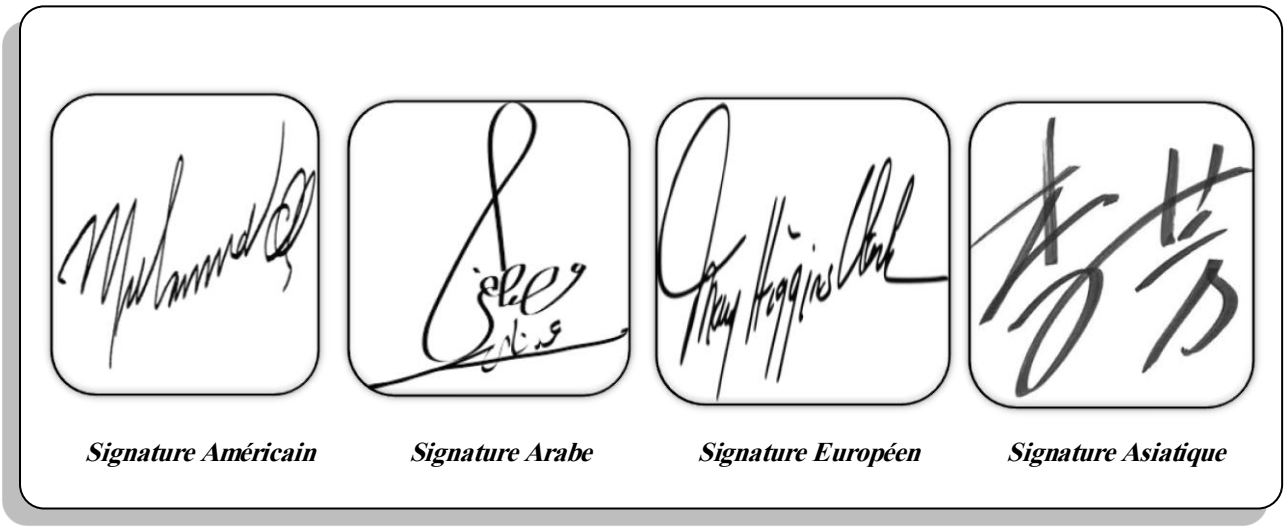


Figure II- 1: Différents types de signatures de classe authentique.

II-3-1-2. La classe des fausses: la classe des fausses signatures est également subdivisée en plusieurs groupes qui ont leurs signes distinctifs. Les principaux groupes de faux sont [1] :

a. *Le faux par déguisement*
b. *Le faux par imitation servile*
c. *Le faux par imitation libre*
d. *Le faux par calque*
e. *Le faux par photocopie*
f. *Le faux grossier*
g. *Le faux aléatoire*
h. *Le faux simple*

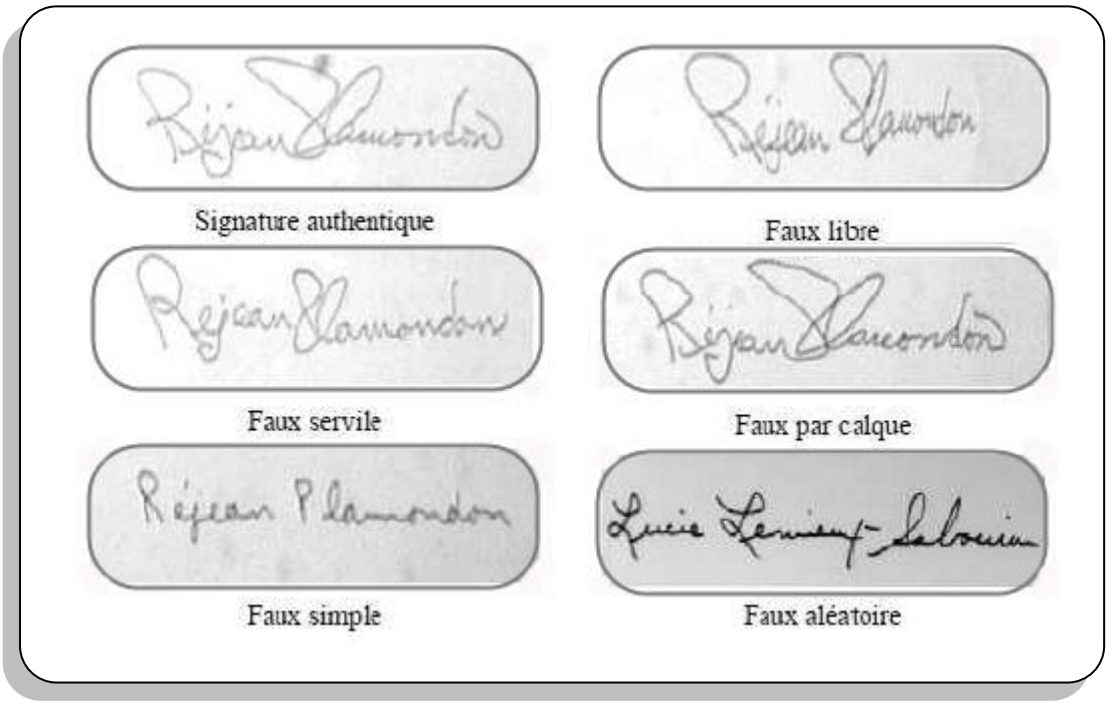


Figure II- 2: Exemple des signatures fausses [1].

II-3-2. Les approches de vérification de signature

En raison de l'acceptabilité élevée des signatures personnelles, particulièrement leur utilisation dans des transactions financières, la vérification automatique de signature est devenu un naissant rapide dans l'horizon de l'authentification biométrique. Les systèmes automatiques de vérification des signatures peuvent être classifiés largement en tant qu'en ligne (online) et hors ligne (offline).

II-3-2-1. L'approche hors-ligne (offline)

Dans un système de vérification de signature offline, les données statiques visuelles d'une signature sont utilisées pour la vérification.

La figure II-3 illustre une représentation du système hors-ligne (offline) de vérification de signature [4]. Le système hors-ligne (*offline*) prend seulement une image de signature à travailler dessus, où il est très difficile d'extraire les paramètres uniques du signataire permanent et véritable avec robustesse. Le système peut être vu suivant trois modules : module d'acquisition et de prétraitement d'image, module d'inscription et de vérification. Le module d'acquisition et de prétraitement d'image est responsable d'extraire l'image de signature à partir d'un document balayé et de la prétraiter après pour une extraction plus lointaine de paramètres. N'importe quel module de balayage ordinaire avec assez de résolution peut être utilisé comme

outil d'acquisition d'image. Pendant le prétraitement, ébruiter probablement présenté par le matériel de balayage est enlevé et la signature est binarisée.

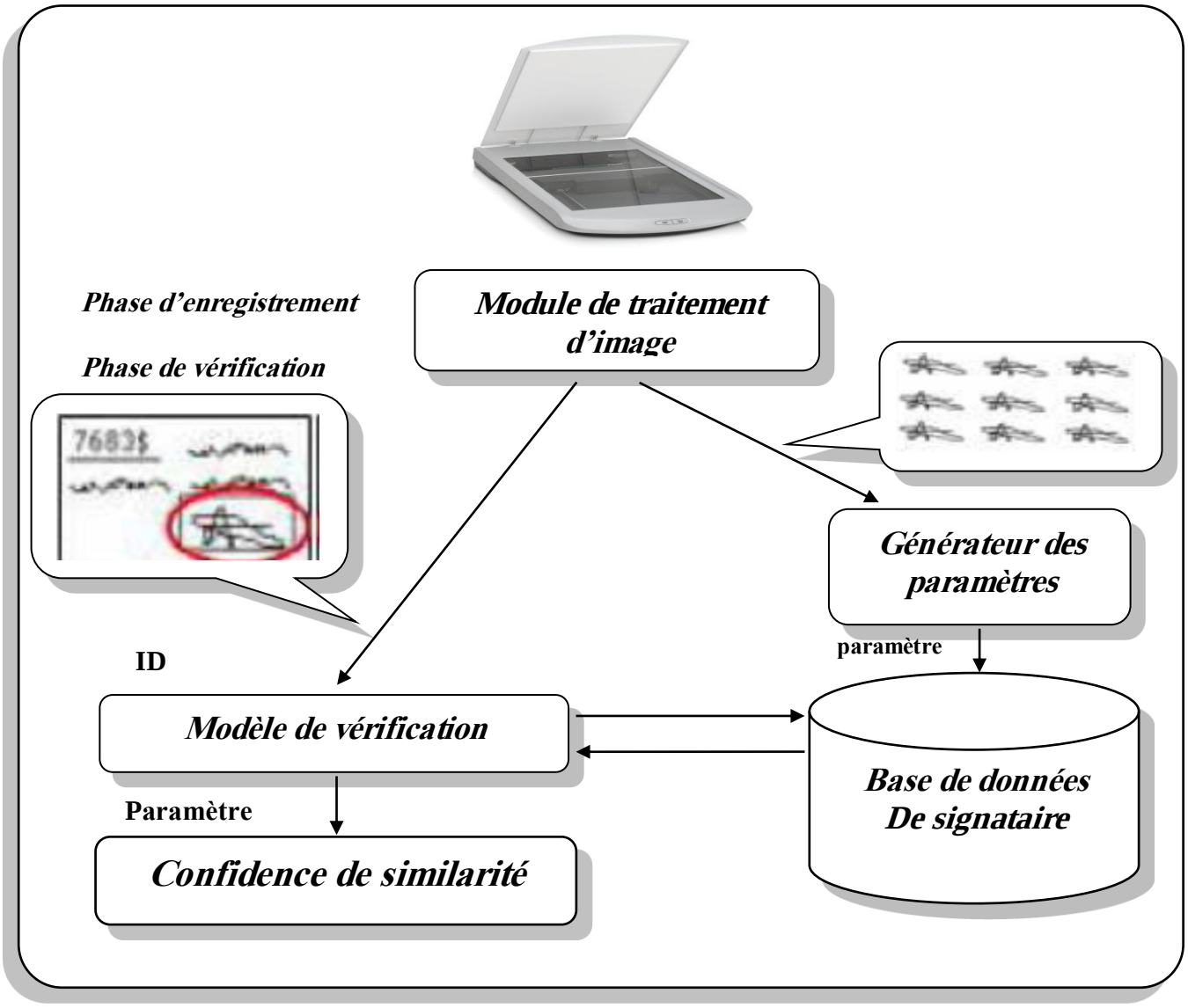


Figure II- 3: Représentation du système de vérification de signature offline

Le module de vérification utilise le profile type pour authentifier une signature donnée par rapport à l'identification référencée premièrement (il a extrait et expérimenté avec des enveloppes de signature et de diverses projections comme paramètres), les signatures de référence et la similitude évaluées correspondant à l'identification référencée, sont recherchées dans la base de données du système .

a/-Prétraitement

Après avoir numériser le document contenant la signature. À partir d'un scanner, ou une camera devant la quelle défile le document. Un prétraitement préliminaire permettant d'enlever le bruit ainsi que toute autre information n'appartenant pas à la signature est effectué, sachant que le prétraitement regroupe toutes les techniques visant à améliorer la qualité d'une image.

Généralement, le processus de vérification de signature se fait en deux phases: l'apprentissage et la vérification,et avant ce processus, il y'a une phase de prétraitement. Cette dernière phase comporte:

- ***Acquisition :***

Dans le contexte de la saisie hors-ligne, les systèmes d'acquisition les plus courants sont essentiellement des scanners ou des caméras . Les scanners actuels ont une résolution qui est au minimum de 300 dpi (dpi : dots par inch).

- ***Base de donnée***

Nous avons crée une base de donnée de cinquante personnes pour notre projet, La plupart sont des étudiants de l'université de Ghardaïa dans une durée de trois semaines, dans chaque semaine nous prenons trois signatures pour tous les personnes dans des périodes de temps différentes pour capturer les variations intra-personnels de signature et on a obligé les signataires d'utiliser un stylo blue ou bien noir pour éviter les problèmes de clarté (niveau de gris) de l'image lors de la numérisation. Après la création de base de donné nous utilisons un scanner de 300 dpi (dpi : dots par inch) pour prendre le signature au format image et on a coupé les neuf signatures de chaque person avec un dimension 128*128 pixels et l'enregistrer en extension (.bmp) et les signatures se nommer comme suivent "PnSm.bmp" **P** et **S** des caractères (P : personne, S : signature) ,**n** est le numéro de personne (1-50) et **m** est le numéro de la signature (1-9) (**Figure II- 4(a)**).

- ***Lissage et binarisation***

Le lissage permet de diminuer les différences des niveaux de gris entre les pixels voisins et le bruit du document en cours d'acquisition qui sera enlevé par un filtrage médian [5] (**Figure II- 4(b)**). La binarisation se fait en employant l'algorithme d'histogramme-base de seuillage global proposé par Otsu [6]. Une opération de fermeture morphologique avec carré structurant 3×3 éléments est appliqué à la binarisation d'image [7]. (**Figure II- 4(c)**).

- ***La squelettisation***

La squelettisation est une opération qui permet de passer d'une image à sa représentationen "fil de fer". Le squelette a un pixel d'épaisseur. C'est une manière de

représenter l'information indépendamment de l'épaisseur initiale de l'écriture (**Figure II-4(d)**).

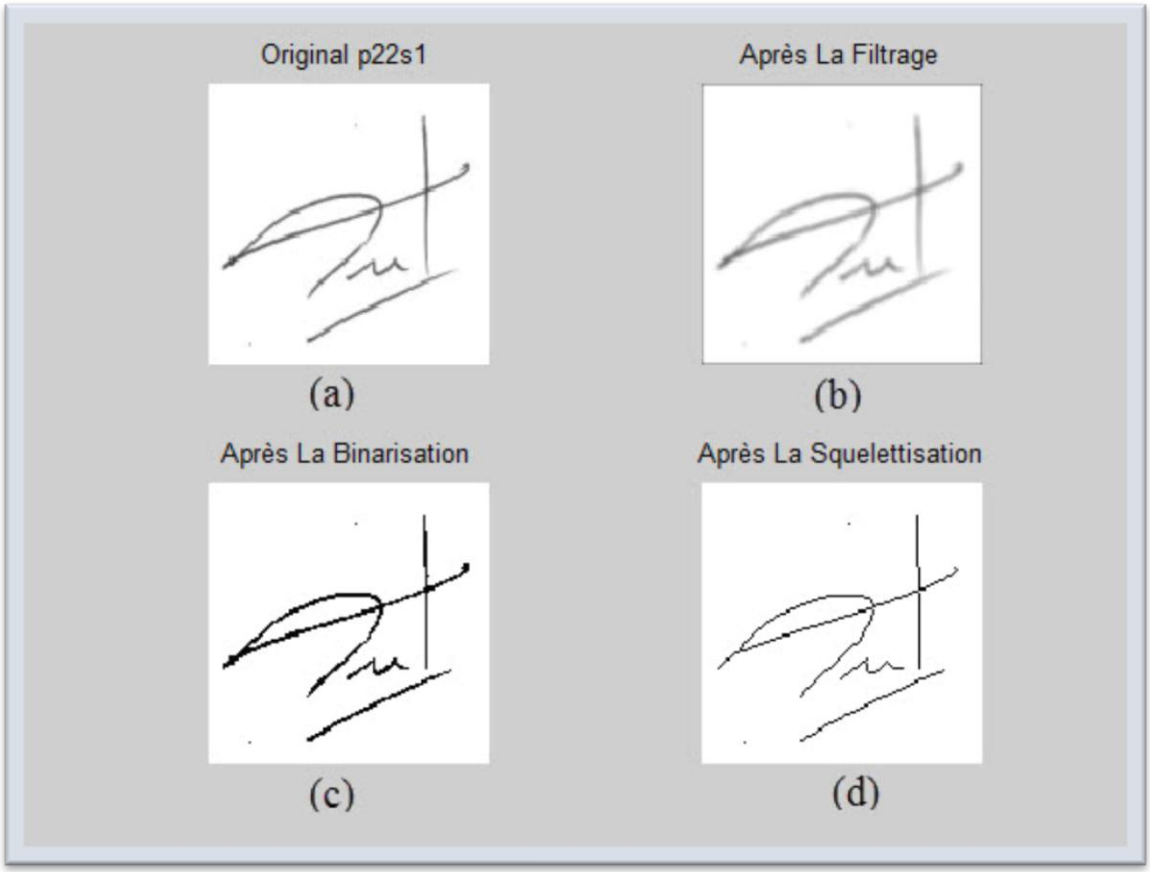


Figure II- 4: phase de prétraitement.

- ***Segmentation en strockes***

C'est la partie la plus importante. Elle a pour but de faciliter l'identification des éléments manuscrits . La segmentation est effectuée se référant le nombre de strokes composants de la signature enregistrée . Dans notre cas nous avons segmente les images de signature (128 * 128 pixels) a seize segments chaque segment de 32 *32 pixel (**Figure II-5**).

- ***Pourquoi segmenter une signature?***

Durant un système de vérification de signatures manuscrites, la segmentation a pour but de faciliter l'identification des éléments manuscrits, si on considère que l'information contenue dans la signature est initialement trop complexe. Par exemple, la segmentation d'une signature de 300 points pourrait produire moins de 20 segments. Identifier 20 segments au lieu de 300 points apparaît comme une tâche beaucoup plus facile à exécuter. D'autre part, si on considère que le tracé de la signature est constitué d'une séquence de

mouvements de la main correspondants aux segments (portions de la signature sans changement « majeur » de direction), il n'est pas nécessaire d'aller chercher l'information située à plus petite échelle, (i.e. les points).

Figure II- 5: signature après la segmentation.

- ***Normalisation*** :

Après la segmentation de signature en strockes on choisi seulement les segments qui contiennent les plus grandes quantités d'information dans la signatures (par exemple : on fixe un seuil, somme des pixels noir dans chaque segment, si la somme est superieure au seuil nous le prenons sinon on l'élimine le segment (**Figure II- 6**) le seuil qui Nous avons choisi c'est 40 pixels.)

b/- La vérification

La vérification hors-ligne (offline) de signature a une utilisation significative principalement en établissant l'authenticité des chèques de banque et d'autres documents officiels, basée sur les signatures qu'ils portent. Dans le système proposé, au lieu de classifier une signature seulement en tant que véritable ou contrefaçon, la signature est classifiée dans trois classes : véritable, contrefaçon, et incertain. De cette façon, les signatures qui peuvent être

identifiées en tant que véritables et la contrefaçon avec confiance sont séparées, et un examinateur humain (agent de banque ex-responsable de l'inspection de signature) examina seulement une petite partie de signatures classifiées dans la troisième classe des signatures incertaines [5].

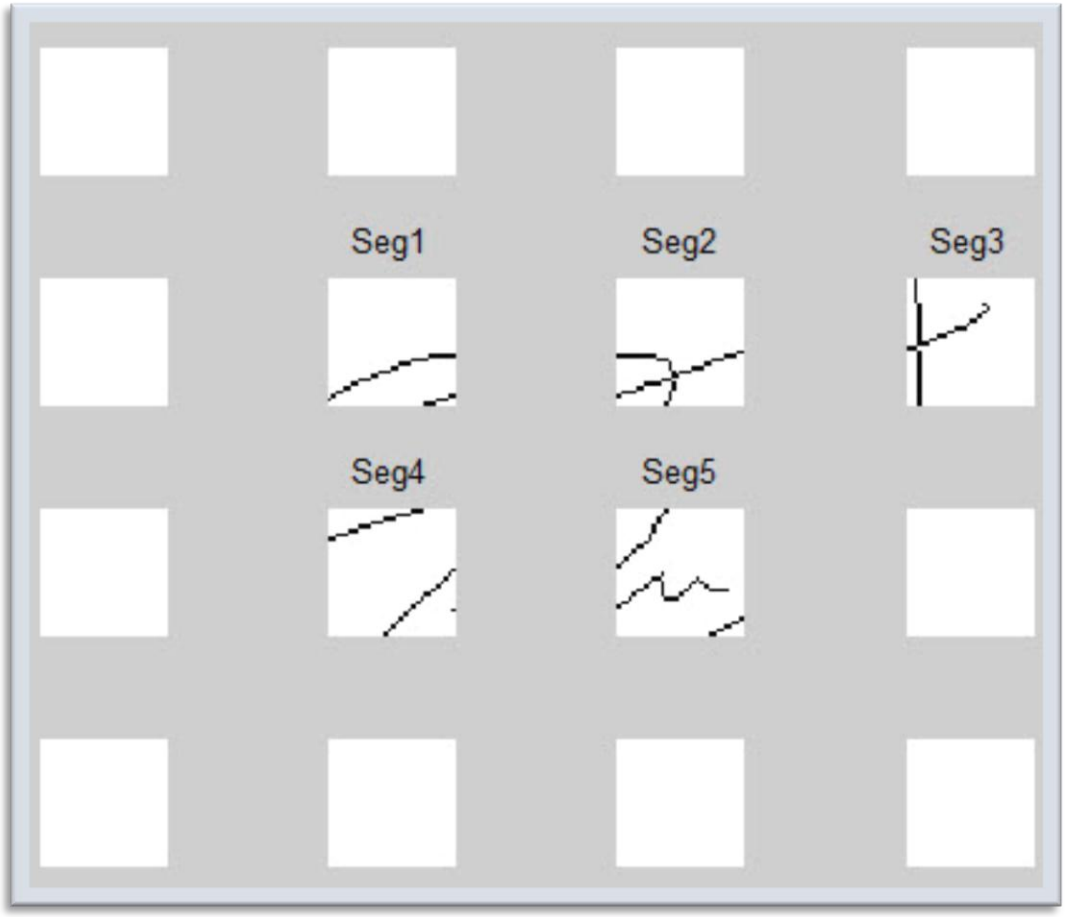


Figure II- 6: signature après normalisation.

II-3-2-2. L'approche en ligne (online)

Les systèmes online sont extrêmement précisés mais exigent la présence du signataire pendant l'acquisition des données de référence et le procédé de vérification limitant leur utilisation aux applications spécifiques .Considérons que la grande majorité de signatures manuscrites sont trouvées réellement dans les documents ou les chèques bancaire précédemment signés, les systèmes offline résolvent ces problèmes mais exigent une étape de prétraitement plus complexe ou plus de raffinage, produisant également d'une plus grande taille de base de données et un manque dans l'efficacité [3] .

La figure II-7 donne une représentation d'un système de vérification de signature online. Le module d'acquisition de données est responsable de capturer des données de signature pendant la session de signature. Le générateur de profile crée un profile, basé sur l'information

extraite à partir des signatures de référence de l'utilisateur, qui est alors stocké dans la base de données du système. Le mécanisme de vérification est responsable de la vérification d'une signature donnée de test, basée sur la similitude entre les signatures de test et les signatures de référence.

Une signature online peut être regardée en fonction du temps. Ceci facilite de dériver les caractéristiques de signature pour un signataire particulier. En raison du même fait, les systèmes de vérification de signature online sont plus fiables comparés aux systèmes de vérification de signature offline [4].

Dans un système online, les signatures sont présentées par des points de prélèvement, comme illustre la figure II-8. Les distances entre ces points ne sont pas égales, à cause de la variation de vitesse de signature avec le temps, qui est une caractéristique dynamique d'un signataire. Selon le matériel disponible utilisé, les caractéristiques dynamiques, telles que la pression au bout de stylo, l'accélération, et l'inclinaison de stylo, peuvent être capturées pendant la session de signature [4].

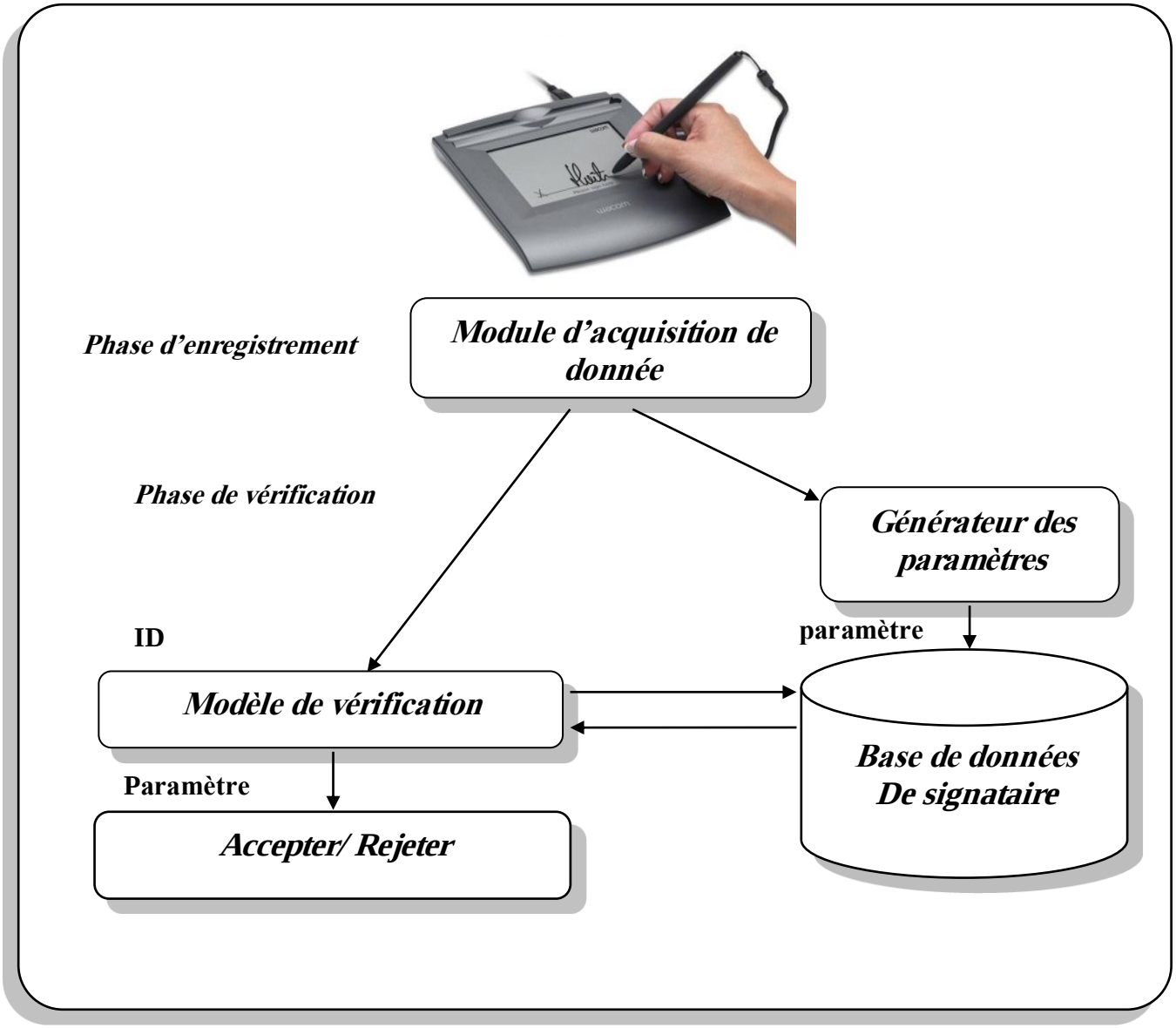
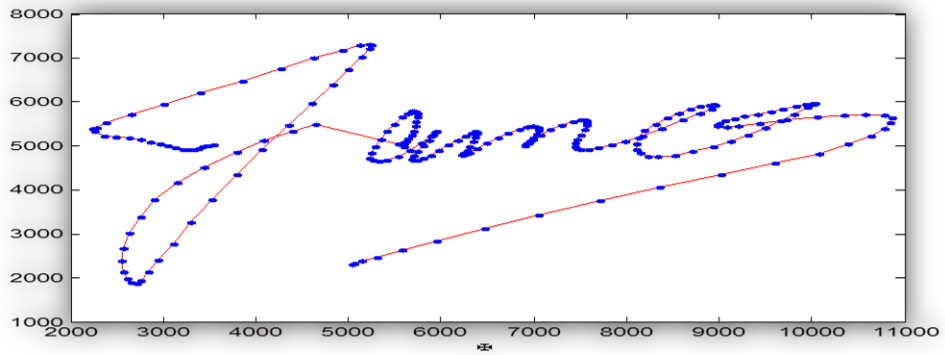


Figure II- 7: Représentation du système de vérification de signature online.



(La signature U40S6 de la base de données SVC 2004)

:

Figure II -8:Points de prélèvement d'exemple de la signature online [11].

Les données online de la base de données (SVC 2004) [11] sont les coordonnées X et Y, la durée de la signature T, les angles d'azimut et d'altitude (γ, φ) et la pression P au bout de stylo. Donc on peut calculer les autres paramètres onlines [12], [13]:

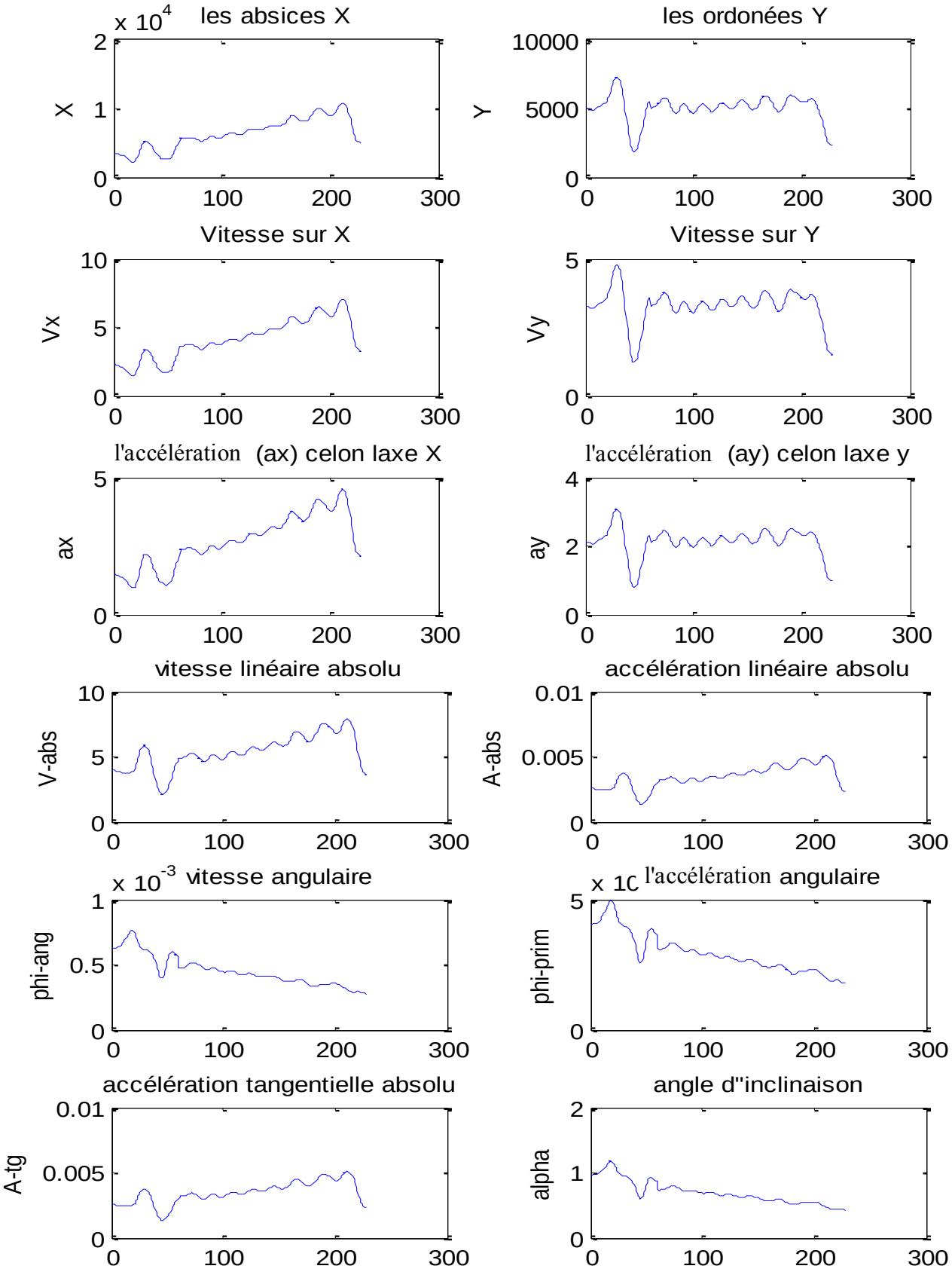
- la vitesse en direction X et Y :$V_X(t) = X'(t)$et$V_Y(t) = Y'(t)$ (2-1)
- la vitesse absolue : $V(t) = \sqrt{V_X(t)^2 + V_Y(t)^2}$ (2-2)
- l'accélération en direction X et Y :$a_X(t) = V'_X(t)$ et $a_Y(t) = V'_Y(t)$ (2-3)
- l'accélération absolue : $a(t) = \sqrt{a_X(t)^2 + a_Y(t)^2}$ (2-4)
- l'accélération tangentielle : $a_t(t) = |V(t)|'$ (2-5)
- l'angle alpha et ses cosinus et sinus :

$$\cos(\alpha(t)) = \frac{V_X(t)}{|V(t)|} \;;\; \sin(\alpha(t)) = \frac{V_Y(t)}{|V(t)|} \quad \text{et} \quad \alpha(t) = arctan\frac{V_Y(t)}{V_X(t)} \qquad (2\text{-}6)$$

- La vitesse angulaire:$\emptyset(t) = \alpha'(t)$ (2-7)
- le rayon : $r(t) = \frac{a_t(t)}{\emptyset'(t)}$ (2-8)
- Log rayon de courbure :ρ(t)= $\log\left(\frac{1}{c(t)}\right)$=$\log\left(\frac{V(t)}{\emptyset(t)}\right)$ (2-9)

où c(t) est la courbure de la trajectoire de position.

Les paramètres onlines de la signature donnés et calculés sont représentés sur la figure II-9. Remarquons que tous les paramètres sont représentés par rapport aux indices de points de prélèvement (échantillonnage), malgré que sont calculés en fonction du temps de ces points.


x 10^4
les absices X
X
les ordonées Y
Y
Vitesse sur X
Vx
Vitesse sur Y
Vy
l'accélération (ax) celon laxe X
ax
l'accélération (ay) celon laxe y
ay
vitesse linéaire absolu
V-abs
accélération linéaire absolu
A-abs
x 10^-3 vitesse angulaire
phi-ang
x 10 l'accélération angulaire
phi-prim
accélération tangentielle absolu
A-tg
angle d''inclinaison
alpha

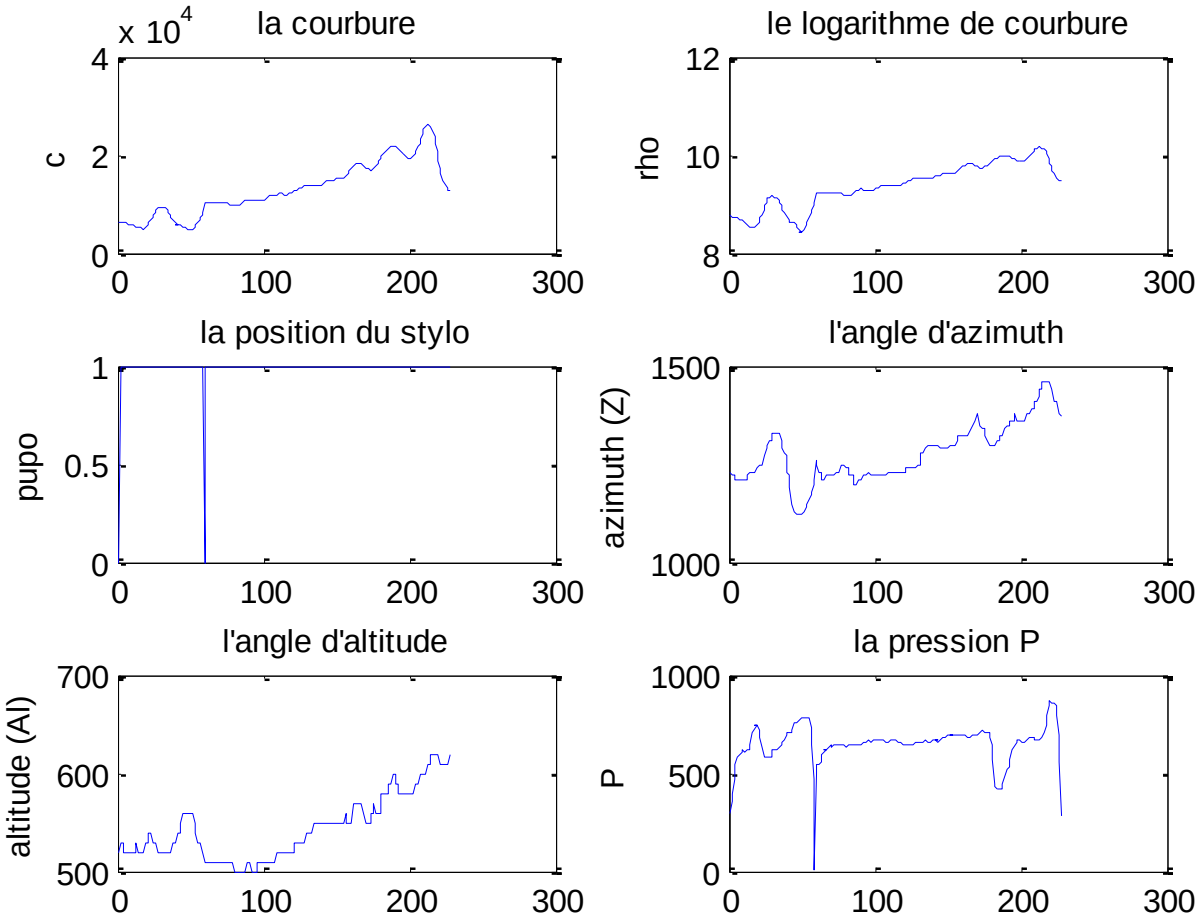


Figure II- 9: Exemple de différents paramètres d'une signature online [11].

- ***Acquisition des signatures***

Les signatures onlines sont généralement acquises en utilisant des outils sensibles à la pression [14]. Les stylos et les gants particulièrement conçus de main sont également utilisés à cette fin. L'objectif du système d'acquisition est de dépister et d'enregistrer les coordonnées spatiales pendant le mouvement du stylo en fonction du temps. Certaines sondes d'acquisition peuvent également obtenir d'autres paramètres tels que des valeurs d'inclinaison, de vitesse et de pression du stylo pendant la signature. Le mouvement du stylo peut également être dépisté en utilisant une caméra pour l'acquisition des signatures online [15], [16].

Le tableau II-1 [4] et la figure II-10 [17] nous donnent une vision sur un ensemble des appareils disponibles sur le marché pour l'acquisition de données des signatures online.

Une partie des appareils d'acquisition de données peut présenter le bruit et l'irrégularité aux données de signature. De même, l'utilisation de différents paramètres d'acquisition dans le même système peut présenter le changement de la balance et de l'orientation de la signature [4].

Figure II -10: Exemples des matériels de capture de signature online.

Marque Et Modèle	Surface Actif	Niveaux de Pression	Résolution
InterlinkePad-ink	***3"x2.20"***	***512***	***300dpi***
Wacom Graphire2	***3.65" x 5"***	***512***	***1016lpi***
AiptekHyperpen 6000U	***4.5"x6"***	***512***	***3048lpi***
DynalinkFreeDraw	***5"x3.75"***	***512***	***2540lpi***
Genius EasyPen	***4"x3"***	***_***	***2540lpi***
Genius WizardPen	***4"x3"***	***512***	***4064lpi***
Genius MousePen	***5.5"x4"***	***512***	***4064lpi***
CalCompDrawingBoard III	***12"x12"***	***256***	***2540lpi***
ParadiseGraphics Tablet	***5"x4"***	***512***	***2048dpi***
UC-LogicSuperPen 4030	***4"x3"***	***512***	***1000lpi***
UC-LogicSuperPen 8060	***8"x6"***	***1024***	***1000lpi***
Acedad Flair	***5"x3.75"***	***512***	***2540lpi***

Tableau II- 1: Appareils sensibles à la pression disponibles sur le marché.

- ***Prétraitement des données***

Il y a beaucoup de méthodes pour le prétraitement ; la plupart d'entre elles ont été discutée par Bourlard et Wellekens [18]. Le prétraitement est effectué avant l'extraction des paramètres afin d'améliorer la fiabilité et l'exactitude du processus d'extraction de paramètres. Pendant les opérations de prétraitement telle que la normalisation en ce qui concerne le placement, la taille et l'orientation des signatures sont exécutées pour réduire l'effet des variations de l'orientation, de la taille et des endroits spatiaux d'une signature. D'autres étapes de prétraitement peuvent inclure au sujet du prélèvement et de lisser des signatures [14].

- ***Extraction des paramètres***

Un grand nombre de paramètres sont disponibles pour la vérification de signature. Ces paramètres peuvent être largement classifiés comme locaux et globaux. Les paramètres globaux analysent toute une signature. Ces paramètres incluent la vitesse de signature, le nombre des points où le stylo se lève, la saccade moyenne, écarts type de la vitesse et des données d'accélération, la boîte de bondissement de signature, et de descripteurs de Fourier d'une signature. Indépendamment de ces paramètres, une grande variété de paramètres locaux sont également employées dans le système online de vérification de signature. Ces paramètres analysent une signature sur la base des points spécifiques de prélèvement le long de la trajectoire

de la signature. La vitesse de signature aux points de courbure élevés (appelés les points critiques) est un exemple des paramètres locaux [14].

II-3-3. Comparaison entre les approches online et offline

Dans un système hors ligne, la signature est effectuée sur un support papier puis scannée. La signature est donc assimilée à une image en niveaux de gris. C'est le cas notamment pour les systèmes de vérification de chèques.

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

II-4. *Conclusion*

Dans ce chapitre, nous avons décrit les deux approches les plus connues dans le domaine de la vérification des signatures manuscrites (en-ligne, hors ligne) :

La vérification des signatures manuscrites hors-ligne : l'écriture de l'utilisateur est acquise par un scanner. L'entrée de ces systèmes est une image. Un système « hors ligne » traite la signature à partir d'une image, tel que l'émargement sur un chèque ou sur un document.

La vérification des signatures manuscrites en-ligne : l'utilisateur écrit sur une table spéciale, le système va reconnaître l'écriture et envoyer le résultat à l'ordinateur.

Dans le cas d'un système « en ligne » la signature est acquise directement sur une tablette ou un stylo électronique, on peut donc relever des caractéristiques dynamiques telles que le temps de signature, la pression ou l'inclinaison du stylo. Pour un système de vérification en ligne l'interface d'acquisition influe sur la conception du système, ainsi une tablette simple ne peut servir à des méthodes de vérifications nécessitant des paramètres tel que la pression ou l'inclinaison du stylo.

Aussi nous parlons sur les étapes de vérification de deux approches, qui sont l'acquisition, le prétraitement et l'identification et nous avons vu que le signe sur papier avec un stylo plus couramment utilisés pour les usagers, moins couteuse par rapport à l'approche online et pour cela nous avons choisi à la traitée.

Chapitre III

Approche de vérification

III.1. *Introduction*:

Les modèles de Markov cachés (Hidden Markov Models ou HMM) ont été introduits par Baum et ses collaborateurs dans les années 1960-70 [1]. Ces modèles sont fortement apparentés aux processus aléatoires. Les modèles de Markov connaissent actuellement un essor important en reconnaissance des formes grâce à leur capacité d'intégration du contexte et d'absorption du bruit [2], [3], [4], [5]. Dans ces modèles, les formes sont décrites par une séquence de primitives qui seront observées dans les états du modèle.

La probabilité d'émission de la forme par le modèle est calculée en maximisant, sur l'ensemble des chemins d'états, la probabilité d'observation des segments pondérée par les probabilités de transitions entre états. Ce calcul se fait généralement par maximum de vraisemblance. Le calcul de la vraisemblance de la forme par rapport au modèle est fondé sur la règle de Bayes qui inclut la probabilité à priori du modèle.

Depuis 1975, les HMM sont utilisés dans des nombreuses applications, principalement dans le domaine de la parole. Ces applications ne se contentent pas de s'appuyer sur la théorie des Modèles de Markov Cachés, mais développent plusieurs extensions théoriques dans le but d'améliorer les modèles. C'est ce qui en a fait leur succès.

Les MMCs sont utilisés dans beaucoup d'applications. Les domaines les plus connus sont des technologies bioinformatiques et des technologies d'Informatique Linguistique. D'autres technologies qui utilisent les MMCs sont la parole, traitement des signaux, etc. Quelques applications de ces techniques:

- Prédiction des régions de protéine-codage dans des séquences de génome
- Prédiction des éléments secondaires de structure des séquences primaires de protéine
- Reconnaissance de la parole
- Reconnaissance d'écriture
- Traduction automatique
- Vérification de signature

III.2. *Présentation*

Un HMM est représenté par :

1) **N**, le nombre d'états du modèle. Les états d'un HMM sont toujours cachés. Ils peuvent être interconnectés (chaque état peut être atteint de n'importe quel autre état) ou non. Nous dénotons les états individuels $S= \{S_1, S_2, \ldots\ldots, S_N\}$ et l'état au temps t est q_t.

2) ***M***, le nombre des observations. Nous dénotons les observations individuelles ***V= {v1, v2, …….v_M}.***

3) La matrice des probabilités de transition des états ***A={a_{ij}} où a_{ij} = P[qt+1 = Sj | qt = Si], 1 ≤ i, j ≤ N.*** Si les états sont interconnectés, tous les ***a_{ij}> 0***, si non, il y a quelques ***a_{ij}= 0*** (c'est-à-dire l'état ***S_j*** ne peut pas être atteint de l'état ***S_i***).

4) La matrice des probabilités des observations ***B = {b_j(k)}* où *b_j(k) = P[v_k au t | q_t = S_j], 1 ≤ j ≤ N, 1 ≤ k ≤ M.***

5) Le vecteur des probabilités initiales ***π = {$π_i$} où $π_i$ = P [q_1=S_i], 1 ≤ i ≤ N.*** En bref, un HMM est dénoté par ***λ = (A, B, π).***

III.3. *Types de distribution des probabilités des symboles*

On distingue différentes classes de HMM en fonction du type de distribution des probabilités des symboles. Deux grandes classes sont remarquables : les HMM discrètes et les HMM continues. Les HMM discrètes sont plus faciles à implémenter. Ils ont moins de paramètres ré-estimer mais sont moins précises que les HMM continues. Les HMM discrètes font moins d'hypothèses sur la nature des observations, mais demandent un ensemble d'apprentissage plus important.

III.4. *Quelques architectures de chaînes de Markov cachées*

Il existe deux types principaux de modèles de Markov cachés en fonction des contraintes imposées sur les transitions entre états et sur les probabilités initiales [6]. Un modèle est sans contraintes, toutes les transitions d'un état vers un autre sont possibles, dite "ergodique". L'autre modèle contient des contraintes sur des transitions, c'est-à-dire que depuis un état donné les seules transitions possibles sont dirigées vers ce même état ou vers un état jamais atteint auparavant, dite "**gauche-droite**" [7].

Certaines architectures possèdent une certaine régularité dans leurs transitions. On définit par exemple que chaque état ne peut atteindre que deux états au maximum (hormis lui-même). Ce nombre est appelé le pas de transition. Parmi ces modèles, remarquons celui de Bakis [7], qui est définit comme une chaîne de Markov cachée de type "gauche-droite" avec un pas de valeur ***Δ=2*** et une matrice de transition défini par [8]:

$$a_{ij} = 0 \quad si \quad j<i \quad et \quad a_{ij} = 0 \quad si \quad j>i+\Delta \qquad (3\text{-}21)$$

C'est ce modèle que nous avons utilisé dans la vérification de notre système.

III.5. *Problèmes principaux*

Il y a trois problèmes principaux dans l'utilisation d'un HMM. Ces problèmes se situent au niveau de :

- **Evaluation**: Etant donné le HMM $\lambda = (A, B, \pi)$ et une séquence d'observations $O= \{o_1, o_2, ..., o_T\}$, comment calculer la probabilité pour que O soit générée par λ (la vraisemblance $P(O \mid \lambda)$). Il existe plusieurs méthodes qui calculent cette probabilité.Parmi eux, on trouve évaluation directe et Forward-Backward [7] (Annexe A-B).
- **Décodage (la détermination du chemin optimal d'états)**: Etant donné le HMM $\lambda = (A, B, \pi)$ et les observations séquentielles $O= \{o_1, o_2, ..., o_T\}$, comment calculer la séquence d'états $Q = q_1 q_2 \ldots q_T$ la plus probable. Ce problème est résolu par l'algorithme de Viterbi [7]. (Annexe C)
- **Apprentissage**: Etant donné les observations séquentielles O, comment déterminer les paramètres du HMM $\lambda = (A, B, \pi)$ pour que $P(O \mid \lambda)$ soit maximisé sur les observations O de la base d'apprentissage. Le problème de l'optimisation d'apprentissage peut être plus difficile en comparant avec les deux autres. Ce problème concerne l'apprentissage supervisé du HMM dont l'architecture (nombre d'états et transitions) est connue. Ce problème est résolu par l'algorithme EM (Expectation-Maximization), connu dans le domaine des HMM sous le nom d'algorithme de Baum-Welsh (BW) [7] (Annexe D).

Comme nous avons vu dans la partie (III-5) d'extraction des paramètres, le vecteur du paramètre est de dimension (4), c'est-à-dire que chaque symbole d'observation de HMM est caractérisé par quatre paramètres, et pour cela on a besoin d'un HMM multi-paramètres (multi-variables).

III.6. *Vecteur multi-paramètres (ou vecteur collecte)*

Le regroupement est le fait de grouper en ensemble les différents types des caractéristiques stockées dans un modèle de vecteur. Au lieu de recueillir tous les paramètres dans un HMM, " la méthode de collecte " construit un HMM par un groupe de paramètres. L'entrée X_t de dimension d est maintenant décrite comme groupe de vecteur de R caractéristiques avec la somme de la dimension pour chaque caractéristique $d(r)$ égal à d. Le paramètre p du vecteur dimensionnel X_t peut être un ensemble de R paramètres P_r du vecteur dimensionnel X_t^r lié ensemble, cela est présenté $X_t=\{x_t^1, x_t^2, \ldots, x_t^r, \ldots, x_t^R\}$,

L'algorithme HMM verra tous les paramètres comme vecteur avec juste un paramètre de dimension ***p***. Pour prendre en compte de chaque paramètre est isolé seul d'une certaine manière, nous proposons de modifier le calcul de la probabilité de vecteur d'observation $b_j(O_t)$.Les autres formules sont inchangées [8]. Pour les calculs voir l'annexe E.

III.7. *Extraction des paramètres*

N'importe quelle image qui peut être identifiée et classifiée possède un certain nombre de propriétés ou de paramètres discriminatoires. L'extraction de paramètres représente le processus d'extraction de ces propriétés discriminatoires à partir d'une image. L'extraction de paramètres est compliquée par le fait que les paramètres qui sont les plus importants pour une image ne sont pas nécessairement facilement mesurables.

Dans le cas des signatures, la littérature disponible semblent indiquer que les paramètres discriminatoires les plus importants sont l'ordre des strockes, la direction des strockes, l'inter-corrélation entre les strockes qui ne sont pas facilement mesurables par les paramètres de balayage et n'exigent pas l'utilisation de l'algorithme spécialisé de développement [9].

L'extraction des paramètres est réalisée d'une manière entièrement automatique. Elle consiste à faire une extraction des caractéristiques statiques de la signature pour chaque composante du tracé de la signature (strockes).

Les paramètres sont classés en deux catégories :

- ***paramètres statistiques*** *:* paramètres comme des moyens, des moments, des rapports de corrélation, etc.…
- ***paramètres morphologiques*** *:* les paramètres comme la forme, la taille, etc.…

Tout en choisissant des paramètres, les facteurs suivants peuvent être considérés :

a) Les paramètres doivent être instructifs et la dimensionnalité du vecteur contenant seulement les paramètres efficaces.

b) Les paramètres doivent être invariants à la rotation et à la translation sur la gamme des échantillons.

Dans notre modèle, les paramètres choisis pour chaque signature sont basés sur sa carte de pixels (valeur du pixel et sa position dans l'image). Il y a plusieurs types de paramètres : le plus simple concerne la valeur du pixel (noir ou blanc). Autre type de paramètres porte sur la position du pixel [10]. Nous avons utilisé quatre paramètres pour chaque stroke, qui sont dans l'ordre :

- La première composante est la valeur du pixel dans les strockes :

$$O_{xy}^{1} = pixel(x, y) \tag{3-11}$$

Donc, elle peut être 0 ou 1.

- La deuxième composante est calculée à partir des valeurs pondérées des trois pixels adjacents sur la même ligne dans chaque strocke:

$$O_{xy}^{2} = 4 \times pixel(x-1, y) + 2 \times pixel(x, y) + pixel(x+1, y) \tag{3-12}$$

Ainsi, une telle valeur peut s'étendre de 0 à 7

- La troisième composante est l'amplitude du gradient de chaque pixel. Cette dernière composante définie deux dérivées selon x et selon y suivant les deux équations (3-13) et (3-14) :

$$d_x = pixel(x+1, y) - pixel(x, y) \tag{3-13}$$

$$d_y = pixel(x, y+1) - pixel(x, y) \tag{3-14}$$

Donc nous définissons l'amplitude par la formule (3-15):

$$O_{xy}^{3} = \sqrt{d_x^2 + d_y^2} \tag{3-15}$$

- La quatrième composante est la distance relative entre le pixel et le centre de gravité par rapport à l'origine de repère de l'image du stroke. Au début, nous calculons le centre de gravité de chaque stroke de l'image de la signature [11] :

$$G_x = \frac{\sum_{y=0}^{M-1}\sum_{x=0}^{N-1} x.f(x,y)}{\sum_{y=0}^{M-1}\sum_{x=0}^{N-1} f(x,y)} \tag{3-16}$$

$$G_y = \frac{\sum_{y=0}^{M-1}\sum_{x=0}^{N-1} y.f(x,y)}{\sum_{y=0}^{M-1}\sum_{x=0}^{N-1} f(x,y)} \tag{3-17}$$

Où x et y sont les coordonnées du pixel dans le stroke, N et M sont les nombres des pixels du stroke sur X et Y successivement et $f(x, y)$=1 si le point (x,y) appartient à la courbe du stroke, 0 sinon. Alors la distance entre le centre de gravité et le point d'origine du repère est définie comme suit:

$$D_G = \sqrt{G_x^2 + G_y^2} \tag{3-18}$$

Puisque les coordonnées d'origine sont $(0,0)$, la distance entre un point (x,y) et l'origine est :

$$D_{x,y} = \sqrt{x^2 + y^2} \tag{3-19}$$

Donc le rapport entre $D_{x,y}$ et D_G est :

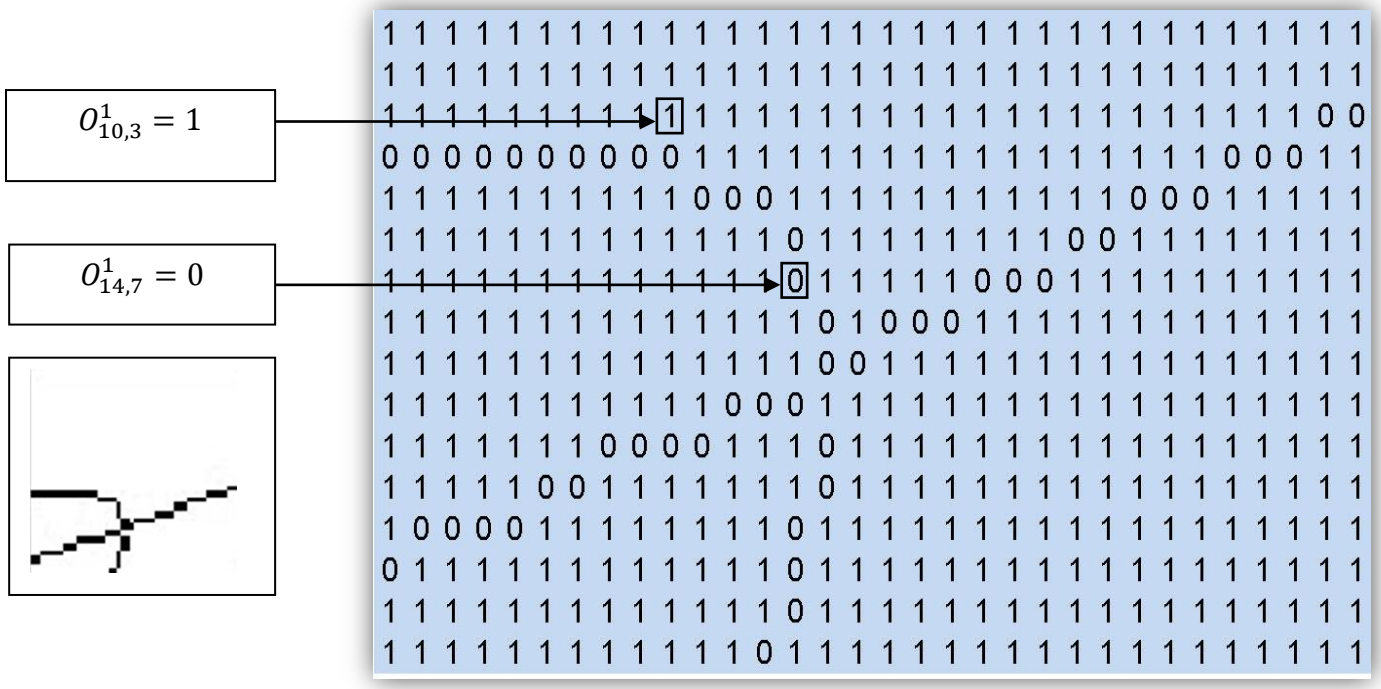
$$O_{xy}^{4} = \frac{D_{x,y}}{D_G} \tag{3-20}$$

Pour illustrer la manière d'extraction des paramètres, nous allons prendre le cas des strokes de la signature de la figure III-1.

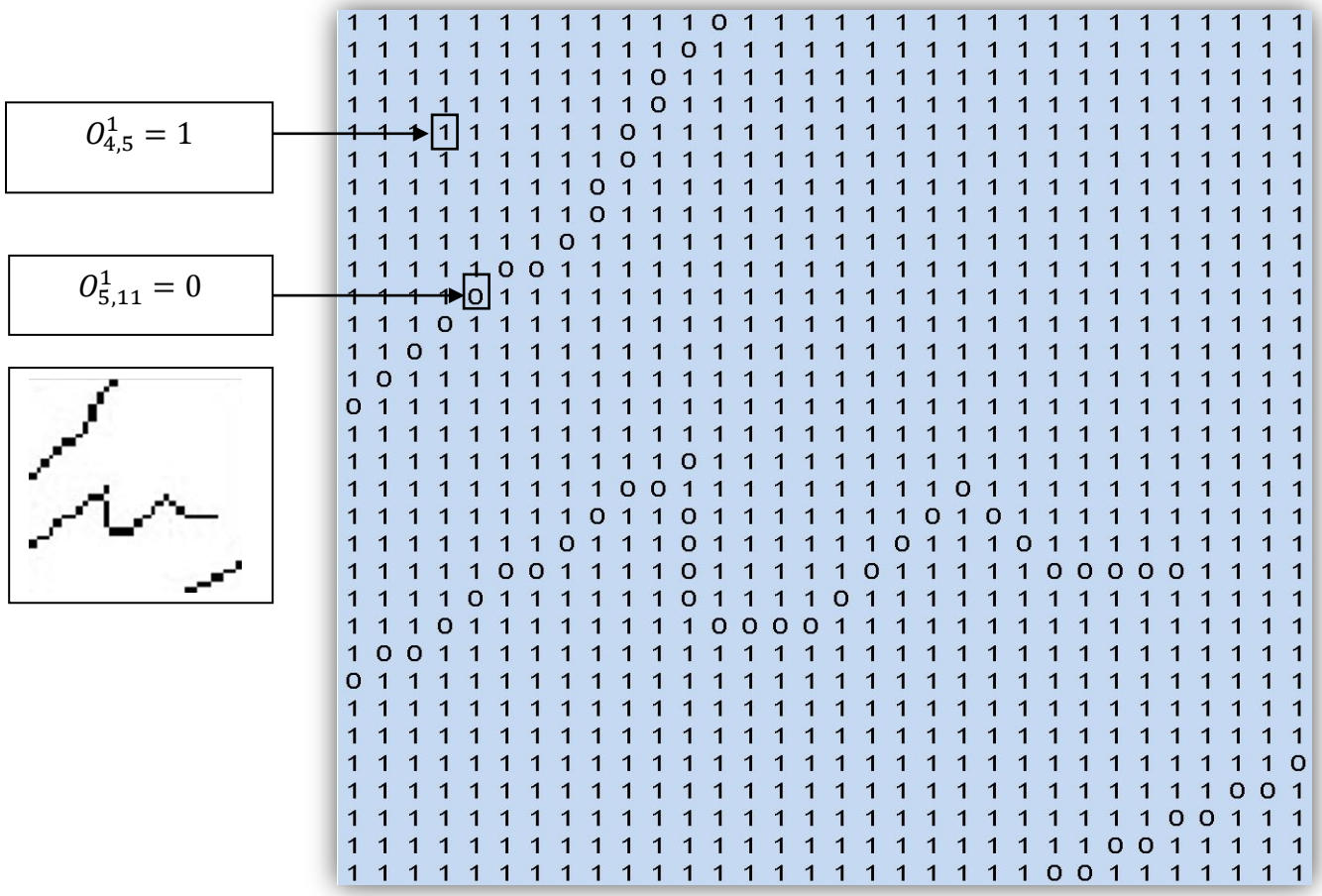
Figure III- 1 : Différentes strokes d'une signature

Dans ce qui suit, nous choisissons le septième et l'onzième strokes, pour présenter ces quatre paramètres extraits à partir des équations mathématiques précédentes.

La figure (III-2(a) et III-2(b)) présente la première composante qui est la valeur des pixels du septième et onzième stroke successivement.



(a) La première composante du septième stroke

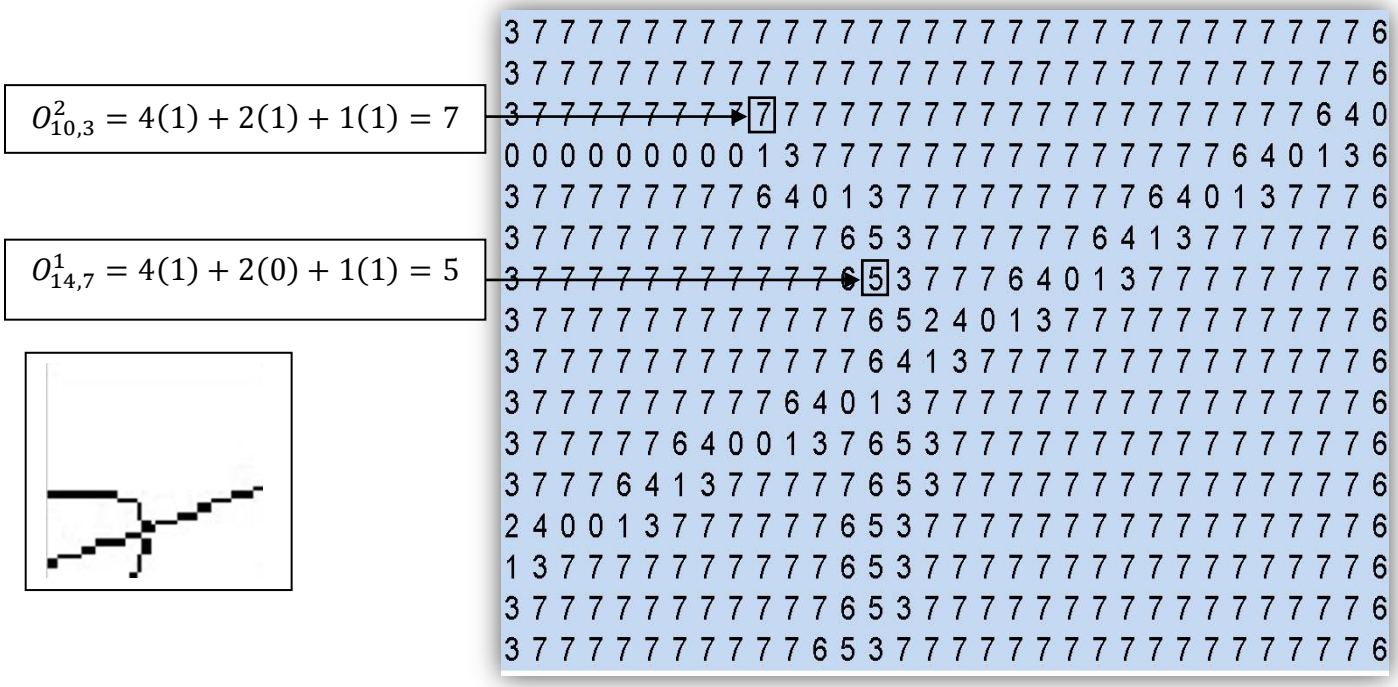


(b) La première composante du onzième stroke

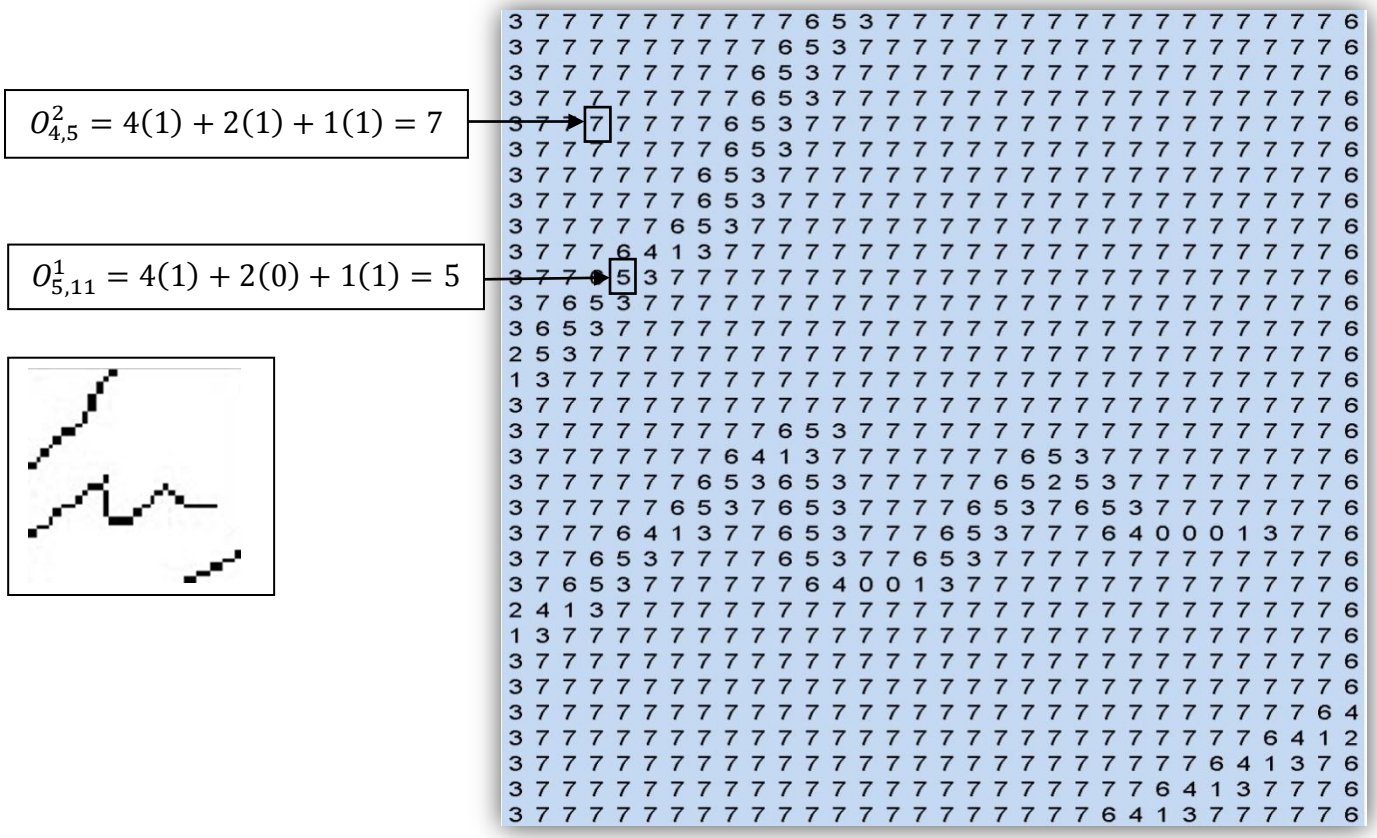
Figure III -2: : Calcul du premier paramètre

Une première vue sur les plans des strokes 7 et 11 sur la figure III-12(a et b successivement), montre qu'on peut distinguer clairement les traits des strokes par leurs valeurs nulles dans les plans représentatifs.

Le deuxième paramètre, qui est la pondération des trois pixels adjacents sur la même ligne, est présenté dans la figure III-3 (a et b) pour les deux stroke 7 et 11 successivement. La représentation des pixels des strokes 7 et 11 est clair avec ses adjacents lorsqu'on concentre bien sur les plans représentatifs de deuxième composante sur la figure III-3 (a et b).



(a) La deuxième composante du septième stroke



(b) La deuxième composante du onzième stroke

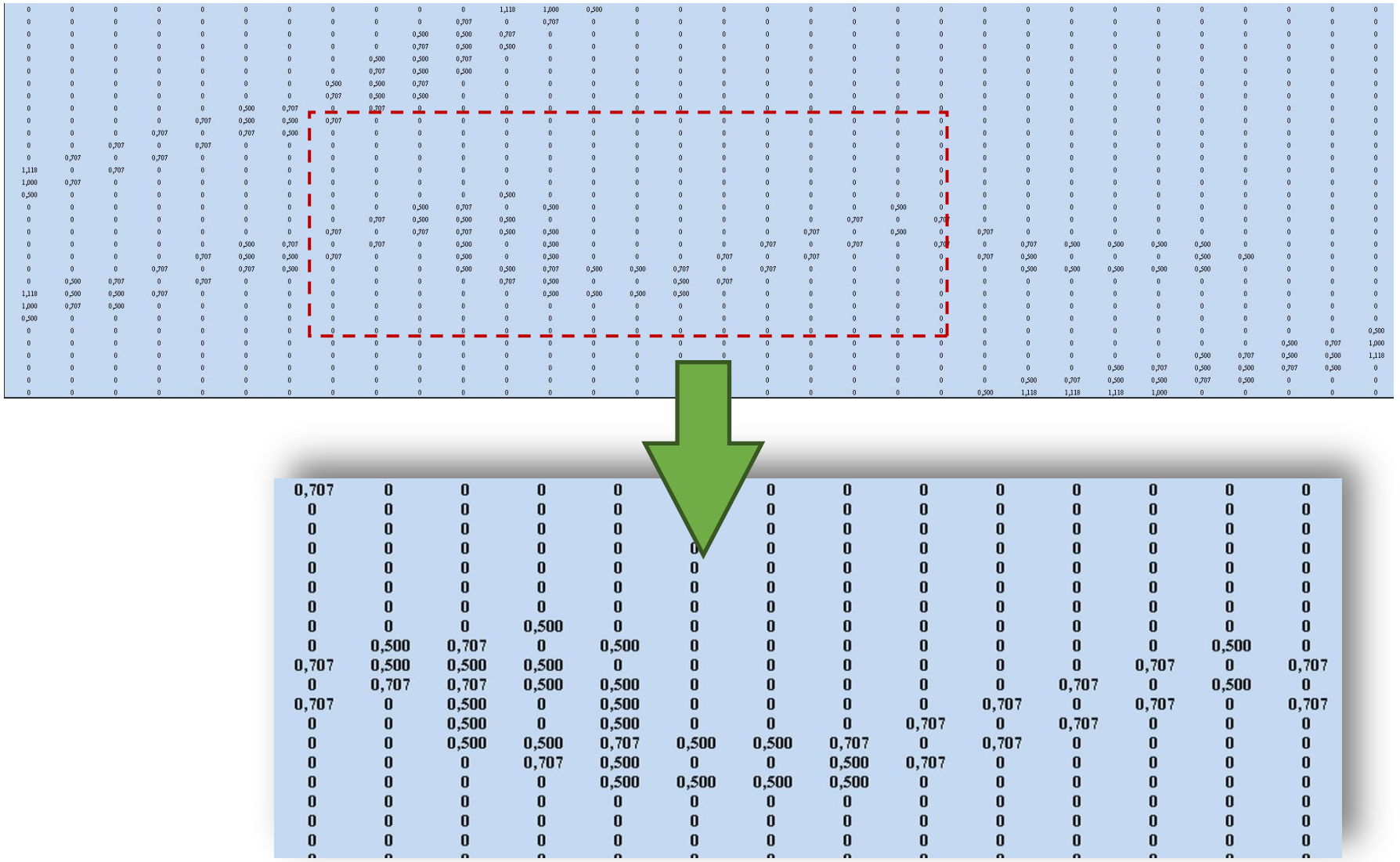
Figure III -3: Calcul du deuxième paramètre

La figure III-4(a) et (b) présente le troisième paramètre pour le septième et l'onzième stroke successivement, qui est l'amplitude du gradient des pixels de l'image de stroke, les pixels de stroke ne sont pas déterminés mais la forme générale des strokes est remarquable avec ses voisinages comme montre les plans de valeurs des pixels dans la figure III-4 (a) et (b).

La distance relative d'un pixel par rapport au centre de gravité de l'image du stroke, qui représente le quatrième paramètre choisi, est représentée dans la figure III-5 (a) et (b). Les pixels des strokes 7 et 11 ne sont pas totalement clairs sur les plans des points qui présentent les images des strokes.

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0,500	0,707	0,500	0,500	0	0	0	0	0	0	0	0	0	0
0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,500	0,707	0,500	0	0,500	0,707	0	0	0	0	0	0	0	0	0,500
0	0	0	0	0	0	0	0	0	0	0,500	0,500	0,707	0,500	0,500	0	0	0	0	0,500	0,500	0,707	0,500
0	0	0	0	0	0	0	0	0	0	0	0	0,500	0,500	0,707	0	0,500	0,500	0,707	0,500	0	0,500	0,707
0	0	0	0	0	0	0	0	0	0	0	0	0	0,707	0,500	0,500	0,500	0	0,500	0,707	0,500	0,500	0
0	0	0	0	0	0	0	0	0	0	0	0,500	0,500	0,707	0,707	0,500	0,707	0,500	0,500	0	0	0	0
0	0	0	0	0	0	0	0,500	0,500	0,500	0,707	0,500	0	0,500	0,500	0,500	0	0	0	0	0	0	0
0	0	0	0	0	0,500	0,707	0,500	0	0	0,500	0,707	0,500	0,707	0,500	0,500	0	0	0	0	0	0	0
0	0,500	0,500	0,500	0,707	0,500	0,500	0,707	0,500	0,500	0,500	0	0	0,707	0,500	0,500	0	0	0	0	0	0	0
1,118	0,500	0	0	0,500	0,707	0,500	0	0	0	0	0	0,500	0,500	0,707	0	0	0	0	0	0	0	0
1,000	0,707	0,500	0,500	0,500	0	0	0	0	0	0	0	0,500	0	0,500	0	0	0	0	0	0	0	0
0,500	0	0	0	0	0	0	0	0	0	0	0	0,707	0,500	0,500	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0	0,500	1,000	1,118	0	0	0	0	0	0	0	0	0

(a) La troisième composante du septième stroke

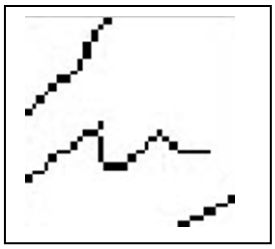


(b) La troisième composante du onzième stroke

Figure III -4: Présentation du troisième paramètre

0,05114	0,08086	0,11435	0,14910	0,18439	0,21997	0,25571
0,08086	0,10228	0,13038	0,16172	0,19474	0,22871	0,26326
0,11435	0,13038	0,15342	0,18081	0,21086	0,24258	0,27540
0,14910	0,16172	0,18081	0,20456	0,23155	0,26077	0,29155
0,18439	0,19474	0,21086	0,23155	0,25571	0,28244	0,31108
0,21997	0,22871	0,24258	0,26077	0,28244	0,30685	0,33340
0,25571	0,26326	0,27540	0,29155	0,31108	0,33340	0,35799
0,29155	0,29820	0,30897	0,32344	0,34115	0,36162	0,38441
0,32746	0,33340	0,34306	0,35616	0,37231	0,39115	0,41231
0,36343	0,36878	0,37754	0,38948	0,40431	0,42172	0,44142
0,39942	0,40431	0,41231	0,42327	0,43695	0,45311	0,47150
0,43545	0,43993	0,44730	0,45742	0,47011	0,48517	0,50238
0,47150	0,47564	0,48246	0,49186	0,50368	0,51776	0,53393
0,50756	0,51141	0,51776	0,52653	0,53759	0,55081	0,56603
0,54364	0,54723	0,55318	0,56139	0,57177	0,58422	0,59859

(a) La quatrième composante du septième stroke



0,059538	0,094138	0,133131	0,173582	0,214668	0,256083	0,297691
0,094138	0,119076	0,151793	0,188276	0,226714	0,266263	0,306491
0,133131	0,151793	0,178614	0,210499	0,245482	0,282414	0,320623
0,173582	0,188276	0,210499	0,238153	0,269570	0,303586	0,339420
0,214668	0,226714	0,245482	0,269570	0,297691	0,328810	0,362156
0,256083	0,266263	0,282414	0,303586	0,328810	0,357229	0,388141
0,297691	0,306491	0,320623	0,339420	0,362156	0,388141	0,416767
0,339420	0,347164	0,359701	0,376552	0,397169	0,420998	0,447527
0,381230	0,388141	0,399394	0,414635	0,433444	0,455379	0,480012
0,423098	0,429336	0,439535	0,453429	0,470690	0,490964	0,513894
0,465008	0,470690	0,480012	0,492766	0,508694	0,527509	0,548914
0,506949	0,512166	0,520746	0,532525	0,547298	0,564828	0,584869
0,548914	0,553737	0,561682	0,572619	0,586383	0,602778	0,621596
0,590899	0,595381	0,602778	0,612983	0,625859	0,641245	0,658966
0,632899	0,637086	0,644003	0,653565	0,665657	0,680143	0,696876
0,674911	0,678839	0,685335	0,694328	0,705722	0,719402	0,735242
0,716934	0,720633	0,726756	0,735242	0,746011	0,758965	0,773996
0,758965	0,762460	0,768250	0,776282	0,786490	0,798788	0,813083
0,801004	0,804316	0,809806	0,817431	0,827130	0,838833	0,852456
0,843048	0,846196	0,851416	0,858671	0,867910	0,879070	0,892079

(b) La quatrième composante du onzième stroke

Figure III -5: Présentation du quatrième paramètre

III.8. *Conclusion*

Dans ce chapitre, nous avons vu l'algorithme de reconnaissance choisir pour concevoir un système d'identification et de vérification des données. Dans cette approche, nous avons choisi les chaînes de Markov cachées (HMM).

Après le choix des chaînes de Markov cachées (HMM), il reste seulement l'extraction des paramètres des strokes qui a été réalisée d'une manière entièrement automatique. Elle consiste à faire une extraction des caractéristiques statiques de la signature pour chaque composante du tracé de la signature (strokes). Dans cette partie, nous avons discuté les problèmes liés à l'extraction des paramètres. Ces problèmes concernent principalement le choix des paramètres qui doivent être très représentatifs de l'ensemble des formes à prendre en compte. Ce choix est important car il conditionne toute la méthodologie mise en œuvre pour la vérification.

A cette fin, nous avons présenté les paramètres d'un HMM, les principaux problèmes dans le calcul du HMM, et donné la méthode de calcul multi-variables, qui nous avons utilisé.

Dans le chapitre suivant, nous présenterons les résultats de test de notre approche.

Chapitre IV

Résultats, Analyses et Discussions

IV-1. Introduction

L'extraction des paramètres des segments est réalisée d'une manière entièrement automatique. Elle consiste à faire une extraction des caractéristiques statiques de la signature pour chaque stroke de la signature.

Dans ce chapitre, à la lumière des résultats présentés et l'algorithme discuté (HMM) dans le chapitre III, nous allons faire les tests de vérification et d'identification de la base de données utilisée dans cette étude.

IV-2. Test en mode vérification

Dans cette étude, nous avons calculé le taux de reconnaissance et tracé les courbes des grandeurs : FAR (False Acceptance Rate) et du FRR (False Rejection Rate) pour les quatre paramètres extraites.

IV-3. Les paramètres d'entrée:

On prend tous les paramètres des segments pour chaque signature dans une seule matrice de quatre colonnes (quatre paramètres). Puis on détermine le nombre de signatures d'apprentissage pour chaque personne (signataire) et fait toutes les combinaisons possible entre les paramètres pour déterminer le meilleur taux de reconnaissance, les résultats trouvés sont présentés dans le tableau IV-1.

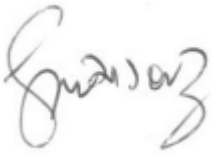
 **P5s1**	 **P6s1**
 **P7s1**	 **P8s1**

Figure IV- 1: Exemple des premières signatures de 5ème personne jusqu'à 8éme personne.

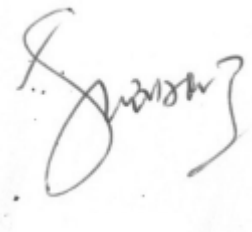
 **P5s9**	 **P6s9**
 **P7s9**	 **P8s9**

Figure IV- 2: Exemple des neuvièmes signatures de 5ème personne jusqu'à 8éme personne.

1er Person jusqu'à 4éme Apprentissage: 3 Test: 2						
Arrangement des paramètres d'entrée				**Taux de reconnaissance par groupe**		
entrée 01	entrée 02	entrée 03	entrée 04	groupe 01	groupe 02	groupe 01 et 02
4	3	2	1	50%	25%	50%
4	3	1	2	25%	25%	25%
4	2	3	1	25%	25%	0%
4	2	1	3	25%	50%	50%
4	1	2	3	25%	25%	25%
4	1	3	2	50%	50%	50%
3	4	2	1	25%	25%	25%
3	4	1	2	25%	25%	50%
3	2	4	1	50%	25%	25%
3	2	1	4	50%	25%	25%
3	1	2	4	50%	25%	25%
3	1	4	2	25%	50%	25%
2	3	4	1	50%	25%	25%
2	3	1	4	50%	25%	25%
2	4	3	1	25%	50%	50%
2	4	1	3	25%	25%	25%
2	1	4	3	50%	50%	25%
2	1	3	4	50%	50%	50%
1	3	2	4	25%	25%	75%
1	3	4	2	25%	25%	25%
1	**2**	**3**	**4**	**50%**	**50%**	**75%**
1	2	4	3	25%	25%	50%
1	4	2	3	25%	50%	50%
1	4	3	2	25%	50%	50%

Tableau IV- 1: choix de bon arrangement des paramètres d'entrées (24 cas)

Pour déterminer le bon arrangement des paramètres d'entrées on prend seulement quatre personnes (signataires) de la base de données pour la vérification et choisir trois signatures d'apprentissage pour chaque personne. On répète la vérification Vingt-quatre fois (toutes les combinaisons d'arrangement possible des quatre paramètres). On divise les paramètres d'entrée en deux groupe chaque groupe contient deux différentes paramètres. Après les tests de vérification on choisit l'arrangement des paramètres qui nous donne le bon taux de reconnaissance. Dans notre cas, nous avons sélectionné l'arrangement des paramètres [1 2 3 4] voir le tableau IV-1. La deuxième étape est de vérifié ces résultats en augmentant la

taille de la base à tester et le nombre des signatures d'apprentissage, le tableau IV-2 montre les résultats trouvés.

- **Première vérification:**

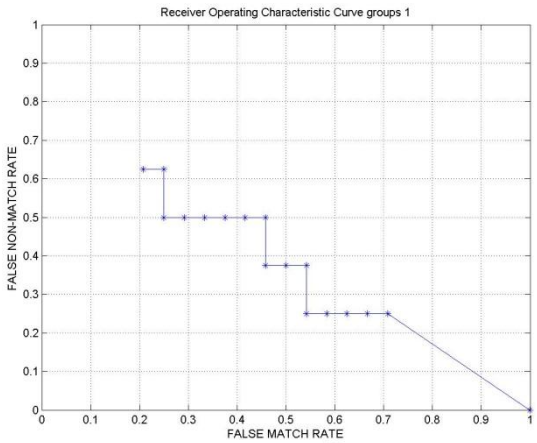
	1er Person jusqu'à 4éme	1er Person jusqu'à 10éme	1er Person jusqu'à 20éme
Apprentissage:6 Test:2	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 10 % GROUPE 2: 15 % GROUPE 1 2: 10 %	GROUPE 1: 5 % GROUPE 2: 10 % GROUPE 1 2: 10 %
Apprentissage:7 Test:2	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 20 % GROUPE 2: 10 % GROUPE 1 2: 20 %	GROUPE 1: 17.5 % GROUPE 2: 10 % GROUPE 1 2: 10 %
Apprentissage:8 Test:2	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 10 % GROUPE 2: 10 % GROUPE 1 2: 10 %	GROUPE 1: 7.5 % GROUPE 2: 5 % GROUPE 1 2: 5 %

Tableau IV- 2: taux de reconnaissance pour quatre, dix et vingt signataires.

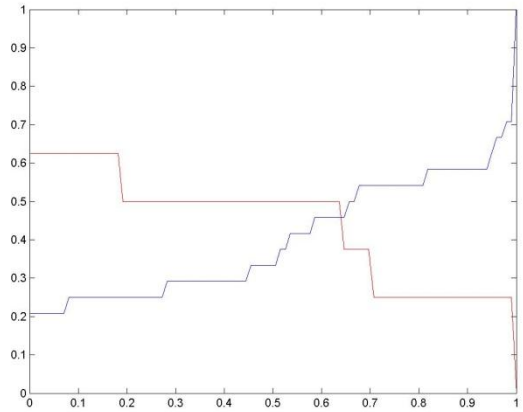
Nous remarquons que le taux de reconnaissance est faible pour les trois cas, il y a plusieurs raisons parmi eux:

- Le choix des paramétrés d'entrée et leurs arrangement.
- Le base de donné crée est très courte pour chaque signataire (09 signatures), et aussi la base d'apprentissage est insuffisante.
- La sérieuse et le respect des agents signataires (raté les rendez-vous de prendre de signature, signé différentes signatures à chaque rendez-vous de prendre les signatures).

1er Person jusqu'à 4éme
Apprentissage: 6 Test: 2



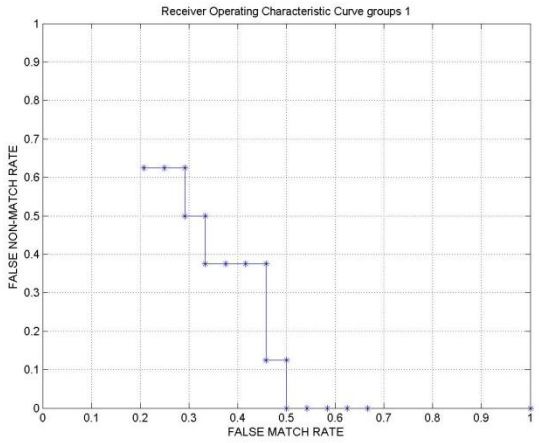
(b)

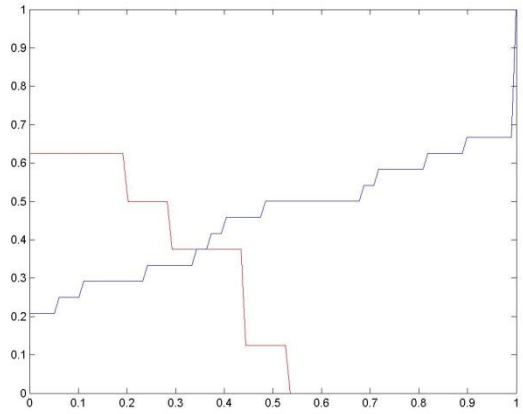


(a)

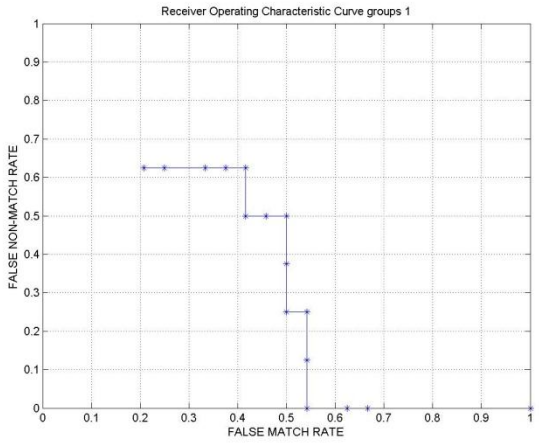
- La première courbe (a) c'est le taux d'egale erreur, donne un point sur lequel le taux de fausses acceptations est égal au taux de faux rejets.
- La deuxième courbe (b) c'est le taux de fausses acceptations en fonction de taux de faux rejets.

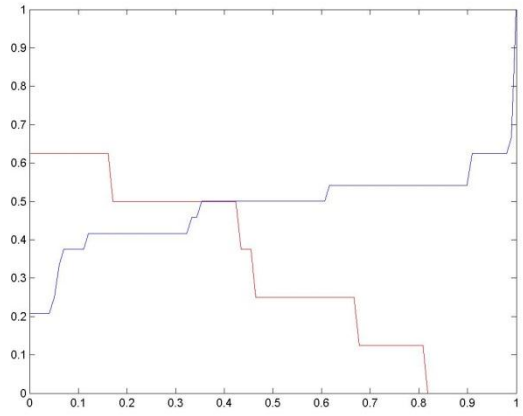
1er Person jusqu'à 4éme
Apprentissage: 7 Test: 2



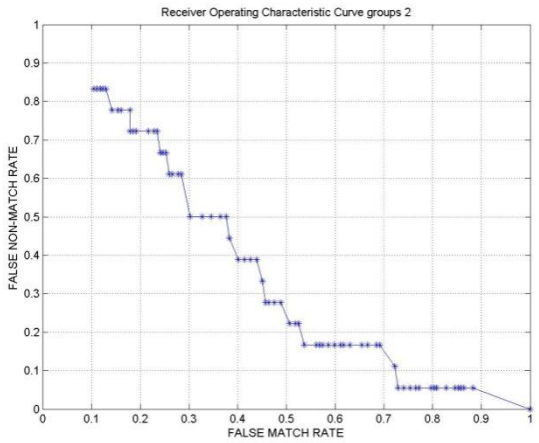


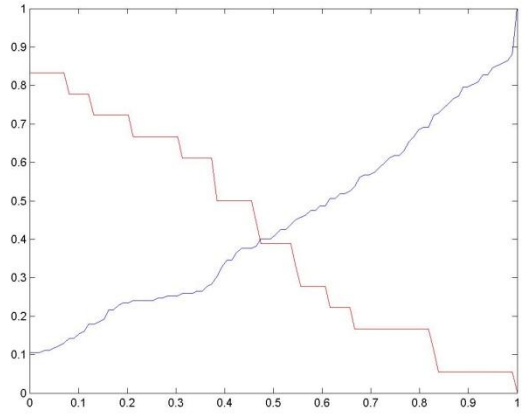
1er Person jusqu'à 4éme
Apprentissage: 8 Test: 2



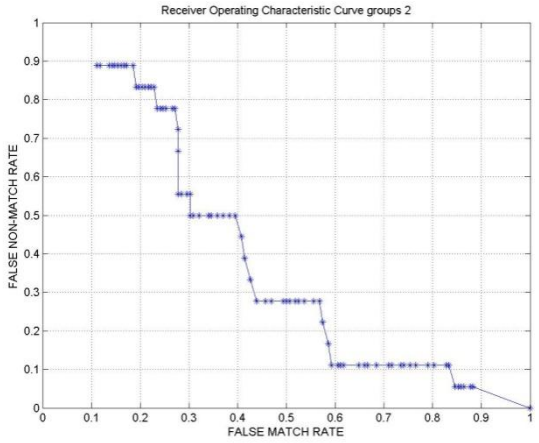


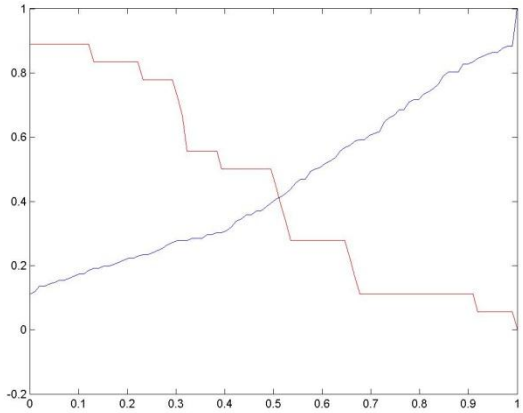
1er Person jusqu'à 10éme
Apprentissage: 6 Test: 2

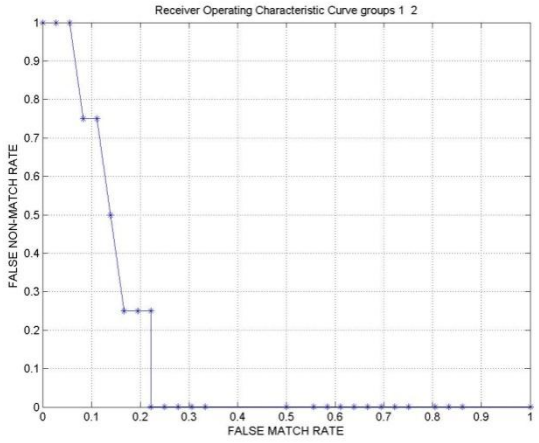


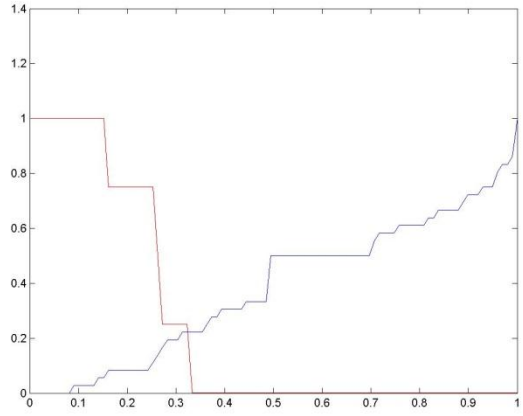


1er Person jusqu'à 10éme
Apprentissage: 7 Test: 2

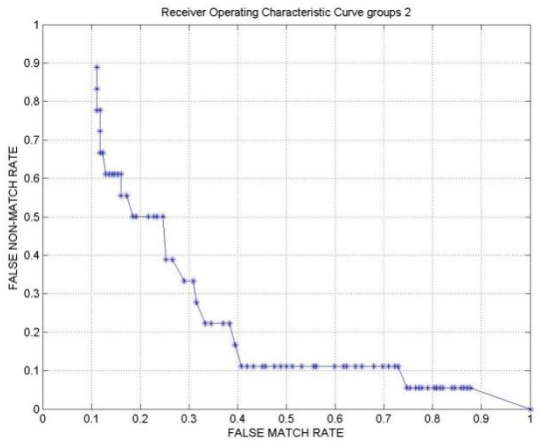


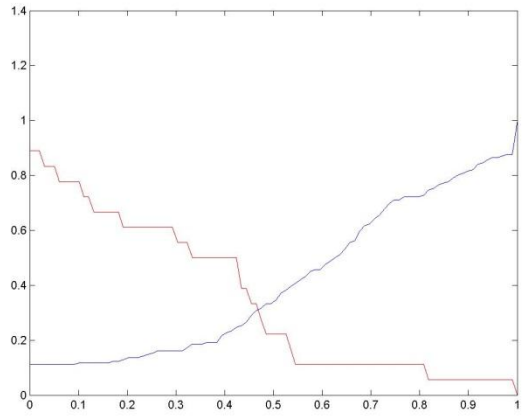




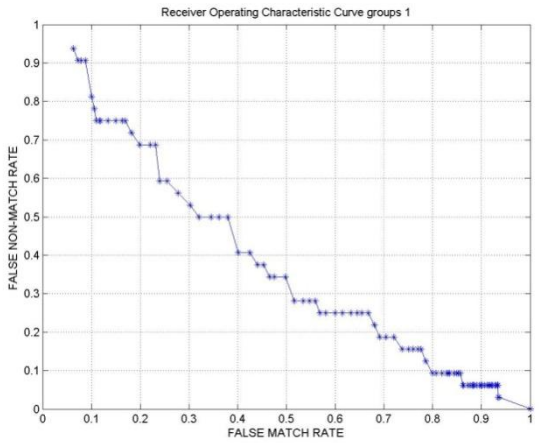


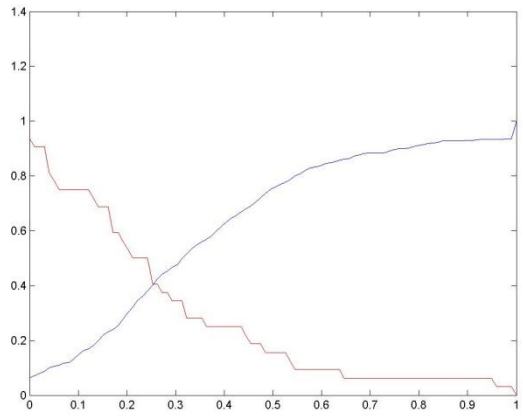
1er Person jusqu'à 10éme
Apprentissage: 8 Test: 2

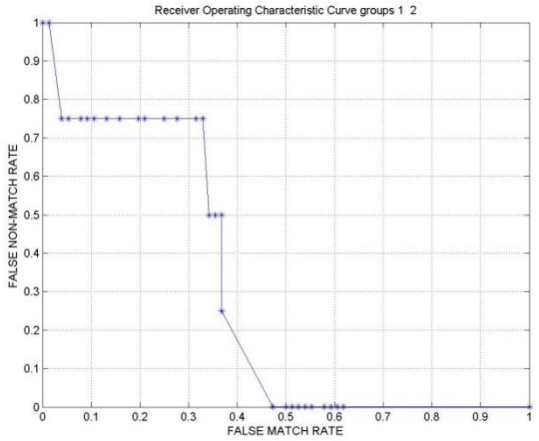


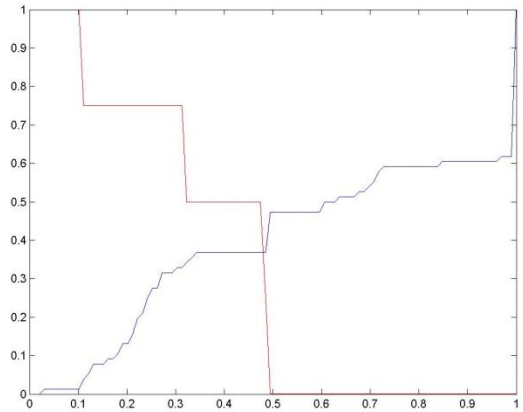


1er Person jusqu'à 20éme
Apprentissage: 6 Test: 2

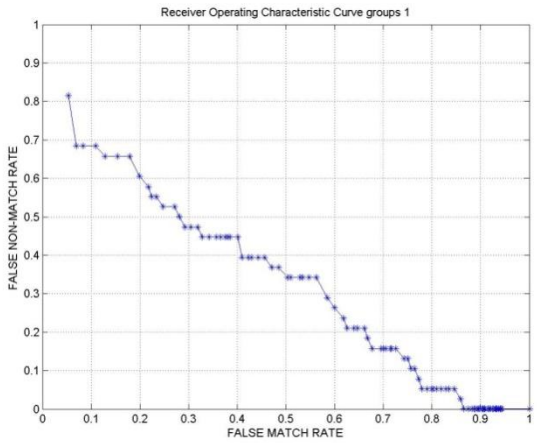


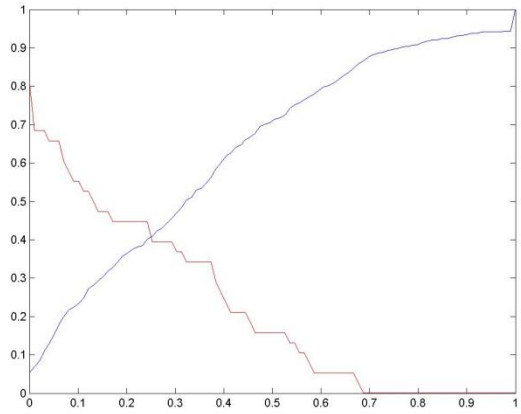


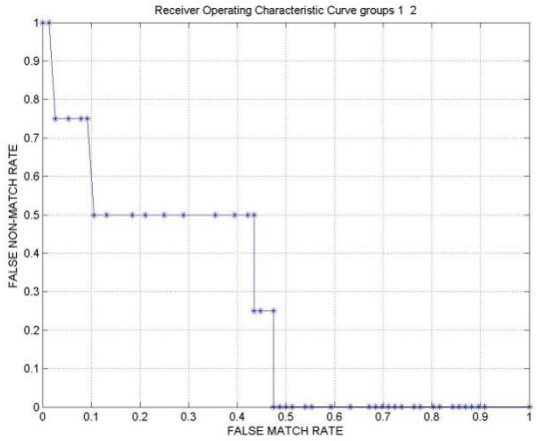


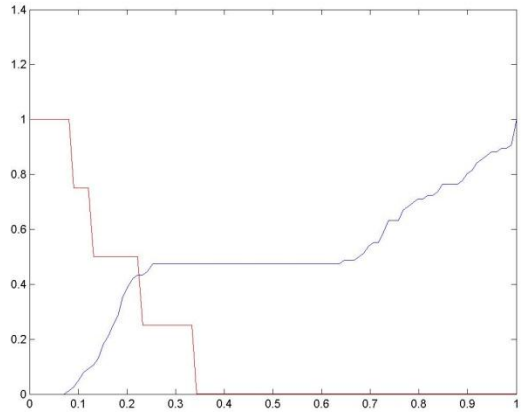


1er Person jusqu'à 20éme
Apprentissage: 7 Test: 2









1er Person jusqu'à 20éme
Apprentissage: 8 Test: 2

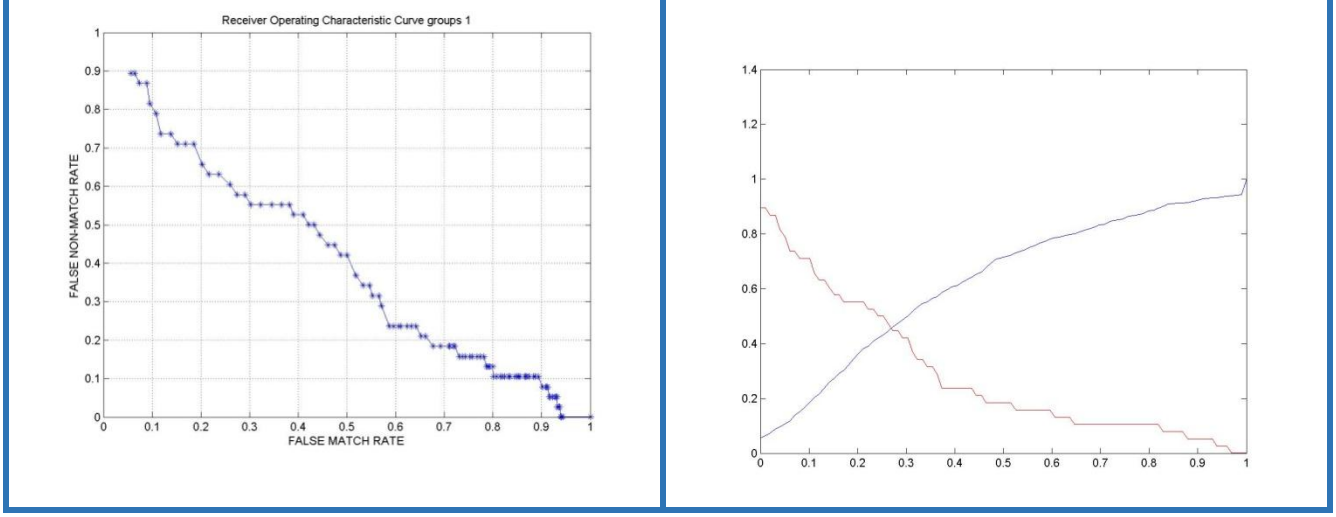


Figure IV- 3: les courbes de FAR et FRR pour les différentes vérifications réalisées

➢ Deuxième vérification:

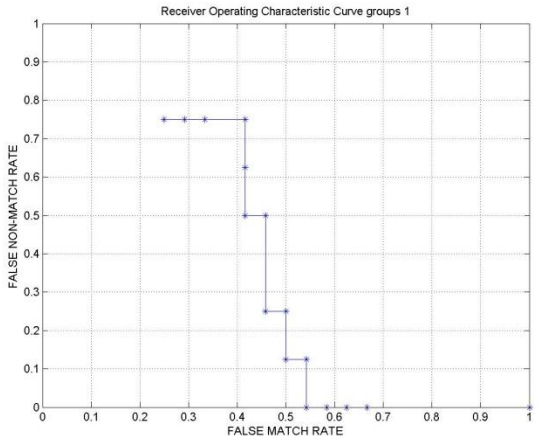
Dans ce test, on choisit de prendre différente parties de la base de données de même taille (quatre signataires). Les résultats trouvés sont représentés au tableau VI-3 :

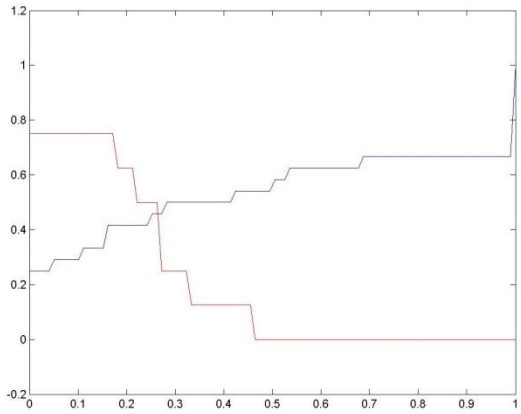
	1er Person jusqu'à 4éme	**5éme Person jusqu'à 8éme**	**20éme Person jusqu'à 23éme**	**35éme Person jusqu'à 38éme**	**47éme Person jusqu'à 50éme**
Apprentissage: 4 Test: 2	GROUPE 1: 37.5 % GROUPE 2: 50 % GROUPE 1 2: 50 %	GROUPE 1: 25 % GROUPE 2: 37.5 % GROUPE 1 2: 37.5 %	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 50 % GROUPE 2: 25 % GROUPE 1 2: 25 %
Apprentissage: 6 Test: 2	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 62.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 25% GROUPE 2: 25% GROUPE 1 2: 25%	GROUPE 1: 37.5% GROUPE 2: 25% GROUPE 1 2: 25%	GROUPE 1: 25 % GROUPE 2: 25 % GROUPE 1 2: 25 %
Apprentissage: 8 Test: 2	GROUPE 1: 25 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 25 % GROUPE 2: 25 % GROUPE 1 2: 25 %	GROUPE 1: 25% GROUPE 2: 25% GROUPE 1 2: 25%	GROUPE 1: 25% GROUPE 2: 25% GROUPE 1 2: 25%	GROUPE 1: 37.5 % GROUPE 2: 25 % GROUPE 1 2: 25 %

Tableau IV- 3: Taux de reconnaissance pour différente partie de la base de données.

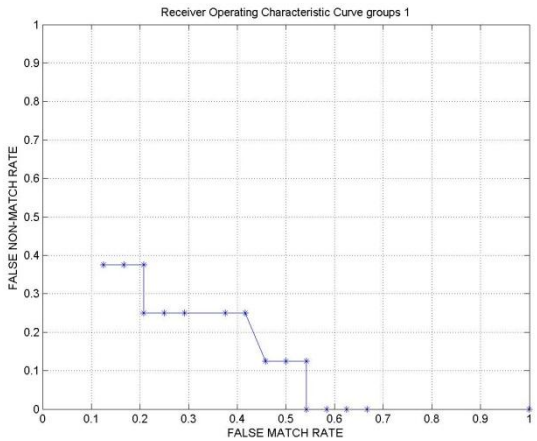
Malgré on a prend des différentes parties de base de données (personnes), mais les résultats restent presque le même le taux de faux rejeté est élevée. (figure VI-4)

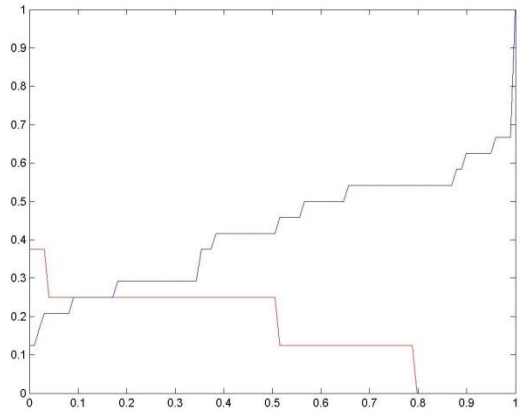
5éme Person jusqu'à 8éme
Apprentissage: 4 Test: 2





5er Person jusqu'à 8éme
Apprentissage: 6 Test: 2





5éme Person jusqu'à 8éme

Apprentissage: 8 Test: 2

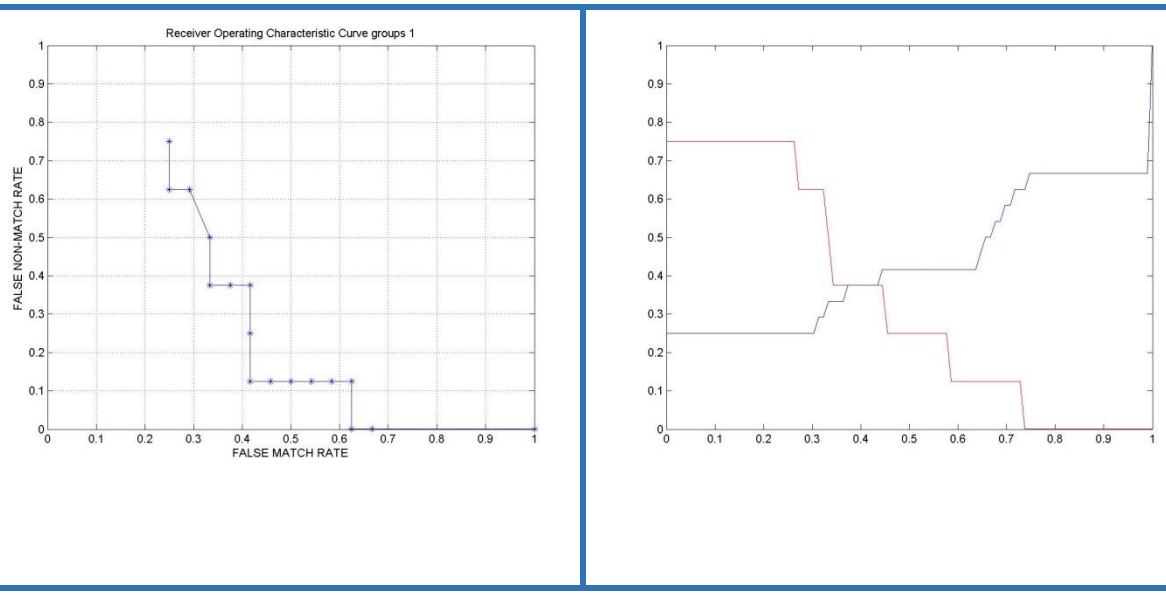


Figure IV- 4: les courbes de FAR et FRR pour le Deuxième vérification

➢ Troisième vérification :

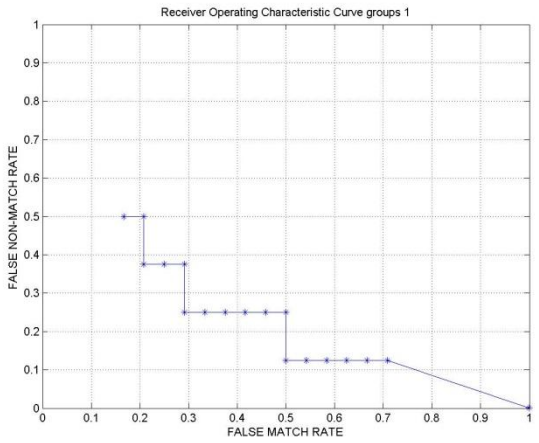
Pour améliorer le taux de reconnaissance nous essayons de prendre autre arrangement pour les paramètres utilisé, nous choisissons ([1 2 1 3]) et ont utilisé ([1 2]) pour le premier groupe et ([1 3]) pour le deuxième groupe et nous essayons pour la partie de 5^{éme} personnes jusqu'à 8^{éme} qui déjà utilisé (voir le tableau IV-3) pour nous pouvons comparer entre les deux taux de reconnaissance.

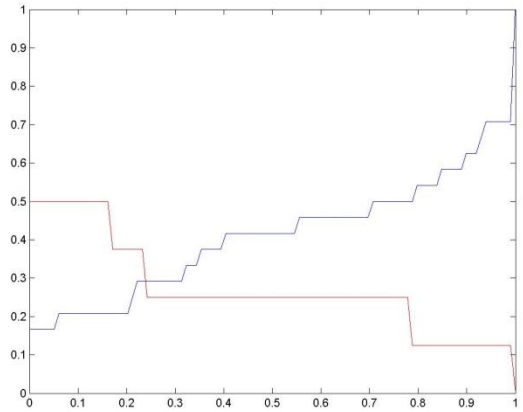
	5^{éme}Person jusqu'à 8^{éme}
Apprentissage: 4 **Test: 2**	RATE OF RECOGNITION BY GROUP 1: 50 % RATE OF RECOGNITION BY GROUP 2: 37.5 % RATE OF RECOGNITION BY GROUP 1 2: 25 %
Apprentissage: 6 **Test: 2**	RATE OF RECOGNITION BY GROUP 1: 62.5 % RATE OF RECOGNITION BY GROUP 2: 50 % RATE OF RECOGNITION BY GROUP 1 2: 75 %
Apprentissage: 8 **Test: 2**	RATE OF RECOGNITION BY GROUP 1: 75 % RATE OF RECOGNITION BY GROUP 2: 37.5 % RATE OF RECOGNITION BY GROUP 1 2: 50 %

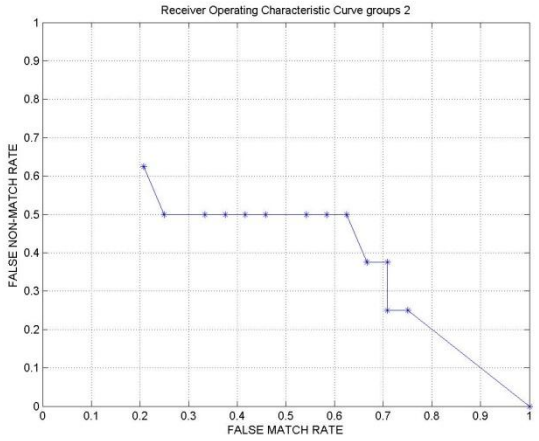
Tableau IV- 4: Taux de reconnaissance de la partie de 5éme personne jusqu'à 8éme après le nouveau choix [1 2 1 3].

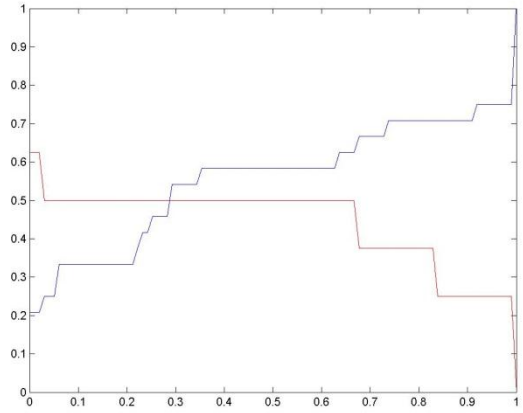
La comparaison des tableaux IV-3 et IV-4 montre que le choix d'arrangement ([1 2 1 3]) plus efficace que le choix ([1 2 3 4]) parce que le taux de reconnaissance est augmenté pour la partie de 5^{éme} personne jusqu'à le 8^{éme} dans les deux tableaux. Nous remarquons aussi que le taux de reconnaissance est augmenté en fonction d'augmentation de nombre des signatures d'apprentissage.

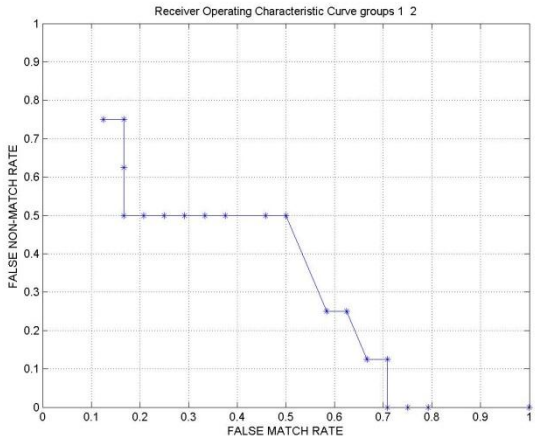
5éme Person jusqu'à 8éme
Apprentissage: 4 Test: 2

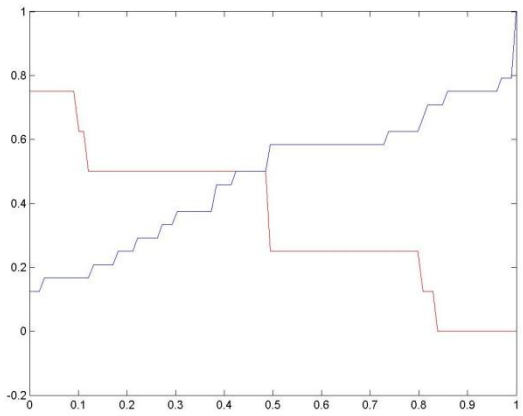




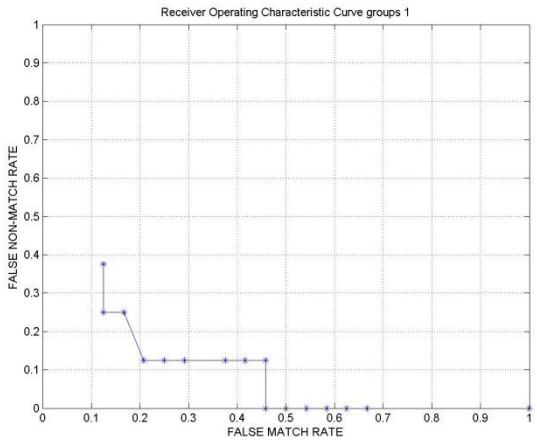


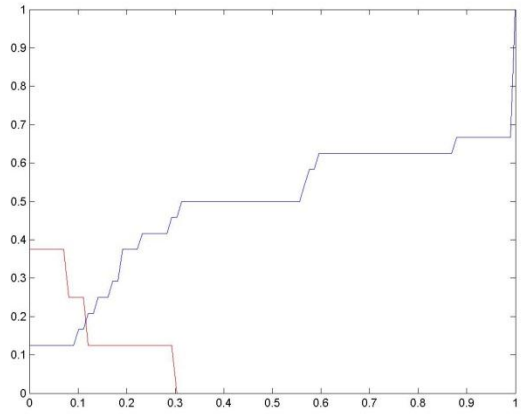


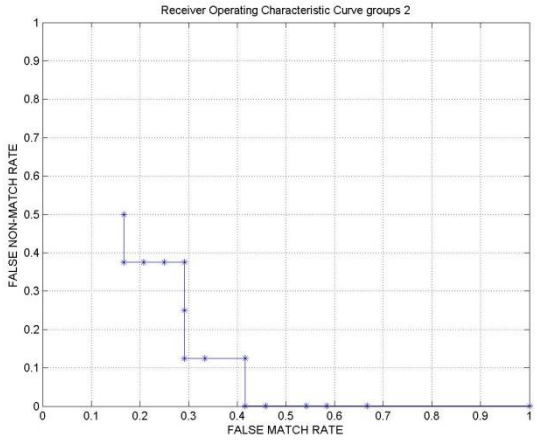


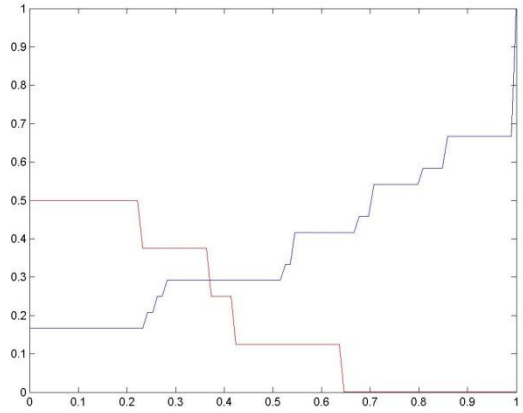


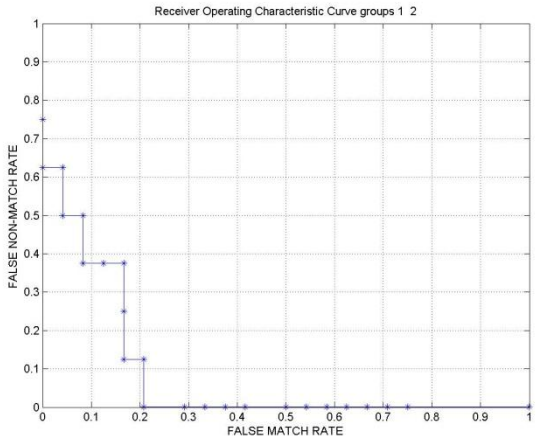
5éme Person jusqu'à 8éme
Apprentissage: 6 Test: 2

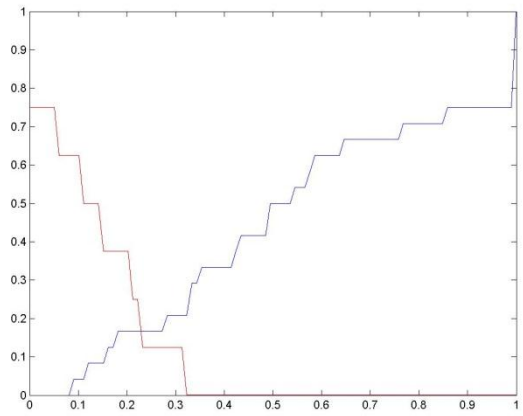












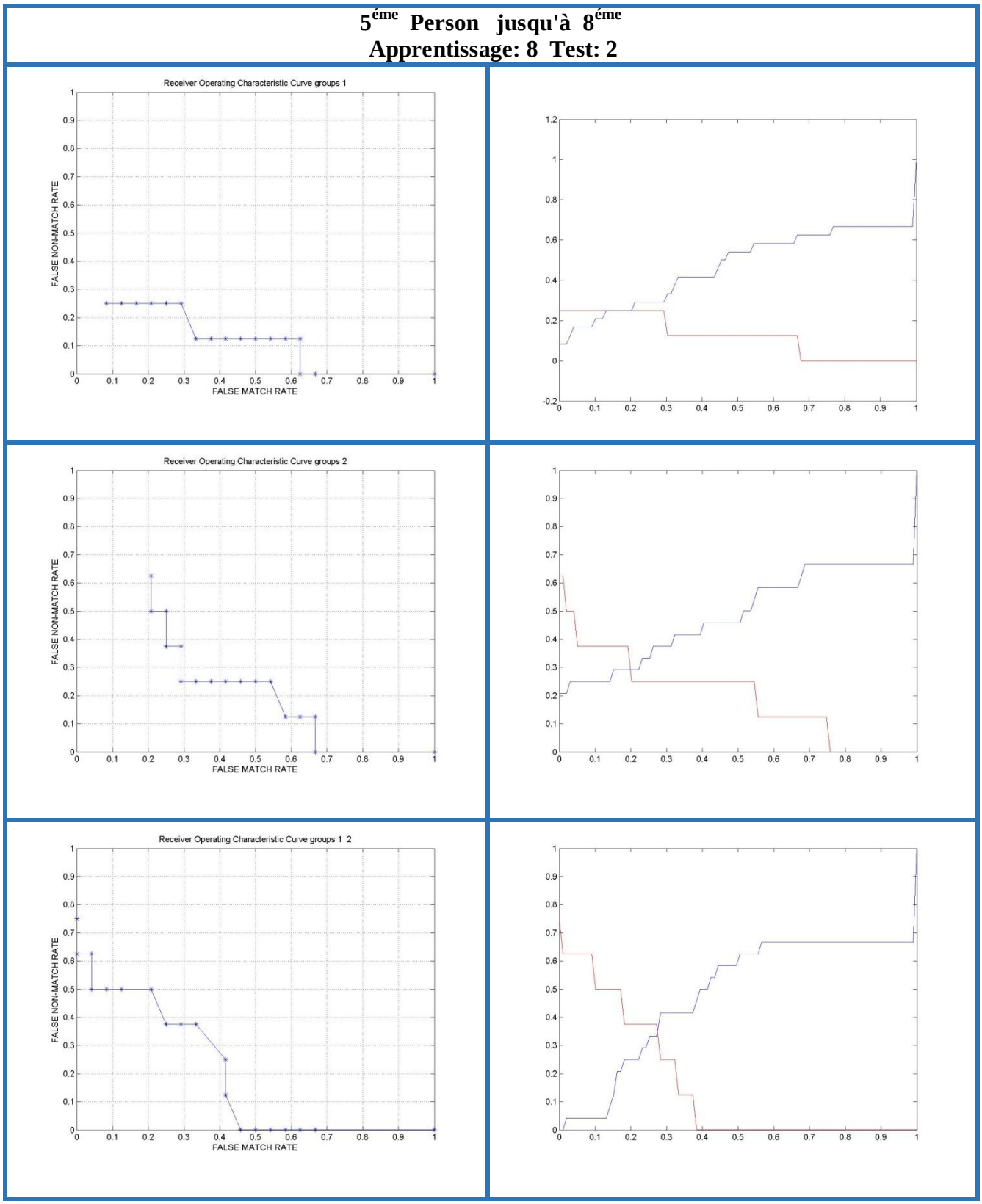


Figure IV- 5: les courbes de FAR et FRR pour la troisième vérification

IV-4. Conclusion

Nous avons évalué dans ce chapitre la performance d'une technique proposée offline pour les systèmes de vérification des signatures manuscrites utilisant le HMM multi-variables comme approche de vérification. Nous avons constaté que cette hypothèse était fiable à un certain degré sur la base MAUG14/15 (Master Automatique Université de Ghardaïa 2014/2015) .Ceci revient à l'efficacité du choix des paramètres utilisés dans l'approche de vérification.

Conclusion générale

Notre projet de fin d'étude s'est porté sur la vérification hors-ligne des signatures manuscrites, Afin d'atteindre notre objectif qui était de concevoir et de réaliser un Système de Vérification hors-ligne de Signatures Manuscrites. Notre approche est basée sur l'application les Modèles de Markov Cachés , une technique plus fonctionnelle actuellement dans le domaine de traitement et de reconnaissance d'écriture.

D'une part nous avons présenté une étude théorique des HMMs, l'une des méthodes qui ont montré leur efficacité dans la reconnaissance des formes et textes. Dans le traitement des images cette méthode ne caractérise pas la nature bidimensionnelle des images.

A ce stade, il faut noter que les recherches dans ce domaine ne cessent de se développer, la plupart des systèmes proposés jusqu'ici, présentent de bonnes performances sur les même types de faux, celle-ci diminuent considérablement si toutes les catégories de faux sont présents.

BIBLIOGRAPHIE

Références chapitre I

[1]. A. K. Jain, A. Ross et S. Prabhakar. "*An introduction to biometric recognition",* IEEE transactions on circuits and systems for video technology, Vol. 14, no. 1, pp. 4-20 Janvier 2004.

[2]. D. Maltoni, D. Maio, A. K. Jain et S. Prabhakar, *"Handbook of Fingerprint Recognition",* Springer Verlag, New York, NY, USA, Juin 2003.

[3]. A. Jain, R. Bolle et S. Pankanti, *"BIOMETRICS: Personal Identification in Networked Society",* Kluwer Academic Publishing, 1999 (quatrième édition 2002).

[4]. D. Polemi, *"Biometrics techniques: review and evaluation of biometric techniques for identification and authentication, including an appraisal of the areas where they are most applicable",* Rapport interne, Institute of communication and computer systems, National technical university of Athens, 1997.

[5]. E. Sender, *"Le corps pour tout passeport",* Revue Sciences et Avenir, pages 64-67, Septembre 2004.

[6]. Guide de sécurité des technologies de l'information, *"Les technologies biométriques : une évaluation d'applications pratiques"*, Sous direction de la sécurité technique, Opérations techniques, Gendarmerie royale du Canada, juin 2002.

[7]. "Biometrics Information Resource: Signature Recognition", http://www.biometricsinfo.org/signaturerecognition.htm

[8]. L. K. Kwong, *"A New Statistical Stroke Recovery Method and Measurement for Signature Verification"*, thèse de PhD, Hong Kong Baptist University, Septembre 2005.

[9]. M. H. Cherpin, *"Identification biologique des personnes",* Revue de l'ACOMEN, Vol.5, n°3, 1999

[10]. A. J. Jeffreys, V. Wilson et S. L. Thein, *"Hypervariable minisatellite ragions in human DNA"*, Nature, 314, pp 67-73, 1985.

Références chapitre II

[1]. L. Laouamer, "*Vérification des signatures avec la pré-topologie et les réseaux de neurones"*, thèse de Maîtrise en Informatique et Mathématiques Appliquées, Université du Québec, 2003.

[2]. S. Impedovo, G. Pirlo, "*Verification of Handwritten Signatures: an Overview"*, 14th International Conference on Image Analysis and Processing (ICIAP 2007), IEEE 2007.

[3]. A. Zimmer, L. L. Ling, *"Off-line Signature Verification System Based on the On-line Data"*, EURASIP Journal on Advances in Signal Processing, volume 2008, ID 492910, 16 pages.

[4]. A. A. Kholmatov, *"Biometric Identity Verification Using On-Line & Off-Line Signature Verification"*, Master of Science thesis, Sabanci University, 2003.

[5]. S. N. Srihari, A. Xu et M. K. Kalera, "*Learning Strategies and Classification Methods for Off-line Signature Verification",* Proceedings of the 9th International Workshop on Frontiers in Handwriting Recognition, IWFHR'9, IEEE 2004.

[6]. N. Otsu, "*A threshold selection method from gray-level histograms"*, IEEE Trans. on Systems, Man and Cybernetics 9 (1979)

[7]. R. C. Gonzalez, R. E. Woods, *"Digital Image Processing"*, Addison-Wesley (2002)

[8]. F. Faure, E. Labbé, *"Système de reconnaissance de texte imprimés"*, ENST, Mars 1996

[9]. J. F. Aguilar, N. H. Alonso, G. M. Moreno et J. O. Garcia, *"An off-line signature verification system based on fusion of local and global information"*, In Proc. European Conf. on Computer Vision, Workshop on Biometric Authentication, BIOAW, Springer LNCS-3087,pages 295–306, Prague, May2004.

[10]. M. R. Freire, J. Fierrez, M. M. Diaz et J. O. Garcia, *"On the applicability of off-line signatures to the fuzzy vault construction"*, ICDAR 2007

[11]. *http://www.cse.ust.hk/svc2004/download.html,2009*

[12]. J. Fierrez, D. R-Castro, J. O-Garcia et J. G-Rodriguez, *"HMM-based online signature verification: feature extraction and signature modeling"*, Pattern Recognition Letters, Vol. 28, n. 16, pp. 2325-2334, December 2007.

[13]. T. T. Doan, *"VERIFICATION DE SIGNATURE EN-LIGNE"*, thèse master informatique, Institut de la Francophonie pour l'Informatique, Institut National des Télécommunications, janvier 2006.

[14]. F.A. Afsar, M. Arif et U. Farrukh, *"Wavelet Transform Based Global Features for Online Signature Recognition"*, 9th International Multi topic Conference, IEEE INMIC 2005

[15]. M. E. Munich et P. Perona, *"Camera-Based ID Verification by Signature Tracking"*, in Proceedings of the 5th European Conference on Computer Vision EECV'98 (pp: 782-796), Freiburg, Germany, June 1998.

[16]. M. E. Munich et P. Perona, *"Visual Input for Pen-Based Computers"*, in Proceedings of the 3rd International Conference on Image Processing, Lausanne, September 1996.

[17]. M. Adamski, K. Saeed, *"Online Signature Classification and its Verification System"*, 7th Computer Information Systems and Industrial Management Applications, pp 189-194, IEEE, 2008

[18]. H. Bourlard, C.J. Wellekens, *"Links Between Markov Models and Multilayer Perceptrons"*, IEEE Transactions on Pattern Analysis and Machine Intelligence, 12(12), pp: 1167-1178, 1990

Références chapitre III

[1]. L. Bréhélin et O. Gascual, "*Modèles de Markov cachés et apprentissage de séquences*", Le temps, l'espace et l'evolutif en sciences du traitement de l'information, Edition Cépaduès, H. Prade, R. Jeansoulin et C. Garbay éditeurs, 2000, pp 407-421.

[2]. A. Belaïd, G. Saon, "*Utilisation des processus markoviens en reconnaissance de l'écriture*", *Traitement de signal, vol.14 n°2, pp 161-178*, 1997.

[3]. N. Ben Amara, A. Belaïd et N. Ellouze, "*Utilisation des modèles markoviens en reconnaissance de l'écriture arabe- Etat de l'art*", Colloque international francophone sur l'écrit et le document, Lyon , France 2000 , pp. 181-191

[4]. N. Ben amara, A. Belaid, "*Une méthode stochastique pour la reconnaissance de l'écriture arabe imprimée*", Forum de la Recherche en Informatique, Tunisie, 16-18 juillet 1996.

[5]. L. R. Rabiner, "*A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition",* Proc. of IEEE, VOL. 77, NO. 2. pp 257-286. Février 1989.

[6]. L. Bréhélin et O. Gascual*, "Modèles de Markov cachés et apprentissage de séquences", Le temps, l'espace et l'evolutif en sciences du traitement de l'information, Edition Cépaduès, H. Prade, R. Jeansoulin et C. Garbay éditeurs, 2000, pp 407-421.*

[7]. L. R. Rabiner*, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition",Proc. of IEEE, VOL. 77, NO. 2. pp 257-286. Février 1989.*

[8]*.http://www.gpds.ulpgc.es/download/index.htm.*

[9]. G. R. Bajekal*, "Characterization and automated verification of handwritten signatures", thèse master ès science, The University of Texas at Arlington, 1992.*

[10]. K. K. Meenakshi, S. Srihari et A. XU*, "Offline Signature Verification and Identification Using Distance Statistics", International Journal of Pattern Recognition and Artificial Intelligence, Vol. 18, No. 7, 2004, pp.1339-1360.*

[11]. P. Porwik, T. Para*, "Some Handwritten Signature Parameters in Biometric Recognition Process", Proceedings of the ITI 2007 29th Int. Conf. on Information Technology Interfaces, June 25-28, 2007, Cavtat,Croatia, pp. 185-190.*

ANNEXE

Cette annexe rassemble l'ensemble des algorithmes utilisés dans ce mémoire. On y trouve les algorithmes traditionnellement associés aux HMM (Forward, Backward, Baum-Welsh, Viterbi) et l'algorithme s'associe à cette étude (vecteur multi-variables).

1- Algorithme Forward

On dénote $\alpha_t(i)$ est la probabilité de la séquence partielle d'observation $O_1, O_2, \ldots, O_t$ et état S_i au temps t :

$\alpha_t(i) = P(O_1 O_2 \ldots O_t, q_t = S_i \mid \lambda)$

Les $\alpha_t(i)$ seront calculés de manière récursive comme suit :

- **Initialisation :**

$$\alpha_0(i) = \pi_i \text{et} \quad \alpha_1(i) = \alpha_0(i).b_1(i) \qquad 1 \leq i \leq N$$

- **Induction :**

$$\alpha_t(i) = b_t(j).\sum_i \{\alpha_{t-1}(i).a_{ij}\} \qquad 1 < t \leq T \quad et \quad 1 \leq i \leq N$$

- **Terminaison :**

$$P(O|\lambda) = \sum_{i=1}^{N} \alpha_T(i)$$

2- Algorithme Backward

A la manière similaire, on peut définir la probabilité backward comme suite :

$$\beta_t(i) = P(O(t+1:T), q_t = s_i|\lambda)$$

C'est à dire, la probabilité de la séquence partielle d'observation $O_{t+1}...O_T$ ayant l'état S_j au temps t et le model λ. Les $\beta_t(i)$ seront calculés de manière récursive comme suit :

- **Initialisation :**

$$\beta_T(i) = 1 \qquad 1 \leq i \leq N$$

- **Induction :**

$$\beta_t(i) = \sum_j \{a_{ij} \,.\, b_{t+1}(j).\beta_{t+1}(j)\} \qquad 1 \leq t < T \qquad et \qquad 1 \leq i \leq N$$

- **Terminaison :**

$$\beta_0(i) = b_1(i).\beta_1(i) \qquad 1 \leq i \leq N$$

3- Algorithme de Viterbi

Pour trouver le "*meilleur*" chemin $Q= (q_1,q_2,...,q_T)$ pour une suite d'observations $O= (O_1,O_2,...,O_T)$, on définit $\delta_t(i)$ qui représente la probabilité du meilleur chemin amenant à l'état s_i à l'instant t en étant guidé par les t premières observations :

$$\delta_t(i) = \max_{q_1,q_2,\dots q_{t-1}} P(q_1, q_2, \dots, q_{t-1}, q_t = s_i, O_1, O_2, \dots, O_t|\lambda)$$

Tout en gardant la trace, lors du calcul, de la suite d'états qui donne le meilleur chemin amenant à l'état s_i à l'instant t dans un tableau ψ. Formellement, on résume :

- **Initialisation :**

$$\left.\begin{matrix}\delta_1(i) = \pi_i . b_i(O_1) \\ \psi_1(i) = 0\end{matrix}\right\} \quad 1 \le i \le N$$

- **Induction :**

$$\left.\begin{matrix}\delta_t(i) = b_j(O_t) . \max_i\left[\delta_{t-1}(i) . a_{ij}\right] \\ \psi_t(i) = \operatorname{argmax}_i\left[\delta_{t-1}(i) . a_{ij}\right]\end{matrix}\right\} \quad 1 \le i, j \le N$$

- **Terminaison :**

$P^* = \max_i[\delta_T(i)]$ P^* étant la probabilité du chemin obtenu

$q_T^* = \operatorname{argmax}_i[\delta_T(i)]$ q_T^* étant le dernier état du chemin

- **Chemin obtenu (en back-traking) :**

$$q_t^* = \psi_{t+1}(q_{t+1}^*) \qquad 1 \le t \le T-1$$

4- Algorithme de Baum-Welsh

L'algorithme de *Baum-Welsh* affine le modèle petit à petit en suivant les étapes suivantes :

- Choisir un ensemble initial de paramètres λ_0.
- Calculer λ_nà partir de λ_{n-1}.
- Répéter ce processus jusqu'à un critère de fin.

On doit toujours vérifier que :

$$\prod_{r=1}^{nombre\ d'observation} P(O^r|\lambda_{n+1}) \geq \prod_{r=1}^{nombre\ d'observation} P(O^r|\lambda_n)$$

1. **Fixer les valeurs Initiales :**

$$a_{ij}^0, b_j^0(k), \pi_i^0 \qquad 1 \leq i,j \leq N, \qquad 1 \leq k \leq M$$

2. **Calculer à l'aide des fonctions Forward-Backward** :

$$\xi_t(i,j) = \frac{\alpha_t(i) \times a_{ij} \times b_j(O_{t+1})\beta_{t+1}(j)}{P(O|\lambda)}$$

$$\gamma_t(i) = \sum_{j=1}^{N} \xi_t(i,j) \quad 1 \leq i,j \leq N, \quad 1 \leq t \leq T-1$$

3. **Réestimer les paramètres du modèle $\bar{\lambda}$**

$$\bar{\pi}_i = \gamma_1(i) = \frac{\propto_1 (i) \times \beta_1(i)}{P(O|\lambda)} \qquad 1 \leq i \leq N$$

$$\bar{a}_{ij} = \frac{\sum_{t=1}^{T-1} \xi_t(i,j)}{\sum_{t=1}^{T-1} \gamma_t(i)} = \frac{\sum_{t=1}^{T-1} \alpha_t(i) \times a_{ij} \times b_j(O_{t+1}) \times \beta_{t+1}(j)}{\sum_{t=1}^{T-1} \sum_{j=1}^{N} \alpha_t(i) \times a_{ij} \times b_j(O_{t+1}) \times \beta_{t+1}(j)} \qquad 1 \leq i,j \leq N$$

$$\bar{b}_j(\mathrm{k}) = \frac{\sum_{t=1,O_t=v_k}^{T} \gamma_t(j)}{\sum_{t=1}^{T} \gamma_t(j)} = \frac{\sum_{t=1 \Lambda O_t=v_k}^{T} \alpha_t(j) \times \beta_t(j)}{\sum_{t=1}^{T} \alpha_t(j) \times \beta_t(j)} \qquad 1 \leq i \leq N, \qquad 1 \leq k \leq M$$

5- Algorithme de HMM multi-variables

Dans le cas, où on a un vecteur de plusieurs paramètres $X_t=\{x_t^1, x_t^2, ..., x_t^r, ..., x_t^R\}$ pour un seul HMM, nous utiliserons le HMM multi-paramètres. Pour prendre en compte de chaque paramètre isolé seul, nous proposons de modifier le calcul de la probabilité de vecteur d'observation $b_j(O_t)$. Les autres formules sont inchangées.

Dans le cas continu, où $O_t=X_t$, $b_j(O_t)$ est calculé comme :

$$b_j(O_t) = \prod_{r=1}^{R} b_j(O_t^r)$$

Où, $b_j(O_t^r) = \sum_{m=1}^{M} c_{jm}^r \, \aleph(O_t^r, \mu_{jm}^r, U_{jm}^r)$

Dans le cas discret, nous calculons un certain nombre de vecteur mesuré de R avec des vecteurs de code $\{v_k^r\}_{k=1,2,....,C_r}^{r=1,2,.....,R}$, et mesurer chaque paramètre x_t^r avec son vecteur de mesure comme suit :

$$O_t^r = v_k^r \; iff \;\; d(x_t^r, v_k^r) < d(x_t^r, v_m^r) \text{pour tout} m \neq k$$

$$b_j(O_t) = \prod_{r=1}^{R} b_j(O_t^r) \text{avec} b_j(O_t^r) = b_j(v_k^r)$$

Et la formule de ré-estimation est : $\overline{b}_j(v_k^r) = \frac{\sum_{t=1}^{T} \gamma_t(i)}{\sum_{t=1}^{T} \gamma_t(i)} \; s.t. O_t^r = v_k^r$

En conclusion, dans le cas discret, il est possible de tenir compte de chaque paramètre a une manière d'isolement ; nous avons tracé chaque vecteur X_t d'entrée dans un vecteur observable $O_t= \{w^1 (x_t^1, v_k^1), w^2 (x_t^2, v_k^2),$

$$w^r(x_t^r, v_k^r) = \frac{1/d(x_t^r, v_k^r)}{\sum_{m=1}^{C_r} 1/d(x_t^r, v_m^r)}$$

étant la probabilité de distribution établie comme

$$b_j(O_t) = \prod_{r=1}^{R} b_j(O_t^r) = \prod_{r=1}^{R} \left(\sum_{k=1}^{C_r} w^r(x_t^r, v_k^r) \, b_j(v_k^r) \right)$$

Et la formule de ré-estimation est : $\overline{b}_j(v_k^r) = \frac{\sum_{t=1}^{T} \gamma_t(i) w^r(x_t^r, v_k^r)}{\sum_{t=1}^{T} \gamma_t(i)}$

	Dimanche	Mardi	Jeudi
1er semaine	02 نوفمبر 2014	04 نوفمبر 2014	06 نوفمبر 2014
2éme semaine	09 نوفمبر 2014	11 نوفمبر 2014	
3éme semaine			

1er Person de base de donnée MAUG14/15

	Dimanche	Mardi	Jeudi
1er semaine	02 نوفمبر 2014	04 نوفمبر 2014	06 نوفمبر 2014
2éme semaine	09 نوفمبر 2014	11 نوفمبر 2014	
3éme semaine			

5éme Person de base de donnée MAUG14/15

	Dimanche	Mardi	Jeudi
1er semaine	2014 نوفمبر 02	2014 نوفمبر 04	2014 نوفمبر 06
2éme semaine	2014 نوفمبر 09	2014 نوفمبر 11	
3éme semaine			

8éme Person de base de donnée MAUG14/15

	Dimanche	Mardi	Jeudi
1er semaine	2014 نوفمبر 02	2014 نوفمبر 04	2014 نوفمبر 06
2éme semaine	2014 نوفمبر 09	2014 نوفمبر 11	
3éme semaine			

22éme Person de base de donnée MAUG14/15

Résumé

L'objectif de ce travail est la contribution à la vérification hors ligne de la signature manuscrite, Nous avons crée une base de donnée de cinquante Personnes, neuf signatures pour chacun.

Dans ce mémoire, nous avons utilisé les traitement des images avant segmenter les images de signatures, les résultats obtenus montrent que cette méthode est efficace, et les strokes extraits à partir de cette segmentation sont valable à utiliser pendant la phase de vérification.

Les chaînes de Markov cachées sont utilisées pour l'identification et la vérification des paramètres extraits à partir des strokes, les résultats obtenus montrent que nous avons obtenu des résultats globalement acceptables.

Mots clés

Biométrie, Vérification hors-ligne, signature manuscrite, Segmentation, Extraction des paramètres, Les chaînes de Markov cachées, HMM, FAR, FRR, ROC.

Abstract

The objective of this work is the contribution to the off line verification of handwritten signature, We have created a database of fifty person for each one nine signatures.

In this thesis, we used the processing images before segmenting the signatures images, the results obtained show that this method is effective and the strokes extracted starting from this segmentation are valid to use during the verification phase.

The hidden Markov models are used for the parameters extracted starting from the strokes identification and verification, the results obtained show that we have obtained Generally acceptable results.

Key words

Biometrics, offline verification, handwritten signature, Segmentation, Features extraction, hidden Markov models, HMM, FAR, FRR, ROC.

خلاصة

الهدف المرجو من هذا العمل هو انجاز برنامج للتأكد غير الخطى على التوقيعات الخطية، لهذا قمنا بإنشاء قاعدة بيانات تضم خمسين شخص لكل واحد منهم تسعة توقيعات .

في هذه المذكرة ، قمنا بمعالجة التوقيعات و تجزئتها ، النتائج المحصلة تثبت أن هذه الطريقة فعالة، والأجزاء المستخلصة من هذه التجزئة مقبولة لاستعمالها أثناء مرحلة التأكد.

نماذج ماركوف الخفية استعملت في التحقق و التأكد من المعالم المستخلصة من الأجزاء، نتائج الدراسة تبين أننا تحصلنا على نتائج نوعنا ما مقبولة.

كلمات مفتاحية

القياس البيولوجي، التأكد غير الخطي، التوقيعات الخطية، التجزئة، استخلاص المعلمات، نماذج ماركوف الخفية، HMM, FAR, FRR, ROC .