وزارة التعليم العالي و البحث العلمي

BADJI MOKHTAR UNIVERSITY- ANNABA
UNIVERSITE BADJI MOKHTAR - ANNABA

جامعة باجي مختار - عنابة

FACULTE DES SCIENCES DE L'INGENIORAT
DEPARTEMENT D'ELECTRONIQUE

Année : 2016

THESE

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

Thème

Reconnaissance Biométrique Multimodale basée sur la fusion en score de deux modalités biométriques : l'empreinte digitale et la signature manuscrite cursive en ligne

Option : Instrumentation et traitement de l'information

Par :

Hafs Toufik

Directeur de Thèse:
BENNACER Layachi - Professeur- Université de Badji Mokhtar, Annaba
Co-Directeur:
BOUGHAZI Mohamed - MCA - Université de Badji Mokhtar, Annaba

Devant Jury:

Président:			
Pr.	**Salah**	**TOUMI**	**Université d'Annaba**
Examinateurs:			
Pr.	**Noureddine**	**DOGHMANE**	**Université d'Annaba**
Pr.	**Abdelhani**	**BOUKROUCHE**	**Université de Guelma**
Pr.	**Rafik**	**DJEMILI**	**Université de Skikda**

Remerciement

Je remercie, avant tout, Dieu, le Tout-Puissant, de m'avoir accordé parmi Ses innombrables Grâces, santé et courage pour accomplir ce travail.

Je remercie, en premier lieu, Monsieur Layachi BENNACER professeur à l'Université Badji Mokhtar Annaba et directeur de cette thèse, pour avoir assuré le suivi de cette thèse. Son expérience et son aide scientifique m'ont été essentielles. Sa disponibilité ainsi que l'attention qu'il a portée à ce travail ont été un atout précieux dans l'avancement de cette étude.

Les mots ne suffisent pas pour exprimer ma profonde gratitude à Monsieur Mohammed BOUGHAZI, Maître de conférences à l'Université Badji Mokhtar Annaba et co-directeur de cette thèse, d'abord de m'avoir suivi pas à pas et d'une manière approfondie, et aussi pour la qualité de ses conseils et ses encouragements et son soutien qui ont été indispensables à l'aboutissement de mes études.

Je tiens à remercier également Monsieur Salah TOUMI , professeur à l'Université Badji Mokhtar Annaba, Directeur du Laboratoire Étude et Recherche en Instrumentation et Communication Avancée Annaba (LERICA) , pour m'avoir accueilli au sein de son laboratoire puis pour l'honneur qu'il m'a fait en présidant le jury de ma soutenance.

Je tiens, également, à remercier, chaleureusement, Monsieur Noureddine DOGHMANE, professeur à l'Université Badji Mokhtar Annaba, qui a été un excellent enseignant et qui a contribué de façon considérable à ma formation. Veuillez trouver ici l'expression de ma sincère reconnaissance d'avoir accepté d'examiner mon travail.

J'adresse également mes remerciements à Monsieur Abdelhani BOUKROUCHE, professeur à l'Université du 8 Mai 1945 de Guelma d'avoir accepté d'examiner mon travail.

Je tiens à remercier également Monsieur Rafik DJEMILI, professeur à l'Université du 20 Aout 1955 Skikda d'avoir accepté d'examiner mon travail.

Je remercie Monsieur Amine NAIT-ALI professeur à l'Université Paris Est Créteil (UPEC) qui m'a prodigué quelques précieux conseils qui ont conduit à l'aboutissement de mon travail.

Je souhaite témoigner également mes profonds remerciements à tous les membres et les doctorants du LERICA qui, de près ou de loin, ont contribué à l'avancement de ce travail.

Dédicace

Je dédie cette Thèse :

À MA TRÈS CHÈRE MÈRE : Autant de phrases aussi expressives soient-elles ne sauraient montrer le degré d'amour et d'affection que j'éprouve pour toi. Tu m'as comblé avec ta tendresse et affection tout au long de mon parcours. Tu n'as cessé de me soutenir et de m'encourager durant toutes les années de mes études, tu as toujours été présente à mes côtés pour me consoler quand il fallait. Puisse le tout puissant te donner santé, bonheur et longue vie afin que je puisse te combler à mon tour.

À MON TRÈS CHER PÈRE : Autant de phrases et d'expressions aussi éloquentes soit-elles ne sauraient exprimer ma gratitude et ma reconnaissance. Tu as su m'inculquer le sens de la responsabilité, de l'optimisme et de la confiance en soi face aux difficultés de la vie. Tes conseils ont toujours guidé mes pas vers la réussite. Ta patience sans fin, ta compréhension et ton encouragement sont pour moi le soutien indispensable que tu as toujours su m'apporter. Que Dieu le Tout-Puissant te préserve, t'accorde santé, bonheur, quiétude de l'esprit et te protège du mal.

À Mes Frères et sœurs (ALI,NACIRA,SAMIA,MAHMOUD,MOURAD,BOUBEKEUR) : Pour toute la complicité et l'entente qui nous unissent, je ne pourrais jamais exprimer le respect et l'amour que j'ai pour vous. Vos prières, vos encouragements et votre soutien m'ont toujours été d'un grand secours.

À MA TRÈS CHÈRE Femme : Ton encouragement et ton soutien étaient la bouffée d'oxygène qui me ressourçait dans les moments pénibles Merci d'être toujours à mes côtés, par ta présence, par ton amour dévoué et ta tendresse.

À mon cher grand-père maternel : Que ce modeste travail, soit l'expression des vœux que vous n'avez cessé de formuler dans vos prières. Que Dieu vous préserve santé et longue vie.

À la mémoire de mes grands-pères et de mes grandes mères: Qui ont été toujours dans mon esprit et dans mon cœur, je vous dédie aujourd'hui ma réussite. Que Dieu, le miséricordieux, vous accueille dans son éternel paradis.

À mes chère ANFEL et ABDELRAHMAN: le symbole de la joie, l'ambiance et la tendresse. Que Dieu les gardent et leurs ouvre les chemins du savoir et de la réussite.

À ma grande famille : mes tantes, mes oncles, ainsi que mes cousins et cousines.

À tous mes amis et à tout le groupe de notre mosquée (Masdjid Billel Ben RABEH)

Résumé

La biométrie multimodale, qui consiste à combiner plusieurs systèmes biométriques, est de plus en plus étudiée. En effet, elle permet de réduire certaines limitations des systèmes biométriques unimodaux, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude intentionnelle, tout en améliorant les performances de reconnaissance. Ces avantages apportés par la multimodalité aux systèmes biométriques unimodaux sont obtenus en fusionnant plusieurs systèmes biométriques.

L'objectif de cette thèse est de combiner plusieurs modalités biométriques (empreinte digitale avec la signature manuscrite d'un individu). On a utilisé la décomposition modale empirique pour extraire les informations les plus pertinentes de la signature manuscrite en ligne ainsi qu'une méthode structurelle basée sur la détermination des minuties pour extraire les paramètres de l'empreinte digitale. Les scores de comparaison ainsi obtenus sont normalisés puis fusionnés à l'aide d'une méthode combinatoire en occurrence la somme pondérée. Les résultats obtenus montrent que la stratégie proposée donne des performances très encourageantes où on a obtenu un EER de 1.69%.

Mots clés: Traitement du signal et de l'image, biométrie multimodale, fusion des scores, Empreintes digitales, Signature manuscrite en ligne, Décomposition modale empirique EMD, Minuties , Min-Max , Somme pondérée.

ملخص

القياسات البيومترية المتعددة الوسائط هي عملية الجمع بين مجموعة من الأنظمة البيومترية للتحقق من هوية الأشخاص . هذه الطريقة تدرس وتستعمل على نحو متزايد لتحديد هوية الأشخاص لأنها تقلل من القيود التي توجد في الأنظمة الأحادية الوسط ، مثل عدم القدرة على الحصول على بيانات من أشخاص معينين أو الغش المتعمد، هذا مع تقليل نسب الخطأ . ويتم الحصول على هذه الفوائد من خلال دمج العديد من أنظمة التحقق من الهوية في نظام واحد.

الهدف من هذه الرسالة هو الجمع بين عدة طرق بيومترية (بصمة الأصبع مع التوقيع بخط اليد للفرد). استخدمنا طريقة تحليلية (Décomposition modale empirique) لاستخراج المعلومات من التوقيع بخط اليد وطريقة هيكلية قائمة على أساس تحديد تفصيلات لاستخراج المعلمات من بصمات الأصابع .قمنا بنمدجة نتائج المقارنة قبل استخدام طريقة اندماجية قائمة على الجمع الموزون .أظهرت النتائج أن الاستراتيجية المقترحة جد فعالة جدا حيث قدرت نسبة الخطأ المساوي المتحصل عليها بـ 1.69٪.

الكلمات المفتاحية: معالجة الاشارة والصورة، البيومترية المتعددة الوسائط، الاندماج على مستوى النتائج، البصمات، التوقيع بخط اليد، EMD ،Min–Max ، تفصيلات، الجمع الموزون.

Abstract

Multimodal biometrics, which is the combination of several biometric systems, is increasingly studied. Indeed, it reduces limitations of unimodal biometric systems, such as the inability to acquire the data from certain persons or intentional fraud, and improve recognition performance. These benefits of multimodality against the unimodal biometric systems are obtained by merging several biometric systems.

The objective of this thesis is to combine several biometric modalities (fingerprint and the online handwritten signature of an individual). Empirical Mode Decomposition was used to extract the most relevant information of the online handwritten signature while a structural method based on the determination of minutiae is used to extract the parameters of fingerprints. The comparison scores thus obtained are normalized and then merged using a combinatorial the weighted sum approach. The obtained results show that the proposed strategy gives very encouraging performance where an EER of 1.69% was obtained.

Keywords: Image and signal processing , Multibiometrics, scores fusion, Fingerprint, online handwritten signature, empirical mode decomposition EMD, Minuties , Min-Max , weighted sum.

Table des matiéres

CHAPITRE II : Etat de l'art sur la fusion de données

CHAPITRE III : Système proposé

liste des Abréviations

AM: *Amplitude modulation*

AUC: *Area under the curve*

ACP: Analyse en composante principale

CCD: Dispositif couplé chargé

CN: *Crossing number*

DET: *Detection error tradeoff*

DSP: *Digital Signal Processor*

EMD : *Empirical mode décomposition*

ECG : Electrocardiogramme

EMG : Electromyogramme

EER: *Equal error rate*

FAR: *False acceptation rate*

FRR: *False rejection rate*

FM: *Frequency modulation*

FPGA: *Field-programmable gate array*

FVC2004: *Fingerprint Verification Competition 2004.*

HMM: *Hidden Markov Models*

HSD: *Hilbert scanning distance*

IRM : Imagerie par résonance magnétique.

IHM: Interaction Homme Machine

IMF: *Intrinsic mode functions*

KNN: *k-nearest neighbors*

LDA: *Linear discriminant analysis*

LED: Diode électrolumineux

MYCT: *Ministerio de ciencia y tecnologia* (en espagnol)

MFCC: *Mel-frequency cepstral coefficients*

ROC: *Receiver operating characteristic*

RNA: Réseaux de neurones artificiels

ROI: *Region of interest*

SVC: *Signature Verification Competition 2004*

SD: *Stopping decision*

SVM: *Support Vector Machine*

liste des figures

liste des tableaux

Introduction générale

Savoir déterminer l'identité d'une personne de façon automatique demeure un dilemme d'actualité. Dans un monde qui devient de plus en plus interconnecté, il est impératif de reconnaître les utilisateurs afin de leurs donner accès à un immeuble ou de les procurer des autorisations d'utiliser de ressources spécifiques. Il s'avère donc plus que nécessaire de développer des systèmes d'authentification automatique capable de lutter contre les fraudes et d'assurer la sécurité dans différents domaines allant des plus emblématiques comme le passage dans les postes frontaliers internationaux au moins ardu comme l'accès aux informations personnelles. En revanche, les techniques d'authentification alors utilisées comme les mots de passe et les cartes d'identité ne sont pas à la hauteur des exigences de sécurité et des fonctions d'authentifications vitales comme la non-répudiation et la détection d'inscriptions multiples. En effet, les utilisateurs peuvent facilement être privés d'utiliser un service en prétendant que leurs mots de passe ont été volés ou devinés ou même oubliés. De plus, les fraudeurs peuvent aussi cacher leurs véritables identités en utilisant des duplicatas de documents d'identités falsifiés.

Cela implique qu'il devient très évident que ces mécanismes ne sont pas suffisants pour déterminer d'une manière fiable l'identité d'une personne et qu'un mécanisme plus solide pour l'identification basé sur quelque chose que vous êtes, à savoir la biométrie, est plus que nécessaire.

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques ou comportementales. C'est un terme dont on entend de plus en plus parler dans la vie de tous les jours. Il peut y avoir plusieurs types de caractéristiques physiques, certaines plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu.

Cependant, la biométrie n'est pas aussi récente qu'on croit. Son apparition remonte aux 19 siècles où les empreintes digitales ont été employées par la police judiciaire pour but d'identifier les personnes coupables d'avoir commis des crimes. Depuis, cette utilisation n'a jamais été abandonnée, et cette technique d'identification est toujours sollicité d'une maniéré plus automatisée.

Face aux nombreuses limitations imposées par l'utilisation des systèmes biométriques unimodaux, la biométrie multimodale s'impose de manière indéniable comme une alternative d'avenir dans le domaine de la sécurité des personnes et leurs biens. Bien que le couplage des systèmes biométriques peut être effectué à différents niveaux, la fusion au niveau des scores est la plus courante puisqu'il a été généralement prouvé qu'elle a été plus efficace que le reste des niveaux de fusion.

Dans cette thèse, nous nous intéressons tout particulièrement à la fusion au niveau des scores de données biométriques. La contribution majeure de cette thèse réside dans le développement d'une nouvelle approche basée sur la décomposition modale empirique pour la signature manuscrite ainsi qu'une approche structurelle basée sur l'extraction des minuties pour les empreintes digitales. Ces approches permettent de tenir compte des éventuelles interactions existant entre les systèmes biométriques unimodaux.

La fusion des scores a nécessité une normalisation préalable avant d'appliquer une fusion par la somme pondérée qui permet de séparer les scores imposteurs et les scores authentiques en les ramenant dans un intervalle commun avec des étendues proches. Les expérimentations ont été effectuées sur trois bases de données biométriques. Les résultats enregistrés montrent que la stratégie proposée donne des performances très encourageantes, en particulier en association avec la décomposition modale empirique (EMD).

Par ailleurs, cette thèse présente une étude sur la biométrie et la multimodalité. L'empreinte digitale et la signature manuscrite ont été particulièrement considérées. L'étude qui suit est organisée autour de cinq chapitres. Je commencerai par présenter au chapitre I, des généralités sur la biométrie. L'état de l'art sur la fusion de donnée sera examiné au chapitre II.

L'organisation générale du système proposé et la démarche adoptée seront développées ensuite. Le chapitre IV est destiné à la validation et à la concrétisation de la démarche adoptée en se basant sur un ensemble de données issues de trois bases de données : l'une réservée aux empreintes digitales, l'autre aux signatures manuscrites et une troisième bimodale qui contient les deux modalités considérées en même temps. Enfin, je présenterai au dernier chapitre les résultats expérimentaux obtenus.

Je terminerai ce travail par une conclusion et les perspectives qui sous-tendent notre travail ainsi que les horizons de recherches futures dans ce domaine.

Chapitre I

La Biométrie

I.1.Introduction

Devant la croissance exponentielle des communications tant physiques que virtuelles et les risques que cela peut représenter, il est apparu nécessaire de contrôler l'identité des acteurs de leurs échanges que ce soit pour garantir la sécurité des gens dans les lieux publics ou pour éviter le détournement ou le vol d'information sensible. La plupart de ces échanges exigent l'authentification de l'utilisateur afin de sécuriser les communications. Comme exemples de telles applications, citons l'achat en ligne, les transactions bancaires, l'e-Gouvernement, etc. On distingue deux manières classiques d'authentification de personnes. La première utilise une connaissance à priori comme un mot de passe. Il n'est pas rare qu'une personne ait à retenir plus d'une dizaine de codes d'accès dans son quotidien que dans son milieu professionnel et c'est souvent considéré comme frustrant pour l'utilisateur. La deuxième est basée sur une possession physique comme une carte à puce ou une clé. Ces deux méthodes présentent quelques inconvénients. En effet, le mot de passe peut être oublié ou espionné et la carte à puce ou la clé risque d'être volée ou perdue. En outre, ces deux méthodes ne s'avèrent pas efficaces pour distinguer entre un client authentique et un imposteur.

La biométrie s'impose de plus en plus comme alternative afin de remédier aux problèmes des méthodes précédentes. La biométrie est basée sur des caractéristiques propres à l'individu, qui ne peuvent n'être perdues. De plus, en pratique il n'est pas assez évident d'imiter une caractéristique biométrique. La biométrie permet de vérifier que l'usager est bien la personne qu'il prétend être. C'est une technologie qui utilise les caractéristiques physiques propres à chaque individu pour établir de façon aussi fiable que possible son identité. Jouissant actuellement d'un certain engouement dû, sans doute, aux différents gadgets d'identification que l'on a pu voir dans certaines productions cinématographiques, la biométrie tend à envahir notre quotidien. Devant cette déferlante, il était nécessaire de faire le

point sur ce qu'est exactement la biométrie, quelles techniques existent vraiment et leur degré de fiabilité.

Dans ce chapitre, nous nous initions aux principes de la biométrie, le fonctionnement d'un système biométrique, les modalités biométriques et leurs performances et les méthodes d'évaluation d'un système biométrique.

I.2. La biométrie

La biométrie est une technique naissante qui nous permet de vérifier l'identité d'un individu en employant un ou plusieurs de ses caractéristiques personnelles. Donc, la reconnaissance biométrique est basée sur ce qui est un individu. Il existe plusieurs appondus biométriques, les plus connues étant:

- **Biologiques:** comme le sang, la salive, l'urine, l'odeur ou encore l'ADN..etc. Ces méthodes sont difficiles à mettre en œuvre pour une utilisation courante.
- **Comportementales:** comme la signature, les frappes clavier, la démarche (le mouvement des hanches, des bras et des épaules)…etc.
- **Morphologiques:** comme les empreintes digitales, le visage, l'iris, la rétine ou la forme de la main...etc.
- **Cachée :** comme la géométrie du cerveau, ECG et la biométrie de la main sans contact...etc. Ces techniques biométriques sont en cours de développement**.**

Pour assurer leurs fiabilités, les modalités biométriques doivent être déterminées par quelques caractéristiques**.** Parmi les propriétés d'une modalité biométrique, on trouve :

- **Universelles** : mesurables sur chaque individu.
- **Uniques** : différents entre-deux individus.
- **Permanentes** : invariables dans le temps.
- **Mesurables** : non coûteuse et non intrusives.
- **Précises** : peu de confusion entre individus.
- **Difficilement reproductibles.**

Malheureusement, dans la pratique, on ne trouve pas toutes ces caractéristiques dans une même modalité.

Un système biométrique est donc un système automatique capable de reconnaitre une personne à travers ses caractéristiques propres : physiques, comportementaux. Dans ces systèmes, on peut procéder avec deux modes d'opération distincts : ceux basés sur la vérification et ceux basés sur l'identification.

En mode identification, le système cherche à établir l'identité de la personne qui a présenté ces données biométriques en entrée. En effet, il s'agit d'une comparaison du type "un contre plusieurs" où le système compare les données biométriques d'un individu à celles de tous les utilisateurs contenus dans sa base de données afin de déterminer l'identité proclamée.

Le mode vérification, également appelé authentification, consiste à confirmer ou infirmer l'identité d'un individu préalablement connu. Il s'agit donc d'une comparaison du type "un contre un". Dans ce cas, les données biométriques fournies aux systèmes sont comparées uniquement avec celle de la personne proclamée.

Il existe plusieurs modes distincts d'applications d'un système biométrique. Ces applications sont classées en trois catégories **[1],[2],[3],[4]**:

- Applications commerciales telles que l'authentification dans les réseaux informatiques, la sécurité électronique de données, le commerce électronique, l'accès internet, l'utilisation des cartes de crédit, le contrôle d'accès (physique, PC, téléphone mobile, PDA, etc.), la gestion des dossiers médicaux, l'enseignement à distance, etc.
- Applications gouvernementales telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle aux frontières, le contrôle des passeports, etc.
- Applications médico-légales telles que l'identification de cadavre, les enquêtes criminelles, la détermination de la parentalité, etc.

I.3. Les systèmes biométriques

Un système biométrique est essentiellement un système de reconnaissance de formes **[1]**. Il est principalement composé de deux phases essentielles : l'apprentissage (entraînement) et la comparaison. Dans la première phase, l'utilisateur est invité à fournir plusieurs échantillons (généralement entre 3 et 5) de la modalité biométrique au moyen d'un périphérique d'acquisition. Cette étape est généralement suivie d'une étape de prétraitement qui a pour but d'améliorer la qualité de la modalité acquise. Ensuite vient l'étape la plus crédible qui consiste à extraire les paramètres les plus pertinents de la modalité qui sont stockés dans une base de données. Enfin, dans l'étape de comparaison (reconnaissance), la même modalité de la personne, que l'on veut soit authentifier (vérifier), soit identifier, est capturée et les mêmes procédures sont effectuées. Si on est en mode identification, on compare les paramètres à tous ceux contenus dans la base. En cas de vérification, les paramètres sont comparés uniquement à ceux de la personne proclamée et la décision d'accepter ou de refuser l'authentification est annoncée par le système. La **Figure 1** montre le schéma bloc d'un système biométrique.

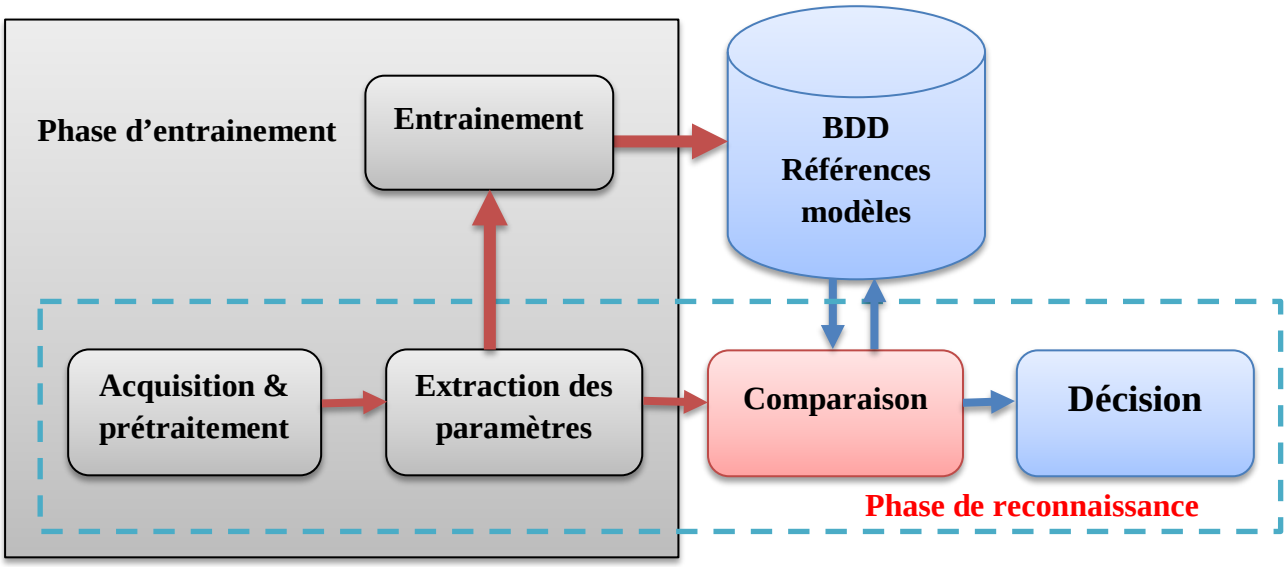


Figure I.1 : Schéma bloc d'un système de reconnaissance biométrique.

Dans la section suivante, nous présenterons brièvement quelques modalités biométriques couramment utilisées.

I.4. Les modalités biométriques

Il existe plusieurs modalités qui ont été utilisées dans divers systèmes biométriques. Dans cette section, nous allons mettre l'accent sur les modalités comportementales et morphologiques. Nous allons aussi introduire quelques modalités cachées qui sont en cours d'expansion. Dans la figure suivante, quelques modalités sont illustrées.

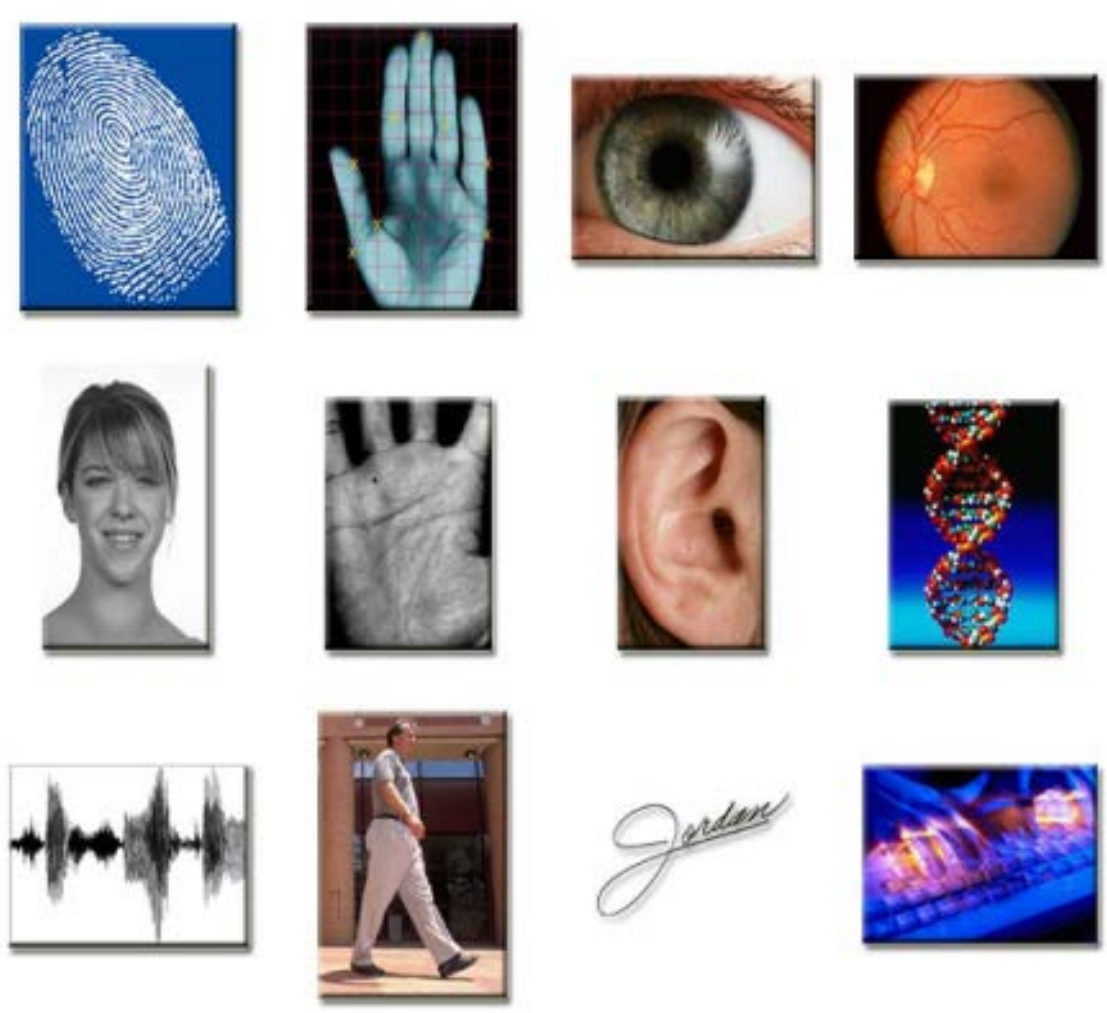


Figure I.2 : Quelques modalités biométriques

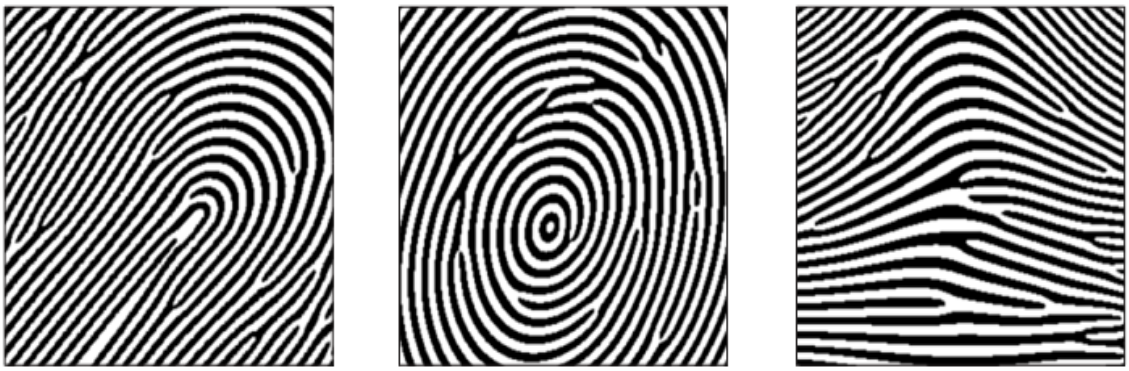
I.4.1.Modalités morphologiques

On peut définir une modalité morphologique comme une mesure de l'une des caractéristiques biologiques ou physiques d'un individu. Dans la suite, nous présenterons quelques modalités de ce type avec leurs modes d'utilisations :

I.4.1.1. L'empreinte digitale

L'utilisation de l'empreinte digitale comme moyen d'identification d'une personne n'est pas nouvelle. En fait, les corps policiers utilisent cette technique depuis plus de 100 ans. Aujourd'hui, les empreintes digitales sont recueillies sur une scène de crime et sont ensuite comparées à celles contenues dans un serveur central **[5]**.

Nous pouvons définir les empreintes comme suit : une empreinte digitale est une impression produite par la transpiration, la graisse, l'huile ou l'encre présente dans les lignes de crêtes non uniformes contenues dans la partie supérieure de chaque doigt de main d'un être humain. Ces empreintes sont uniques pour chaque individu. Même des jumeaux parfaits n'ont jamais des empreintes digitales identiques. Il en existe trois types : les arcs, les verticilles et les boucles comme montre la figure suivante.



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

Figure I.3: Les grandes familles d'empreintes : (a)Arche, (b) Boucle à droite, (c)Tourbillon.

Le recours à l'empreinte digitale compte pour plus du tiers du marché des procédés biométriques. Elle représente nettement la solution préférée des entreprises œuvrant dans ce domaine. La force de ce procédé tient au fait que l'utilisation de l'empreinte digitale est généralement plus facile à accepter par la communauté et qu'elle est l'une des modalités les plus efficaces et les moins coûteuses **[6]**.

I.4.1.2. L'iris

Elle est considérée comme la modalité la plus précise pour l'identification et l'authentification [7]. Son seul inconvénient est son coût assez élevé, ce qui la rend pas autant répondu pour des applications quotidiennes. Alors, son utilisation s'est limitée dans des endroits où la sécurité est primordiale et même critique comme dans les bases nucléaires par exemple. La reconnaissance par l'iris [8] est utilisée aussi dans le secteur financier pour les employés et les clients, dans les hôpitaux et dans les grands aéroports. Une personne voulant s'identifier place son œil à quelques centimètres du capteur et l'image de l'iris est prise par une caméra. Ensuite, les caractéristiques sont extraites de l'image de l'iris et comparées à celles enregistrées dans la base de données.

I.4.1.3. Le visage

La reconnaissance par cette modalité s'effectue de façon spontanée dans la vie quotidienne des êtres humains. L'authentification par le visage est la technique la plus commune et la plus populaire puisqu'elle correspond à ce que nous utilisons naturellement pour reconnaître une personne [9]. Les caractéristiques qui servent à la reconnaissance du visage sont : les yeux, la bouche, la forme du visage (contour), etc [10] .

Dans un système de reconnaissance faciale, la photo d'une personne est prise volontairement ou involontairement à l'aide d'une caméra. Puis, un ensemble de caractéristiques propres à chaque individu est extrait (le tour du visage, la position des oreilles, les coins de la bouche, l'écartement des yeux et la taille de la bouche) à partir de la photo. Ces systèmes sont capables de faire face aux techniques de *spoofing* [11] comme le port de lunettes, la barbe, le maquillage, etc.

I.4.1.4. La rétine

Cette technologie est bien adaptée aux applications de haute sécurité (sites militaires, salles de coffres forts, etc). Lors de l'acquisition, l'utilisateur place son œil à proximité du capteur où un rayon lumineux illumine le fond de l'œil pour extraire des points repères. La détermination des caractéristiques de la rétine consiste à l'extraction de la distribution géographique des vaisseaux sanguins [12]. Cette mesure peut ainsi fournir jusqu'à 400 points caractéristiques du sujet [13]. Cependant, la rétine n'est pas appropriée pour une grande

population à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques centimètres). En outre, des risques liés à la santé sont signalés, ce qui réduit l'utilisation de cette modalité.

I.4.1.5. La voix ou la parole

À travers cette modalité, on peut analyser et reconnaitre la voix humaine **[14]**. Elle est captée via un microphone afin de permettre la transcription sous forme d'un texte exploitable par la machine. Ensuite, plusieurs caractéristiques issues de cette modalité (comme la tonalité, la fréquence, l'harmonique, la vitesse et le rythme, etc.) sont extraites afin de les comparée à celles déjà stockés dans une base de données pour affirmer ou nier l'identité d'un locuteur **[15]**.

Cette modalité est employée dans de nombreuses applications, on peut citer les applications de dictée vocale sur ordinateur, des applications de criminalité par la police, par les agences d'espionnage et en téléphonie.

Mais cette modalité trouve des limitations à cause de la grande différence entre le langage formel, qui est compris et utilisé par les machines, et le langage naturel que les humains utilisent couramment. Le chalenge est donc de trouver un compromis entre ces deux langages.

I.4.1.6. La géométrie de la main

La biométrie par la reconnaissance de la géométrie de la main extrait près d'une centaine de paramètres comme les épaisseurs, les longueurs, les surfaces et les largeurs des doigts de la main **[16]**. L'acquisition de cette modalité ne nécessite aucune lecture d'empreintes et la mesure des épaisseurs des doigts s'effectue à l'aide de miroirs ce qui veut dire que l'acquisition s'effectue en trois dimensions. La taille du capteur est le major inconvénient de cette modalité. De plus, ce capteur coute très cher par rapport aux autres modalités. Tous ces inconvénients réduisent l'utilisation de cette technique biométrique.

I.4.2.Modalités comportementales

Il s'agit d'un type de biométrie caractérisé par un trait d'attitude qui est appris et acquis au fil du temps plutôt qu'une caractéristique physiologique. En conséquence, une

modalité comportementale peut changer avec le temps. Voici quelques exemples de ce type de modalités biométrique :

I.4.2.1. Dynamique de la frappe au clavier

La dynamique de la frappe au clavier est une caractéristique comportementale de l'individu. C'est en quelque sorte la transposition de la graphologie aux moyens électroniques.

Les paramètres suivants sont généralement pris en compte par les systèmes de reconnaissance de cette modalité : la vitesse de frappe, la suite de lettres, la mesure des temps de frappe, la pause entre chaque mot et la reconnaissance de mot(s) précis **[17]**.

La différence avec ces systèmes se situe plus au niveau de l'analyse, qui peut être soit statique et basée sur des réseaux neuronaux **[18],** soit dynamique et statistique (comparaison continuelle entre l'échantillon et la référence). Ces techniques sont assez satisfaisantes, mais restent néanmoins statistiques.

I.4.2.2. La démarche

La manière dont une personne marche peut la distinguer des autres. Dans un système de reconnaissance par cette modalité, on cherche à identifier un individu par sa façon de marcher et de bouger tout en analysant des images vidéo de la promenade du candidat **[19]**. Alors, c'est une modalité d'identification à distance. Les gens montrent de différents traits tout en marchant comme le maintien du corps, la distance entre les deux pieds, la position des joints tels que les genoux et les chevilles et les angles de balancement **[20]** ce qui aide de manière significative à les identifier.

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

I.4.2.3. La signature

La signature manuscrite est le moyen le plus accepté et le plus utilisé pour authentifier des documents. Les systèmes de vérification de signatures se rangent dans deux catégories selon le type d'acquisition des données : en ligne ou *online* **[21]** hors-ligne ou *offline* **[22]**. Les systèmes *online* traitent les signatures, qui sont produites à l'aide d'une tablette à digitaliser,

comme étant un signal dynamique et font l'extraction de plusieurs primitives comme les points de pauses, la pression, la direction, la vitesse pendant la signature et l'angle d'inclinaison. Ces caractéristiques dynamiques sont spécifiques à chaque individu parce qu'il pourrait être facile de reproduire l'aspect graphique de la signature, mais il n'est jamais évident d'imiter la signature avec le même comportement que la personne montre tout en signant. .

En revanche, les systèmes *offline* traitent la signature à partir d'une image provenant d'un scanner. Ces systèmes sont assez complexes dû à l'absence de caractéristiques dynamiques stables. La difficulté se situe également dans le fait qu'il est difficile de caractériser l'allure de la signature.

I.4.3.Modalités cachée

Ces modalités sont un concept biométrique particulièrement robuste. En comparaison aux modalités biométriques classiques qui sont à la base des caractéristiques évidentes de l'être humain, les modalités cachées considèrent plutôt les caractéristiques intrinsèques et non visibles du corps humain **[23].** N'importe quel signal physiologique ou organe humain est potentiellement un candidat pour des applications biométriques **[24]**. Dans la première catégorie, nous pouvons employer l'électrocardiogramme (ECG), l'électromyogramme. (EMG). Dans la deuxième catégorie, nous pouvons considérer, comme exemple, la morphologie ou la texture du cerveau humain. Voici quelques exemples de ces modalités :

I.4.3.1. Electrocardiogramme ECG

L'ECG est un signal représentant l'activité du cœur. Il est principalement employé dans des applications cliniques pour diagnostiquer les maladies cardio-vasculaires. Le signal d'ECG est caractérisé par la forme de ses battements composés de cinq vagues typiques, à savoir P, Q, R, S, et T ou parfois la vague U (**Figure I.4**) .

La biométrie par ECG a fait l'objet d'un certain nombre de travaux **[25], [26]** et **[27]**. L'utilisation de l'ECG en biométrie est relativement nouvelle. En fait, il existe plusieurs méthodes biométriques basées sur l'ECG. Il y a des approches qui sont basées sur l'analyse de l'ECG **[28]**. D'autres basées sur l'intégration des caractéristiques analytiques et d'apparence extraite des signaux ECG **[29]**.

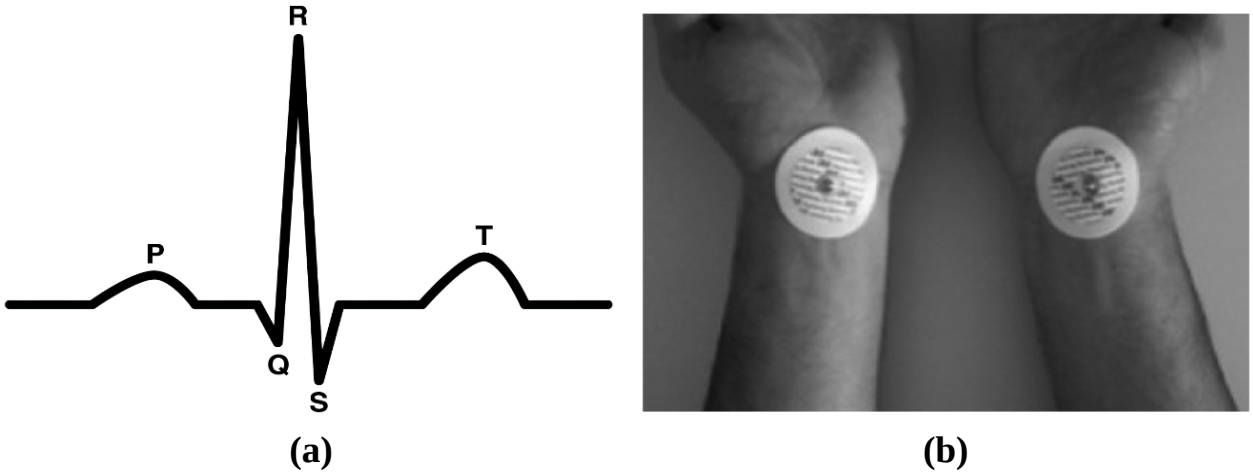


Figure I.4:Biométrie par ECG : (a) Signal d'ECG avec le rythme régulier (b) positionnement des électrodes sur les avant-bras pour la capture d'ECG

I.4.3.2. Electromyogrammes EMG

Les signaux électromyogrammes (EMG) sont des signaux bioélectriques enregistrés au niveau des muscles. Ils fournissent des informations diverses sur l'état des nerfs périphériques.

Le signal d'EMG a plusieurs applications cliniques. Son utilisation en tant que modalité biométrique cachée peut être particulièrement intéressante. Dans ce contexte, quelques expériences récentes ont été réalisées **[23],[24]** et **[29]**. En particulier, ces travaux ont mis l'accent sur l'analysé des signaux électromyographie de surface (SEMG) **[30]**. Lors de l'acquisition de ces signaux, les individus sont invités à appliquer une pression manuelle d'une intensité constante sur une sonde de force pendant plusieurs secondes (**Figure I.5**). Le signal ainsi obtenu est analysé dans le domaine spectral. Puis, des paramètres sont extraits comme la puissance du signal, la fréquence moyenne, le coefficient d'aplatissement et le coefficient de dissymétrie. En effet, ces paramètres fournissent un vecteur de dispositif que nous pouvons employer pour caractériser des individus.

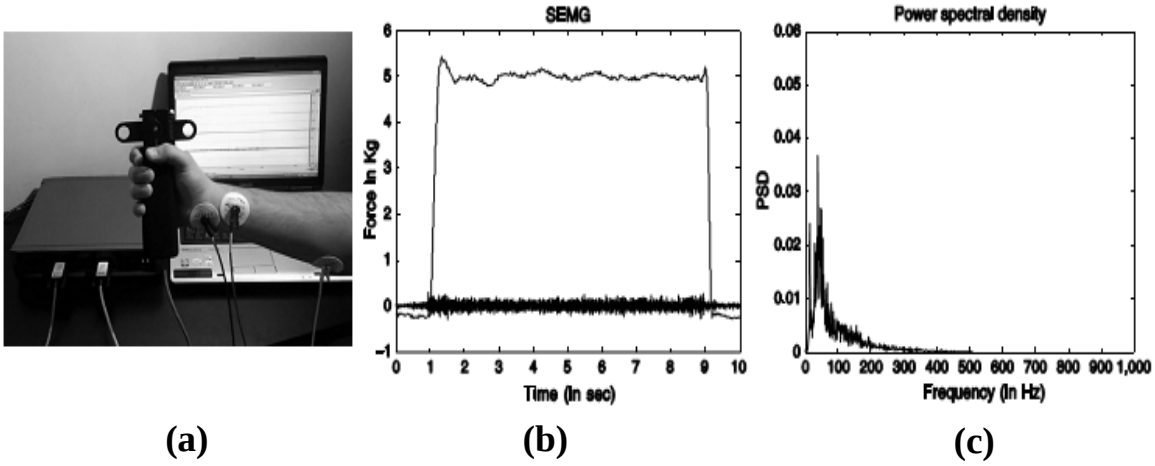


Figure I.5: Biométrie par l'EMG : (a) Acquisition d'un signal EMG (b) L'intensité appliquée par l'utilisateur et l'EMG relatif (c) périodogramme d'EMG [31]

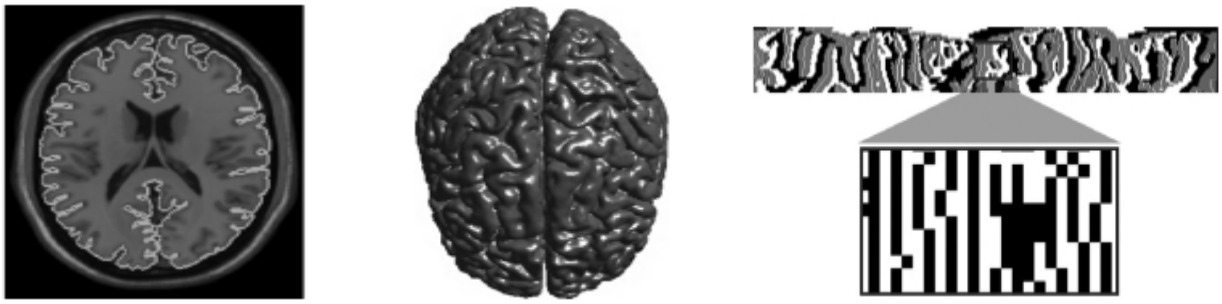
I.4.3.3. Biométrie du cerveau avec des images IRM

Dans des applications médicales, l'IRM (imagerie par résonance magnétique) est une technique de formation image non envahissante employée pour visualiser des images en 2D ou 3D des organes du corps humain (par exemple cerveau, muscles, et cœur) avec une résolution relativement élevée. Ceci est rendu possible avec l'utilisation d'un champ électromagnétique puissant et constant, produit par un supraconducteur.

La Biométrie par le cerveau **[32]** cherche à caractériser le cerveau humain à travers des images IRM 2D et 3D **[33]**. Depuis les images IRM 2D (**Figure I.6.a**) , on peut faire la reconstruction en 3D (**Figure I.6.b**) du cerveau pour avoir des informations sur la texture. Ainsi d'autres caractéristiques géométriques du cerveau peuvent être considérées comme le rapport isopérimètre et la courbure extérieure corticale.

En fait, la quantité de paramètres qui peuvent être extraits à partir d'une image du cerveau 3D est plus grande que ce que nous pouvons extraire à partir d'autres modalités classiques. On peut aussi définir ce qu'on appelle *brain code* ou code du cerveau à travers une segmentation de la zone d'intérêt du cerveau (**Figure I.6.c**) **[34].**

L'avantage principal de ce type de modalité cachée est le fait que le cerveau est totalement protégé contre toutes sortes de changements. Il est difficile d'imaginer qu'un individu modifie la structure de son propre cerveau pour usurper l'identité d'un autre individu. Cependant, l'inconvénient principal de cette modalité est la non-disponibilité de systèmes d'IRM robuste consacrés à la biométrie.



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

Figure I.6: Biométrie du cerveau avec des images IRM : (a) Extraction des textures de cerveau par segmentation (b) reconstruction de 3D d'image de cerveau montrant les circonvolutions qui peuvent être employées pour identifier des individus (c) extraction du *Brain Code* [31]

I.4.3.4. Biométrie avec des images de rayon X

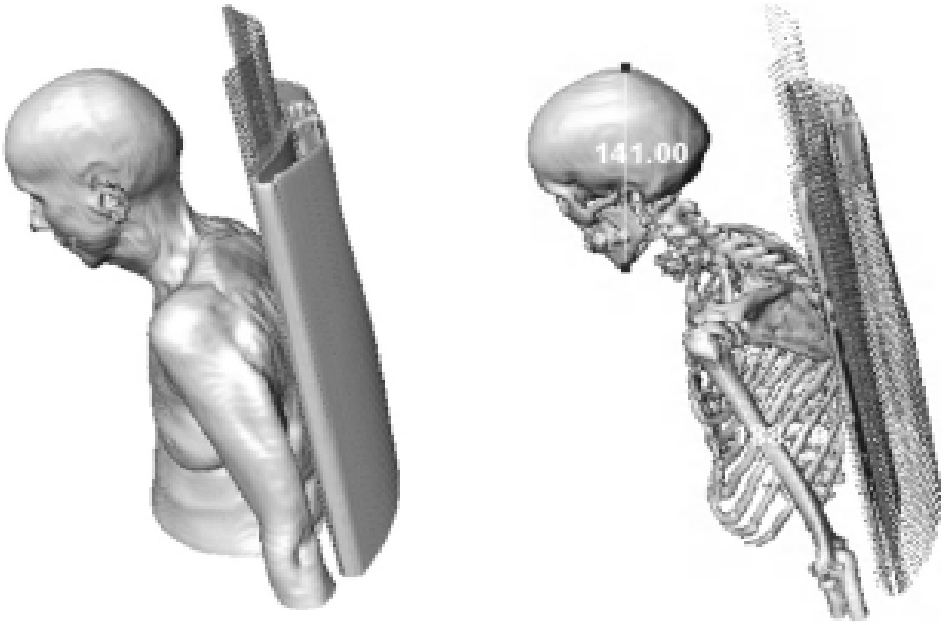
La radiographie est une technique d'imagerie de transmission par rayons X. Elle permet d'obtenir un cliché dont le contraste dépend à la fois de l'épaisseur et du coefficient d'atténuation des structures traversées. La radiographie est utilisée en radiologie médicale, en radiologie industrielle et en radiothérapie.

La radiographie médicale permet le développement d'images en 2D des os humain. Avec ce type d'images, des structures d'os sont clairement accentuées.

L'application de ce type de technologie dans la biométrie est envisageable en exploitant des images radiographiques de la main par exemple (**Figure I.7**) où le but est de caractériser les phalanges à l'aide de quelques outils de traitement d'images **[23]**.

Figure I.7: Biométrie de la main avec des images à rayon X.

Basée sur les idées ci-dessus, une prolongation en 3D peut être considérée afin de visualiser la totalité d'un squelette humain (**Figure I.8**) cela va permettre l'application de la biométrie cachée sur n'importe quel os. Mais l'utilisation de ces technologies trouve des reproches dus à certaines contraintes, à savoir le risque sanitaire potentiel d'un côté et le respect de l'intimité des personnes d'un autre.



(a) **(b)**

Figure I.8: Biométrie cachée du corps humain employant les rayons X : (a) image reconstruite du corps humain obtenu à l'aide d'un scanner à rayon X (b) extraction du squelette [31]

I.5. Comparaison entre les modalités biométrique

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

Dans la **Figure I.9**, on a effectué un classement des différentes modalités biométriques selon deux axes : la performance et le coût. Les systèmes à base de la voix ou du visage ne sont pas couteux, mais leurs performances restent limites. Les modalités de la biométrie cachée sont incontestablement les modalités les plus performantes. En revanche, les systèmes à base de ces modalités sont très coûteux à cause du prix élevé des dispositifs d'acquisition.

L'empreinte et la signature manuscrite représentent un compromis en matière de performance. C'est l'une des raisons pour laquelle on a choisi ces modalités dans notre système.

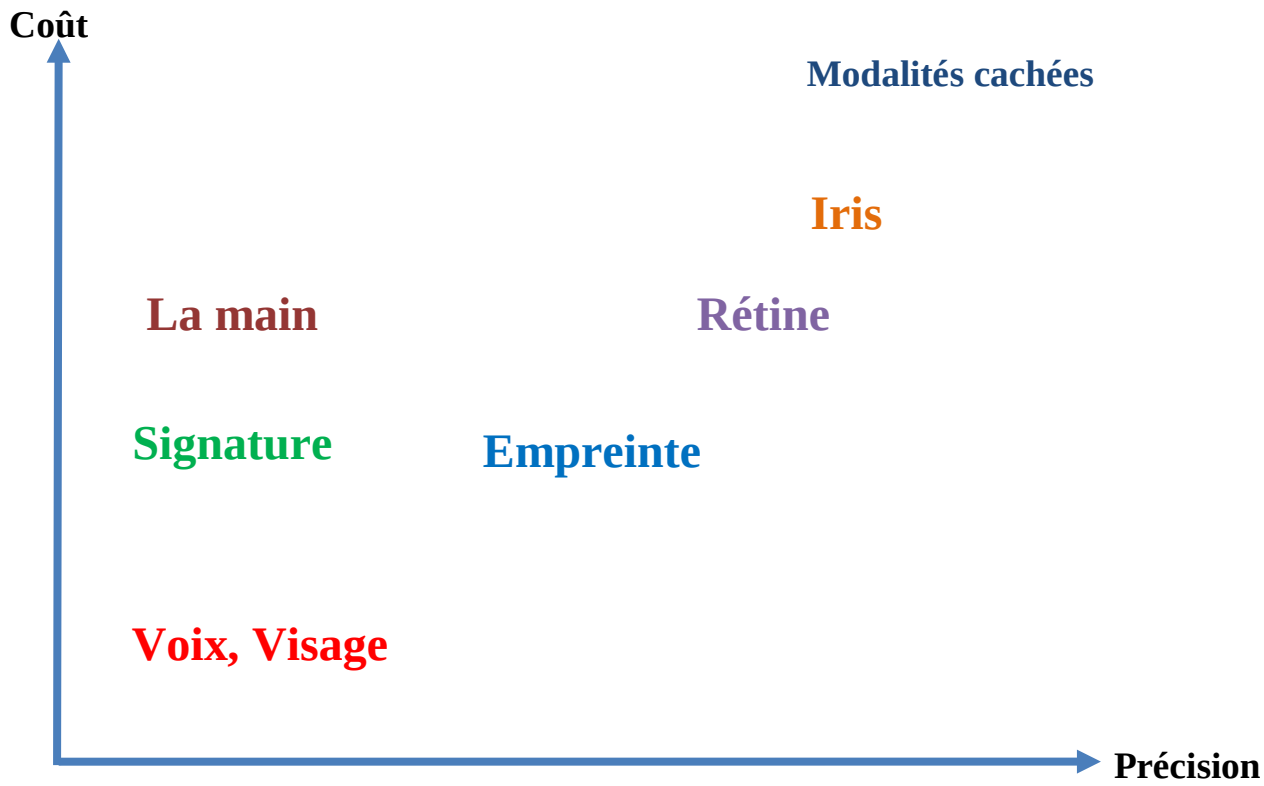


Figure I.9: Classement des modalités biométriques selon le coût et la précision

Ainsi, dans le tableau suivant, en plus de la précision de chaque modalité, on a ajouté d'autres paramètres de comparaison qui sont la simplicité d'utilisation et l'acceptation par l'utilisateur. La simplicité d'utilisation peut être définie comme étant la quantité d'énergie fournie par un individu pour être reconnue par un système. L'acquisition de certaines modalités ne nécessite parfois aucun effort de l'utilisateur (visage, empreinte…). Pour d'autres modalités, la tâche se complique de façon significative. L'acquisition de l'iris ou du cerveau par exemple est très délicate, car ça nécessite des positions bien précises. En conséquence, ça nécessite un effort considérable de l'utilisateur.

L'acceptation d'une modalité par un utilisateur est liée à des paramètres sociaux, psychologiques et parfois sanitaires. La signature par exemple est une pratique quotidienne, c'est pourquoi elle est la plus acceptée des modalités biométriques. Quant à l'iris, les gens hésitent toujours à l'utiliser à cause du laser qui traverse l'œil et qui peut provoquer des problèmes de santé. Les modalités cachées ont aussi du mal à être acceptées à cause de forts risques sanitaires qui peuvent être engendrés par leurs utilisations.

Type	Modalité	Précision	Simplicité d'utilisation	Acceptation par l'utilisateur
Morphologique	Empreinte	Haute	Moyenne	basse
	Iris	Haute	Moyenne	moyenne
	Rétine	Haute	Basse	basse
	visage	Basse	Haute	haute
	Voix	Moyenne	Haute	haute
	Géométrie de la main	Moyenne	Haute	moyenne
Comportementale	Frappe au clavier	Basse	Haute	moyenne
	Démarche	Basse	Moyenne	moyenne
	signature	Moyenne	Moyenne	haute
Cachée	ECG, EMG	Haute	Moyenne	Moyenne
	Cerveau	Haute	Basse	Basse
	Imagerie par rayons X	Haute	Basse	Basse

Tableau I.1: Comparaison entre les modalités biométriques en matière de simplicité et acceptabilité.

I.6. Performances des systèmes biométriques

L'évaluation des systèmes biométriques est un enjeu majeur en biométrie pour plusieurs raisons. Premièrement, elle donne accès aux chercheurs pour mieux tester et évaluer leurs systèmes avec ceux qui existent dans la littérature. En conséquence, elle permet de prendre en considération le comportement des utilisateurs durant le processus d'évaluation. De plus, elle permet d'identifier, pour chaque système, les applications industrielles en se basant sur ces performances.

Ces derniers dépendent de plusieurs circonstances de test incluant le capteur utilisé, le protocole d'acquisition, la disposition de la personne, le nombre d'utilisateurs, le nombre d'échantillons par utilisateur, le profil démographique des utilisateurs, l'habitude des utilisateurs et les laps de temps séparant l'acquisition, etc. **[1]**.

Afin de permettre aux chercheurs d'évaluer leurs systèmes biométriques ainsi que la comparaison entre les différents systèmes, la communauté scientifique a mis à disposition plusieurs bases de données des différentes modalités biométriques. Certaines de ces bases de données contiennent une seule modalité alors que d'autres sont multimodales. Le **tableau I.2** **[34]** résume les caractéristiques de certaines bases multimodales.

En biométrie, nous sommes en face de deux populations: les véritables clients (*Genuine*) qui sont dûment autorisés à pénétrer dans la zone protégée et les imposteurs (*Imposters*) qui n'ont aucune autorisation, mais qui vont quand même essayer de rentrer.

Le résultat issu d'un système biométrique est un score de similarité compris dans l'intervalle [0,1]. En effet, plus le score est proche d'un, plus le système est sûr de l'identité proclamée. Plus le score est proche de 0, moins le système est confiant en vers l'identité proclamée. La décision du système est arbitrée par un seuil ***t***: les échantillons biométriques qui génèrent des scores supérieurs à ***t*** sont appariés et la conclusion d'appartenance à la même personne est prise. En revanche, les échantillons qui génèrent des scores inférieurs à ***t*** sont non appariés entraînant la conclusion qu'ils proviennent de deux personnes différentes.

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

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

Tableau I.2 : Quelques bases de données biométriques multimodales et leurs caractéristiques [34].

Dans la littérature, Il existe plusieurs métriques et plusieurs types de courbes **[35-38]** pour définir les performances d'un système biométrique, voici quelques-uns les plus utilisées :

- **Taux de fausses acceptations (*false acceptance rate*, FAR)** : ce taux détermine la probabilité pour qu'un système reconnaisse une personne qui normalement n'aurait pas dû être reconnue. C'est un ratio entre le nombre de personnes qui ont été acceptées alors qu'elles n'auraient pas dû l'être et le nombre total de personnes non autorisées qui ont tenté de se faire accepter.

- **Taux de faux rejets (*false rejection rate*, FRR)** : ce taux détermine la probabilité pour qu'un système ne reconnaisse pas une personne qui normalement aurait dû être reconnue. C'est un ratio entre le nombre de personnes légitimes dont l'accès a été refusé et le nombre total de personnes légitimes s'étant présentées.
- **Taux d'égale erreur (Equal Error Rate, EER)** : Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où FRR = FAR, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

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

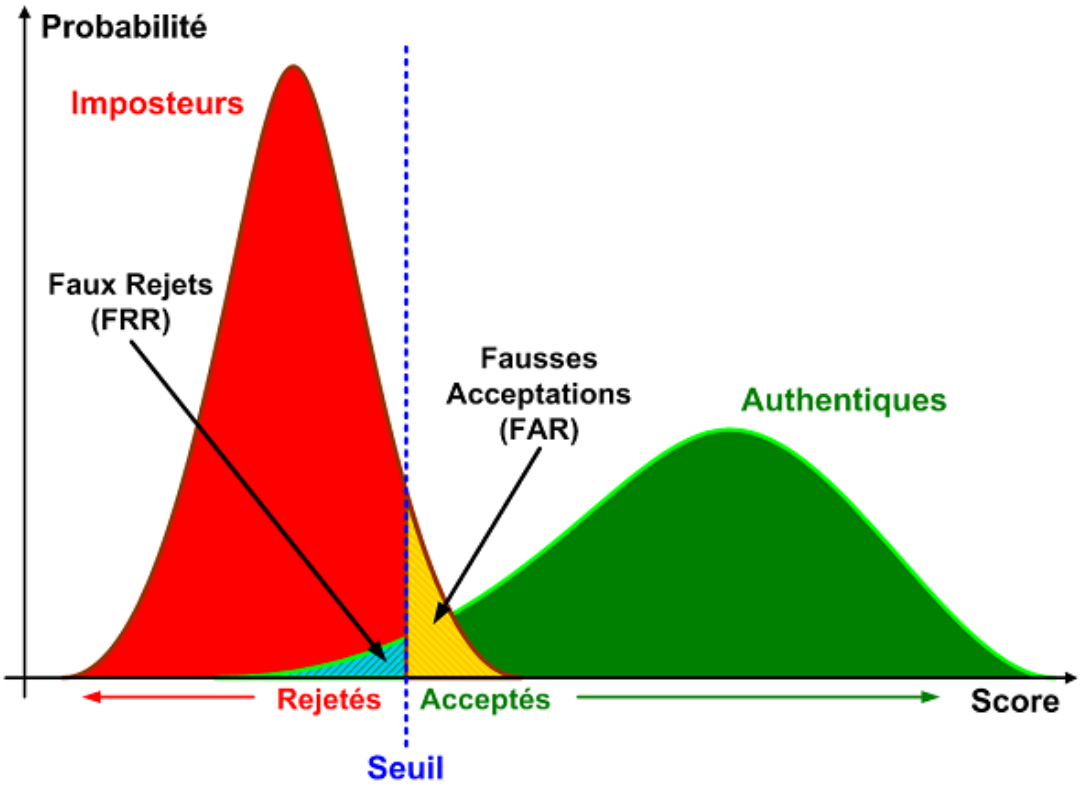


Figure I.10. Illustration du FRR et du FAR.

À présent, nous allons définir deux types de courbes de performances :

- **La courbe ROC (Receiver Operating Characteristics)** : Cette courbe représente en ordonnée la proportion de tests positifs parmi les utilisateurs authentique (la sensibilité) en fonction de la proportion de tests positifs parmi les imposteurs (complément de la spécificité ou 1 – spécificité, en abscisse) pour toutes les valeurs

des seuils de test envisageables. Pour pouvoir déterminer la validité d'un test à travers cette courbe, il est nécessaire de calculer la surface située sous la courbe ROC appelée AUC (***Area Under the Curve***). Plusieurs méthodes ont été proposées dans **[39]** pour estimer l'AUC. Ainsi, quand le test est parfaitement discriminant, la surface sous la courbe (AUC) vaut 1 mais cela n'est jamais réalisable. En réalité, plus l'AUC est grande, plus l'algorithme est performant. La **Figure I.11** illustre un exemple de la courbe ROC :

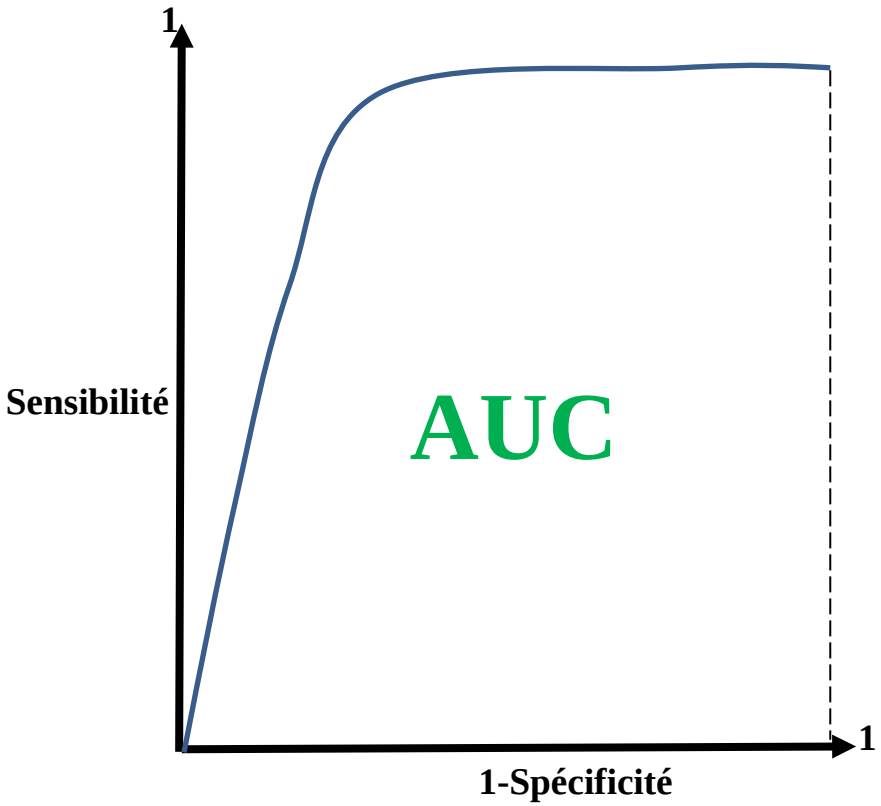


Figure I.11. Exemple d'une courbe ROC.

- **La courbe DET** (***Detection error tradeoff***) : Cette courbe illustre la relation entre le FRR et le FAR. Elle est obtenue en faisant varier le seuil de décision et en calculant à chaque fois les deux valeurs FRR et FAR. La **Figure I.12** illustre un exemple de la courbe DET.

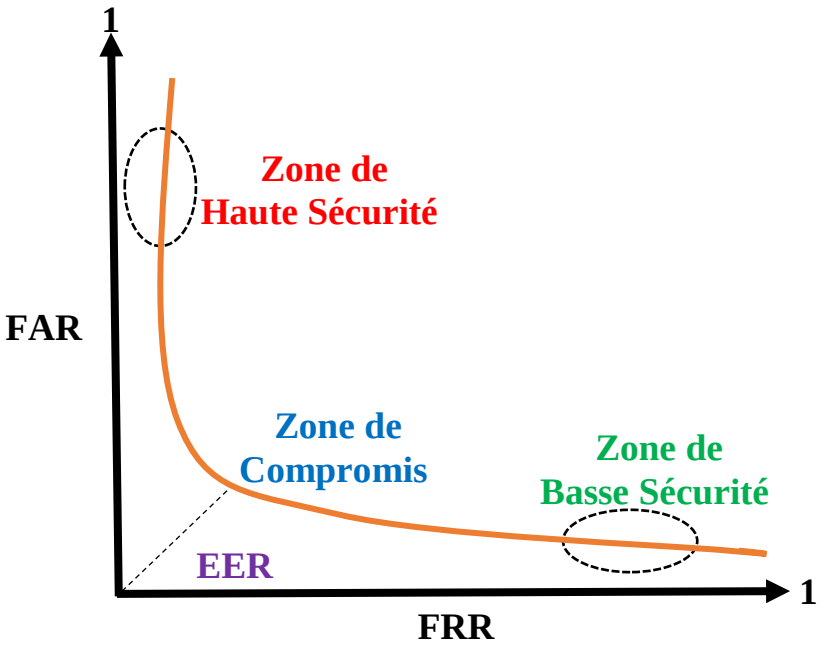


Figure I.12. Exemple d'une courbe DET.

I.7. Conclusion

La biométrie s'impose de plus en plus comme un outil de reconnaissance d'individu dans diverses applications. Elle gagne sa place comme le moyen numéro un d'authentification. Cependant, un certain nombre de défis, comme les attaques contre les systèmes biométriques, restent à surmonter. Malgré cela, l'avenir de la biométrie est prometteur pour l'authentification et l'identification des personnes. Dans ce chapitre nous avons vu l'émergence des méthodes de reconnaissance biométriques et des problèmes qui en découlent. Les caractéristiques des modalités biométriques ainsi que leurs avantages et inconvénients ont été décrits dans ce chapitre. De plus, on a défini les différentes techniques utilisées pour l'évaluation de ces systèmes où on a pu affirmer que le taux de faux rejets ou de fausses acceptations sont des indicateurs de performances permettant l'adaptation de l'application au contexte d'utilisation de la modalité biométrique et que le degré de sécurité d'un système biométrique peut être adapté à l'utilisation attendue du système. D'autre part, l'efficacité d'une modalité particulière dépend de sa pertinence vis-à-vis de l'application visée. La combinaison (fusion) entre plusieurs modalités dans la même application permet d'augmenter la fiabilité du système. Le chapitre suivant est dédié à la présentation des différents concepts liés à la fusion de données.

Chapitre II

Etat de l'art sur la fusion de données

II.1 Introduction

L'implémentation du raisonnement humain sur une machine occupe depuis de nombreuses années une place importante dans le domaine scientifique. Les premières approches d'automatisation du raisonnement reposent sur l'imitation du comportement humain par la machine dans le but du traitement de l'information. Ces approches ont donné naissance au terme d'intelligence artificielle ou l'Interaction Homme Machine (IHM) **[41]**.

D'après **[42]**, la fusion de données est un procédé relativement récent dans la littérature scientifique. Bien que ce concept est utilisé depuis toujours en nature par les animaux et les êtres humains. La fusion multi-sources a été initialement développée surtout pour des applications militaires afin d'atteindre des objectifs tels que la localisation des cibles ennemies, la fusion d'images radar et l'autonomie de véhicules mobiles, etc. Les systèmes employés reposent sur des techniques diverses issues de domaines variés tels que le traitement du signal, l'intelligence artificielle, l'estimation stochastique, la reconnaissance de formes et la classification, etc. De façon générale, la fusion de données est une opération d'intégration de plusieurs données en vue d'en extraire une nouvelle information plus représentative de l'ensemble des données.

En biométrie, associé une modalité à un système biométrique unimodale, c'est ajouter une nouvelle source d'information. C'est pour cette raison que les systèmes multimodaux permettent d'obtenir de meilleures performances en comparaison aux systèmes unimodaux. L'ajout des modalités permet également d'augmenter l'universalité du système, car si l'utilisateur est réfractaire à une caractéristique biométrique donnée, l'information récoltée sur les autres modalités peut compenser la faible qualité de l'acquisition. La fusion biométrique est possible à plusieurs niveaux : aux deux premiers niveaux, elle consiste souvent en une normalisation des données suivie d'une concaténation **[43]**. Au niveau de la comparaison, elle se traduit par une combinaison des

scores. Enfin, au niveau de la décision, elle consiste en une confrontation des résultats de classification qui aboutit à une décision finale **[44]**. Dans ce qui suit, nous traitons la question de la fusion et ses différents niveaux. Les principales méthodes de normalisation des scores, de fusion par combinaison et classification sont étudiées. On s'intéresse particulièrement à la fusion des scores qui fait l'objet de notre travail.

II.2 Intérêt de la fusion de données

La fusion de données est un sujet de plus en plus actuel, car susceptible d'aider efficacement les scientifiques à extraire des informations de plus en plus pertinentes et précises. La fusion de données offre de nombreux avantages **[45]** :

- Robustesse et fiabilité : le système est opérationnel même si une ou plusieurs sources d'informations sont défectueuses.
- Augmentation de la couverture spatiale et temporelle de l'information et des déductions.
- Accroissement du nombre de dimensions de l'espace des observations, menant à un accroissement de la qualité des déductions, et à une réduction de la vulnérabilité du système.
- Réduction de l'ambiguïté des déductions : des informations plus complètes ou plus précises permettent un meilleur choix entre les différentes hypothèses.
- Apport d'une solution à l'explosion de la quantité d'informations disponibles aujourd'hui.

II.3 Les types de fusion

Il existe plusieurs types de scénarios de fusion de traits biométriques **(Figure II.1)** qui dépend essentiellement du type de sources et de caractéristiques utilisées :

- **Systèmes multi-algorithmes:** C'est le plus classique des types. L'extraction des caractéristiques s'effectue par le biais de différents algorithmes avant l'étape de fusion. Par exemple, on peut associer deux algorithmes pour traiter la même image d'empreinte digitale, l'un qui analyse la texture tandis que l'autre fait l'extraction des minuties. Dans ce cas, l'utilisation d'un seul capteur est largement suffisante.

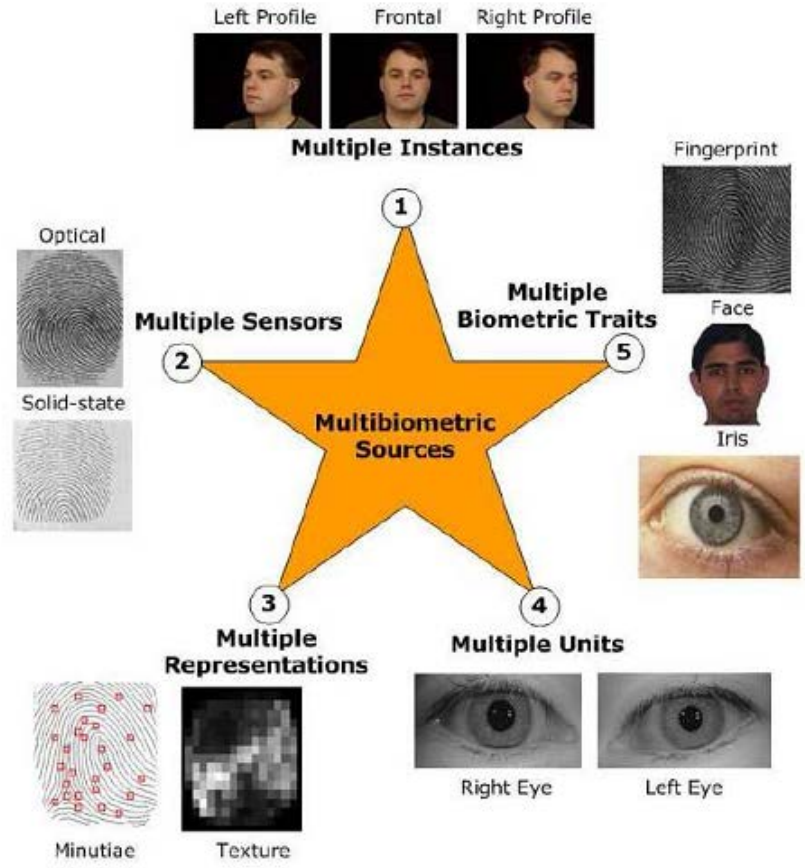


Figure II.1 Les différents types de fusion de traits biométriques [46].

- **Systèmes multi-échantillons:** dans ce type, on effectue plusieurs captures d'une même modalité à l'aide du même dispositif d'acquisition dans le but d'enrichir le modèle biométrique d'une personne. On peut citer par exemple, l'acquisition du profil frontal du visage d'une personne ainsi que les profils gauches et droits afin de tenir compte des variations de la pose faciale.

- **Systèmes multicapteurs:** les systèmes de ce type font appel à plusieurs capteurs afin d'acquérir le même caractère biométrique sous différents angles. Ainsi l'acquisition d'une image 2d d'un visage se fait à l'aide d'une caméra classique alors que la même acquisition en 3D s'effectue avec une autre caméra plus sophistiquée. Ce type de système peut intervenir notamment lors de la fusion au niveau capteur.

- **Systèmes multi-instances:** à travers ce type de système, on peut faire l'acquisition du même caractère biométrique sur plusieurs intervalles temporaux. Le but ici est de considérer la variation inter personnelle du de la modalité biométrique. L'acquisition de plusieurs empreintes digitales via le même capteur est l'exemple typique de ce type de système.

- **Systèmes multicaractères ou multimodaux:** ce type de système combine différentes modalités biométriques d'un individu. Cette combinaison fournit une nette amélioration de la performance d'un système. Ces systèmes nécessitent différents capteurs ainsi que des algorithmes dédiés à chaque modalité biométrique. Ce type de système a comme principale caractéristique que les caractères biométriques considérés peuvent être plus décorrélés que pour les systèmes multicapteurs. Un tour d'horizon de nombreux systèmes biométriques multimodaux développés peut être trouvé dans **[47]**.

II.4 Stratégies de fusion des systèmes multimodaux

Comme nous avons déjà énoncé, les systèmes multimodaux combinent plusieurs modalités biométriques. En conséquence, ces systèmes ont besoin donc d'effectuer l'acquisition et le traitement de plusieurs données. L'acquisition et le traitement peuvent se faire successivement, on parle alors d'architecture en série, ou simultanément, on parle alors d'architecture en parallèle.

Les stratégies ou architectures de fusion décrivent l'ensemble des sources, la manière dont elles sont assemblées et les techniques mathématiques ou statistiques pour le traitement.

La multiplication des travaux sur la fusion dans les différents domaines (imagerie, intelligence artificielle et reconnaissance de formes, etc.) a entraîné la mise au point de nombreux schémas traitant les données de manières différentes. Les stratégies de fusion proposées peuvent être regroupées en trois approches principales : séquentielle **[48-50]** parallèle **[51-55]** et hybride **[56-58]**.

Si l'acquisition et le traitement se font de façon successive, on parle alors d'architecture séquentielle ou en série (**Figure II.2**).

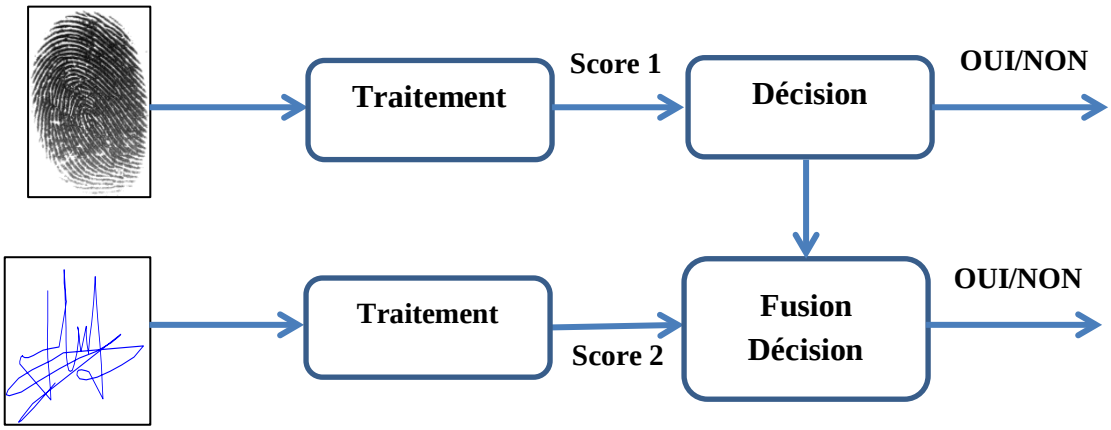


Figure II.2 Architecture de fusion en série.

Si l'acquisition et le traitement se font simultanément, on parle alors d'architecture en parallèle (**Figure II.3**).

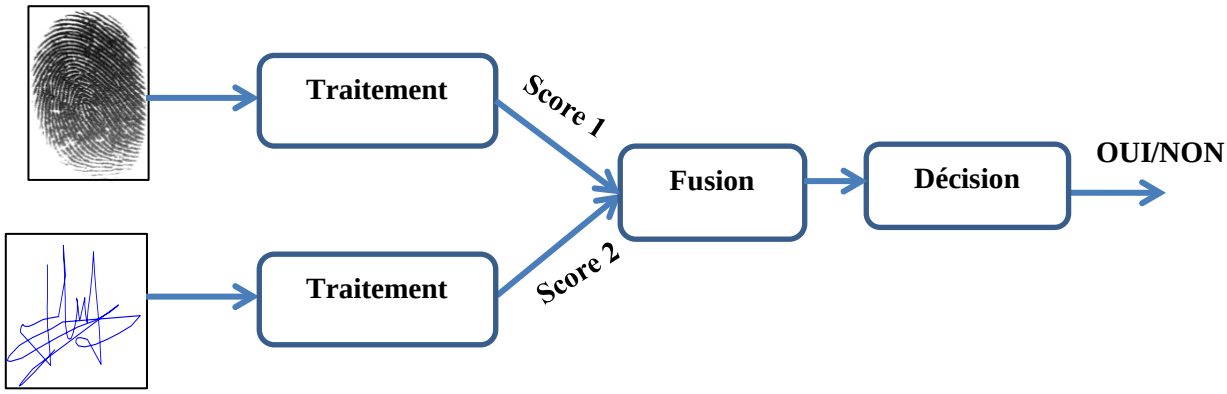


Figure II.3 Architecture de fusion en parallèle.

Généralement, l'acquisition des données biométriques s'effectue séquentiellement pour des raisons purement pratiques par ce qu'il est difficile d'acquérir en même temps une signature et une image d'iris dans de bonnes conditions.

Cependant, on peut être confronté à des cas où les acquisitions doivent être faites simultanément lorsque les différentes données utilisent le même capteur par exemple les capteurs d'empreintes multi doigts qui permettent d'acquérir plusieurs doigts simultanément

ou même les empreintes palmaires. L'architecture est donc en général liée au traitement et en particulier à la décision.

La différence entre un système multimodal en série et un autre en parallèle réside dans le fait qu'à l'issue du premier on obtient un score de similarité de chaque acquisition tandis que le deuxième système procède à l'ensemble des acquisitions avant de prendre une décision.

Actuellement, l'architecture en parallèle est la plus utilisée, car elle permet d'utiliser toutes les informations disponibles et donc d'améliorer les performances du système. En revanche, l'architecture en série peut être privilégiée dans certaines applications , par exemple si la multi modalité est utilisée pour donner une alternative pour les personnes qui ne peuvent pas utilisées une modalité quelconque.

II.5 Les niveaux de fusion

Un système de fusion est généralement composé de sources d'information, de moyens d'acquisition d'information, de moyens de communication et de capacités à traiter l'information. Il peut être par conséquent très complexe. Il est fréquent et pratique, lors de l'étude ou de la présentation d'un système, de séparer les aspects topologiques et les aspects traitement d'informations, même s'il existe des interconnexions. La topologie a une influence importante sur le choix de l'architecture du système de fusion, sur les choix d'outils, des méthodes de traitement et de communication.

On peut trouver dans la littérature plusieurs manières de classer les différentes étapes ou types de fusion. Cette différence provient principalement du niveau où l'opération de fusion est accomplie, de l'objectif de cette opération, du type de sources (ou capteurs) et de l'application considérée **[59]**.

La combinaison de plusieurs systèmes biométriques peut se faire à quatre niveaux différents : au niveau des données, au niveau des caractéristiques extraites, au niveau des scores issus du module de comparaison ou au niveau des décisions du module de décision (**Figure II.4**).

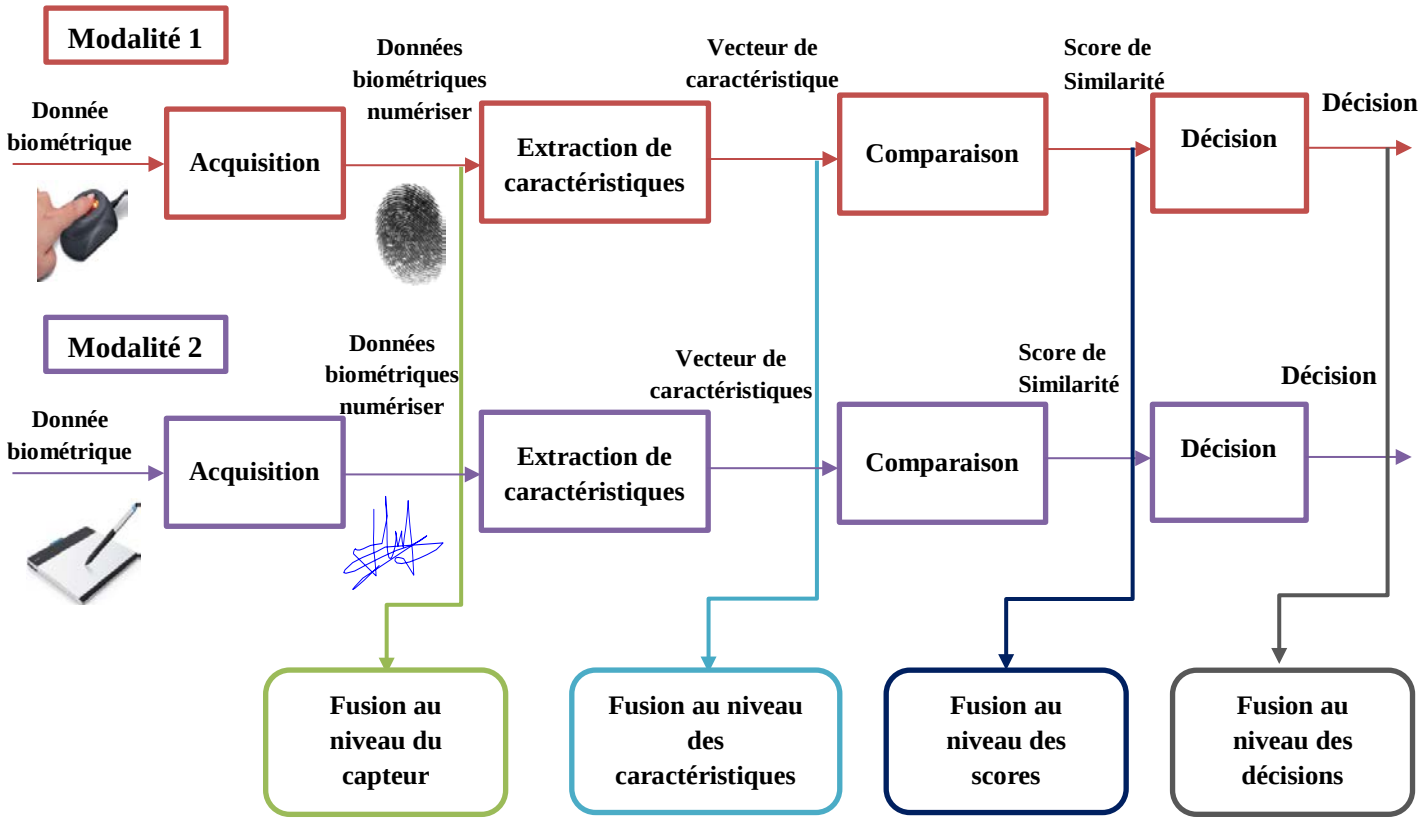


Figure II.4 Les différents niveaux de fusion

Ces quatre niveaux de fusion peuvent être classés en deux grandes familles :

- La fusion pré-classification (avant comparaison),
- La fusion post-classification (après la comparaison).

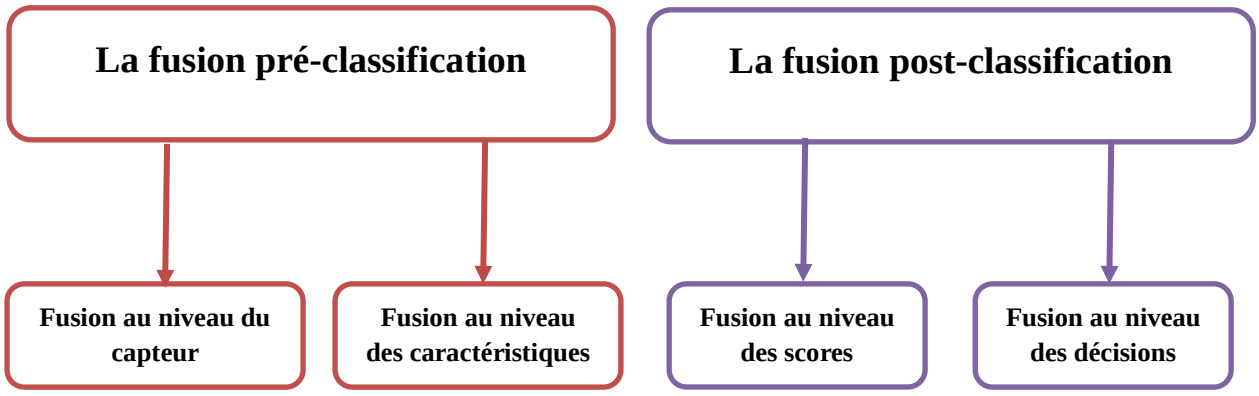


Figure II.5 Les familles des niveaux de fusion

II.5.1 La fusion pré-classification

La fusion pré-classification correspond à la fusion des informations issues de plusieurs données biométriques au niveau du capteur ou au niveau des caractéristiques extraites par le module d'extraction de caractéristiques.

II.5.1.1 Fusion au niveau du capteur (*Sensor Level*) : Les systèmes biométriques multi capteur prélèvent le même exemple d'une modalité biométrique avec deux capteurs distinctement différents **[60]**. Le traitement des échantillons capturés peut se faire avec un ou plusieurs algorithmes. Comme exemple de ce niveau, on peut citer l'emploi d'une caméra de lumière visible et une caméra infrarouge pour l'identification du visage. Un autre exemple de fusion au niveau capteur consiste à mettre en mosaïque plusieurs images d'empreintes digitales afin de former une image d'empreinte digitale finale plus complexe. La fusion au niveau capteur est relativement peu utilisée, car les captures doivent être compatibles entre elles et la correspondance entre les points dans les données brutes doit être connue par avance.

II.5.1.2 Fusion au niveau des caractéristiques (*Feature Level*): La fusion au niveau caractéristique est très utile à la classification **[60]**. Ce niveau de fusion concerne la combinaison d'informations extraites après diverses phases de traitement et d'analyse des mesures. Différents vecteurs de caractéristiques, issues de plusieurs capteurs ou obtenus à l'aide de différents algorithmes d'extraction sont combinés **[61]**. On peut trouver un exemple de ce niveau de fusion dans **[62]** où les auteurs proposent une méthode de fusion de caractéristiques pour de la fusion du visage et de l'empreinte palmaire. La fusion est effectuée par concaténation d'images obtenues par transformée de Gabor sur les images du visage et l'empreinte de la main.

Les méthodes de fusion pré-classification sont assez peu utilisées, car elles posent un certain nombre de contraintes qui ne peuvent être remplies que dans certaines applications très spécifiques. En revanche, la fusion post-classification est la plus prometteuse pour les chercheurs.

II.5.2 La fusion post-classification

La fusion post-classification peut se faire au niveau des scores issus des modules de comparaison ou au niveau des décisions. Dans les deux cas, la fusion est en fait un problème bien connu dans la littérature sous le nom de "*Multiple Classifier systems*".

II.5.2.1 Fusion au niveau des décisions (*Decision Level*) : avec cette approche, chaque sous-système biométrique effectue de façon autonome les étapes d'extraction des caractéristiques, comparaison et reconnaissance **[63]**. Ensuite, chaque système fournit une décision binaire sous la forme OUI ou NON que l'on peut représenter par 0 et 1, et le système de fusion de décisions consiste à prendre une décision finale en fonction de cette série de 0 et de 1. Les méthodes les plus utilisées sont les fonctions booléennes. Dans **[64]** un grand nombre de méthodes de fusion de décision sont présentées. La fusion au niveau des décisions est souvent utilisée en raison de sa simplicité.

II.5.2.2 Fusion au niveau score (*Score Level*) : La fusion au niveau des scores est le type de fusion le plus utilisé, car elle peut être appliquée à tous les types de systèmes. D'ailleurs c'est le type de niveau de fusion utilisée dans notre travail. Dans ce type de niveau, on effectue une combinaison des scores fournis par les différents systèmes **[65]**. La fusion de scores consiste donc à la classification : OUI ou NON pour la décision finale d'un vecteur de nombres réels dont la dimension est égale au nombre des sous-systèmes. Il existe un grand nombre de méthodes de fusion de scores que nous allons les présenter dans ce qui suit.

II.6 Les méthodes de fusion

Dans cette section, nous allons maintenant nous intéresser particulièrement aux méthodes de fusion de scores. Comme on a déjà énoncé, les méthodes de fusion de scores focalisent sur la combinaison des informations au niveau des scores issus des modules de comparaison comme indiqué sur la **Figure II.6**. Un système de fusion est constitué essentiellement de deux modules, un module de fusion et un module de décision. Alors on est en face d'un problème de classification à 2 classes (OUI ou NON, Client ou Imposteur) à partir d'un vecteur de nombre réel dont la dimension est égale au nombre des sous-systèmes du système multi-algorithmes.

Il existe deux approches pour combiner les scores obtenus par différents systèmes. La première approche consiste à aborder le sujet comme un problème de combinaison, tandis que l'autre approche l'abord comme un problème de classification. Il est important d'affirmer que les auteurs de **[66]** ont démontré que les approches par combinaison sont plus performantes que la plupart des méthodes de classification. Dans ce qui va suivre, nous allons faire un tour d'horizon des différentes méthodes de fusion en scores de chaque catégorie.

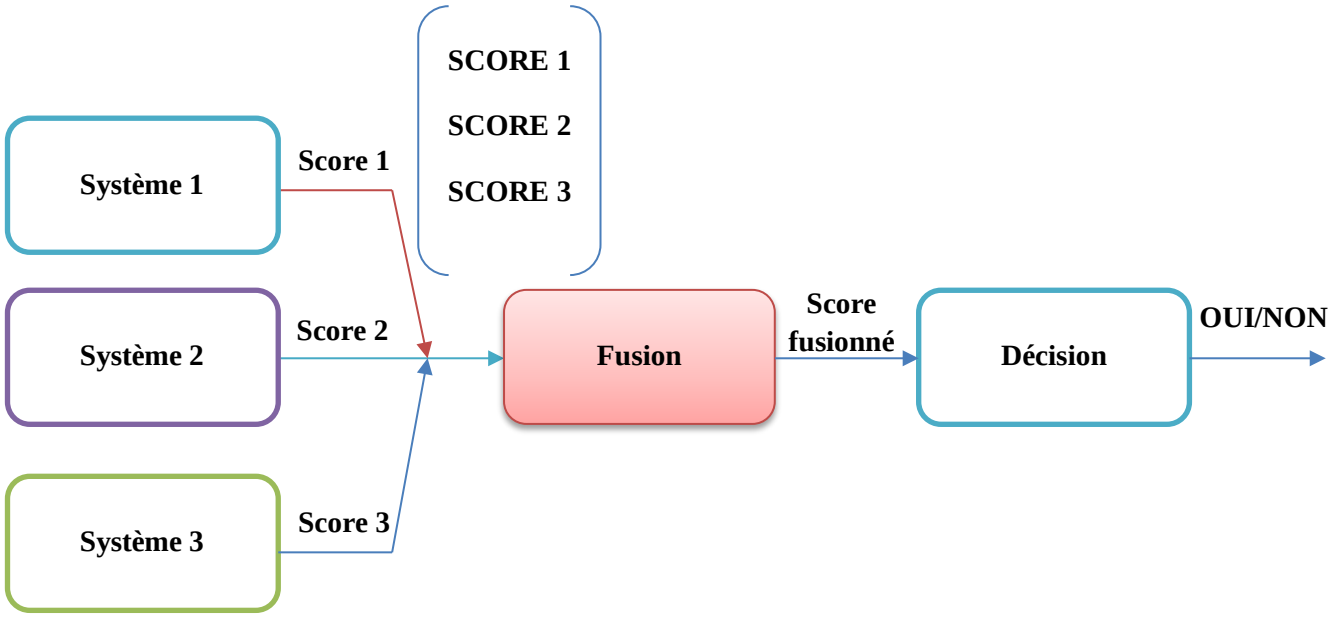


Figure II.6 Principe de la fusion en scores

II.6.1. Méthodes de fusion par combinaison de scores

Les méthodes de cette catégorie font la fusion de scores par des méthodes mathématiques de combinaison. Les scores individuels sont combinés de manière à former un unique score qui est ensuite utilisé pour prendre la décision finale. Afin de s'assurer que la combinaison des scores provenant de différents systèmes soit cohérente, les scores doivent subir une phase de normalisation **[67]**. On va présenter les méthodes de normalisation de scores avant de se tourner vers l'illustration des méthodes de cette catégorie.

La normalisation des scores a pour but de transformer les scores de chaque signature pour les rendre homogènes avant de les combiner. En effet, les scores provenant de chaque système peuvent être de nature différente (scores de similarité, scores de distances ….). Autrement dit, une étape de normalisation est généralement nécessaire avant que les scores bruts provenant de différents classificateurs puissent être combinés dans l'étape de fusion. La normalisation aborde le problème des scores incomparables représentant les sorties des différents classificateurs biométriques. Nous présentons dans la suite, les trois méthodes de normalisation les plus connues en occurrence la méthode Min-Max, la méthode Z-score et la méthode TanH **[68]**:

- **Normalisation par la méthode Min-Max :** Cette méthode normalise les scores bruts tout en conservant leurs distributions à un facteur d'échelle près et transforme tous les scores dans l'intervalle [0,1] selon :

$$E_{iNorm} = \frac{E_i - E_{\max}}{E_{\max} - E_{\min}} \quad \textbf{(II.1)}$$

- **Normalisation par la méthode Z-score :** Cette méthode transforme les scores en une distribution avec une moyenne égale à 0 et un écart type égal à 1 selon :

$$E_{iNorm} = \frac{E_i - \mu}{\sigma} \quad \textbf{(II.2).}$$

Où μ est la moyenne arithmétique et σ l'écart-type des données.

- **Normalisation par la méthode tangente hyperbolique Tanh:** Cette méthode est parmi les techniques statistiques les plus solides. Elle met chaque score normalisé dans l'intervalle [0, 1] selon :

$$E_{iNorm} = 0.5[Tanh(0.01\frac{E_i - \mu}{\sigma}) + 1] \quad \textbf{(II.3).}$$

Où μ est la moyenne arithmétique et σ l'écart-type des données.

Après avoir introduit les techniques de normalisation les plus utilisées, nous allons maintenant nous consacrer à la présentation des méthodes de fusion par combinaisons des scores. Ces dernières peuvent être divisées en deux catégories : les méthodes simples et les méthodes utilisant la logique floue.

II.6.1.1 Méthode de combinaisons simples

Les méthodes de combinaisons de scores simples sont des méthodes basées sur un fondement théorique très simples et qui ont pour objectif de ressortir un score ***S*** à partir des ***N*** scores disponibles issus de *N* systèmes. Les méthodes les plus utilisées sont la moyenne, le produit, le minimum, le maximum, la médiane et la somme pondérée.

- La combinaison des scores par la moyenne se fait selon la relation suivante :

$$S = \frac{1}{N}\sum_{i=1}^{N} S_i \quad \textbf{(II.4).}$$

- La combinaison des scores par le produit se fait selon la relation suivante :

$$S = \prod_{i=1}^{N} S_i \quad \textbf{(II.5).}$$

- La combinaison des scores par le minimum se fait selon la relation suivante :

$$S = Min(S_i) \quad \textbf{(II.6).}$$

- La combinaison des scores par le maximum se fait selon la relation suivante :

$$S = Max(S_i) \quad \textbf{(II.7).}$$

- La combinaison des scores par la médiane se fait selon la relation suivante :

$$S = Med(S_i) \quad \textbf{(II.8).}$$

- La somme pondérée est la technique la plus évoluée de cette catégorie qui nécessite une adaptation par le réglage de paramètres appelés poids.

$$S = \sum_{i=1}^{N} \omega_i S_i \quad \textbf{(II.9).}$$

La somme pondérée permet de donner des poids différents ω_i à chacun des systèmes en fonction de leurs performances individuelles ou de leurs intérêts dans le système multi algorithmes. Nous allons développer en détail les concepts et l'utilisation de cette méthode un peu plus tard dans le chapitre IV.

II.6.1.2 Méthode de combinaisons par logique flou

La théorie de la logique floue (des sous-ensembles flous) fut proposée par Zadeh **[69]** afin d'épauler la logique binaire d'une part et d'améliorer la logique multivolume d'autre part. Contrairement à la logique binaire qui est très proche du langage machine, la logique floue converge vers le raisonnement humain qui se base sur l'intégration et le traitement du caractère approximatif. Dans **[70]** les auteurs ont employés l'intégration floue de Choquet pour réaliser deux méthodes de fusion : la première consiste à combiner des images des traits du visage (yeux, nez et la bouche) et des images globales de visage tandis que la deuxième approche fait l'agrégation des classificateurs opérants sur quatre ensembles de sous-images générées par décomposition en ondelettes.

- **Mesure floue :** Un jeu de fonction g : P(**Y**) → [0, 1] est appelée une mesure floue si les conditions suivantes sont remplies :

1. conditions aux limites: $g(\phi) = 0$, $g(\mathbf{Y}) = 1$

2. monotonie : $g(A) \leq g(B)$, si $A \subset B$ et $A, B \in P(\mathbf{Y})$

3. continuité : $\lim_{x \to \infty} g(A_i) = g(\lim_{x \to \infty} A_i)$, si{Ai} est une suite croissante d'ensembles mesurable

À partir de cette définition, Sugeno **[71]** a défini une gλ mesure floue qui est livrée avec une propriété supplémentaire comme suit :

$$g(AB) = g(A) + g(B) + \lambda g(A) g(B) \quad \textbf{(II.10).}$$

Pour tous les A, B $\subset$ Y et A $\cap$ B = ϕ, et pour certains $\lambda > -1$. Évidemment quand λ=0, le gλ mesure floue devient une mesure de probabilité standard. En général, la valeur de $\boldsymbol{\lambda}$ peut être déterminée en raison de l'état limite de la mesure floue gλ. Cette condition pour g(Y) = 1. Par conséquent, la valeur de λ est déterminée par la résolution de ce qui suit:

$$g\lambda(Y) = \frac{1}{\lambda}\left(\prod_{i=1}^{n}(1 + \lambda g^{i}) - 1\right), \lambda \neq 0 \quad \textbf{(II.11).}$$

Est équivalant à :

$$\lambda + 1 = \left(\prod_{i=1}^{n}(1 + \lambda g^{i}) - 1\right) \quad \textbf{(II.12).}$$

Où $\lambda \in (-1, +\infty)$, $\lambda \neq 0$, et g_i est la valeur de la fonction de densité floue. La solution peut être facilement obtenue; évidemment on s'intéresse à la racine supérieure à -1.

- **Intégrale floue**

L'intégrale floue de la fonction h calculée sur Y par rapport à une mesure floue g est définie sous la forme

$$\int_{Y} h(y) \circ g(.) = \sup_{\alpha \in [0,1]} \left[\min\left[\alpha, g(\{y \mid h(y) \geq \alpha\})\right]\right] \quad \textbf{(II.13).}$$

- **L'intégrale de Sugeno**

Lorsque les valeurs des h(.) sont classées dans l'ordre décroissant, $h(y_1) \geq h(y_2) \geq \ldots \geq h(y_n)$

L'intégrale floue de Sugeno est calculée comme suit:

$$\int_{Y} h(y) \circ g(.) = \max_{i=1:n}\left[\min(h(y_i), g(A_i))\right] \quad \textbf{(II.14).}$$

Où Ai = $\{y_1, y_2, \ldots, y_i\}$ désigne un sous-ensemble d'éléments. Les valeurs de $g(A_i)$ pris en charge par la mesure floue sur les sous-ensembles correspondants peuvent être déterminées de manière récursive sous la forme :

$$g(A_1) = g(y_1) = g^1 \quad \textbf{(II.15).}$$

$$g(A_i) = g^i + g(A_i - 1) + \lambda g^i g(A_{i-1}) \quad \textbf{(II.16).}$$

Le calcul de la fonction de densité floue g_i sur la base des données est assurée de la manière suivante :

$$\begin{cases} g^i = \beta p_i, i = 1 \\ g(A_i) = g^i + g(A_i - 1) + \lambda g^i g(A_{i-1}), i = 2,3,4 \end{cases} \quad \textbf{(II.17).}$$

Où p_i est le taux de classification dans l'intervalle [0, 1] pour chaque système. $\beta \in [0, 1]$ est un facteur qui met en place un certain équilibre entre les résultats de la classification.

- **L'intégrale de Choquet**

  Il a été démontré que l'équation de l'intégrale flou **(II.13)** n'est pas une extension correcte de l'intégration de Lebesgue habituelle. Autrement dit, lorsque la mesure est addition l'expression ci-dessus ne retourne pas l'intégrale au sens de Lebesgue. Afin de remédier à cet inconvénient, Murofushi et Sugeno **[72]** ont proposé une soi-disant intégrante floue de Choquet calculé de la manière suivante:

  $$\int_Y h(y) d\ g(.) = \sum_{i=1}^{n} [h(y_i) - h(y_{i+1})] g(A_i) h(y_{n+1}) = 0 \quad \textbf{(II.18).}$$

Shukla et al **[73]** proposent de plus amples explications sur la combinaison de scores par logique floue à base de l'intégrale de Sugeno ou de Choquet.

II.6.2. Méthodes de fusion par classification de scores

Les approches de fusion par classification de scores considèrent l'opération de fusion comme étant un problème de classification. Elles cherchent à prendre une décision à partir du vecteur des scores de dimension ***N***. Le but des méthodes de fusion basées sur des classifieurs est d'effectuer une discrimination entre les deux classes (Client et Imposteur) dans l'espace à ***N*** dimensions des scores. La discrimination entre ces deux peut être plus ou moins complexe selon la nature du classifieur utilisé. Toutefois, les méthodes classiques de classification utilisées en reconnaissance des formes et en apprentissage automatique peuvent être utilisées pour la fusion

de scores de ce type. A noter que ces méthodes sont moins performantes que leurs antécédents (les méthodes fusion par combinaisons) à cause de leurs complexités. Dans le domaine des systèmes biométriques multimodaux, plusieurs types de méthode de classification ont été employés. Nous allons développer quelques-uns les plus utilisées :

II.6.2.1 Fusion par méthode des machines à vecteurs de support (SVM : *Support Vector Machine*)

Les machines à vecteurs de support (SVM pour "*Support Vector Machines*") sont des classificateurs binaires qui permettent de séparer deux distributions de classes dans l'espace de représentation à l'aide d'un hyperplan afin de maximiser la *marge* de séparation. Pour un ensemble d'échantillons $\{(x_1, y_1), \ldots, (x_n, y_n)\}$ à deux classes $y_i = \{\pm 1\}$, le problème consiste à trouver un hyperplan tel que :

- Les données des étiquettes de classe +1 et -1 se trouvent de chaque côté de l'hyperplan.
- La distance des vecteurs les plus proches de l'hyperplan (pour chacune des deux classes) est maximale.

  Ces vecteurs sont appelés vecteurs de support et la distance de ceux-ci par rapport à l'hyperplan constitue la marge optimale.

D'une façon plus formelle, l'objectif de cette méthode est de trouver un hyperplan $wx + b$, $w \in \mathrm{R}$ et $b \in \mathrm{R}$ qui sépare les deux classes avec la plus grande marge. La recherche de la marge optimale permettant de déterminer les paramètres w et b de l'hyperplan conduit à un problème d'optimisation quadratique qui consiste (dans le cadre général) à minimiser :

$$[\|w\|^2 + C\sum_i \xi_i \mid y_i(w.\varphi(x_i) + b) \geq 1 - \xi_i,\ \xi_i \geq 0] \qquad \textbf{(II.18).}$$

Où **C** représente un paramètre de compromis entre la marge et les erreurs, ξ_i représente un variable ressort associé à l'observation x_i, et φ est une transformation (**Figure II.7**).

Le problème peut être résolu (entre autres) par la méthode Lagrangienne d'optimisation quadratique avec contraintes (formulation duale) pour maximiser la marge **[74]** :

$$\{\sum_i \alpha_i - \frac{1}{2}\sum_{i,j} \alpha_i \alpha_j y_i y_j K(x_i, x_j) \mid 0 \leq \alpha_i \leq C, \sum_i \alpha_i y_i = 0\} \qquad \textbf{(II.19).}$$

Où α_i est le multiplicateur Lagrangien associé au vecteur x_i. Si la valeur de α_i est non-nul alors x_i est un vecteur de support et $K(xi, xj) = \varphi(x_i)\varphi(x_j)$ est le noyau de transformation.

Le noyau d'un SVM est une fonction symétrique définie positive qui permet de projeter les données dans un espace transformé de grande dimension dans lequel s'opère plus facilement la séparation des classes (**Figure II.7**). Parmi les noyaux les plus utilisés, nous avons :

- Le noyau linéaire : $K(x_i, x_j) = x_i.x_j$ (**Figure II.7.a**)
- Le noyau gaussien : $K(x_i, x_j) = exp^{(-\frac{\|x_i - x_j\|^2}{2\sigma^2})}$ (**Figure II.7.b**)
- Le noyau polynomial : $K(x_i, x_j) = (ux_ix_j + v)^p$ (**Figure II.7.c**)

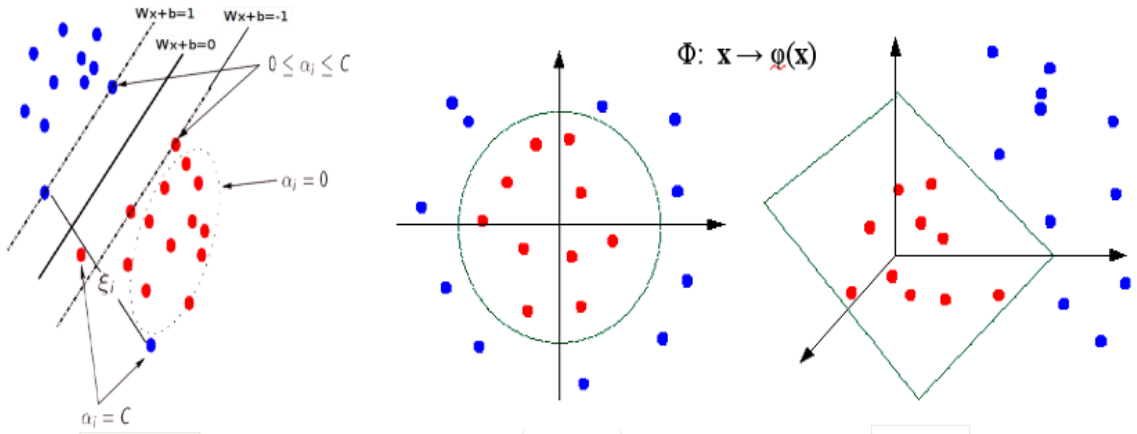


Figure II.7. Principe de l'SVM : (a) SVM avec un noyau linéaire(b) SVM avec un noyau gaussien (c) SVM avec un noyau polynomial

La décision est obtenue selon (le signe de) la fonction :

$$f(x) = sign\ [\sum_{i,j} \alpha_i y_i K(x_i, x) + b] \qquad \textbf{(II.20).}$$

La fusion de donnée avec la méthode SVM a été employée dans plusieurs travaux **[75,76,77,78]**.

II.6.2.2 Fusion par méthode des réseaux de neurones

Le principe général des Réseaux de Neurones Artificiels (RNA) est à l'origine inspiré de certaines fonctions de base des neurones naturels du cerveau. Un réseau de neurones artificiel est généralement constitué de plusieurs couches :

- **Une couche d'entrée** : retransmets les inputs sans distorsion.
- **Des couches intermédiaires appelées couches cachées :** transformation non linéaire xi → φ(xi) des entrées. Ces couches permettent de discriminer des classes d'objets non linéairement
- séparables.
- **Une couche de sortie** : transformation linéaire φ(xi) → yi des fonctions cachées. Pour un problème de classification, on aura autant de sorties que de classes et chaque sortie est interprétée comme une probabilité a posteriori.

Il existe deux types de réseaux de neurones : monocouches et multicouches. Les réseaux monocouches ont été rapidement écartés, car ils ne sont capables de séparer ni les classes non linéairement séparables ni les multi-classes. Les réseaux multicouches se présentent comme une solution efficace face à ces problèmes grâce à leurs propriétés d'approximation universelle **[79]**, qui leurs rendent capable d'approcher une fonction quelconque avec une précision arbitraire. La figure suivante montre un exemple d'un réseau de neurones avec trois entrées, trois couches cachées et deux sorties. Les fonctions d'activation peuvent être quelconques, et le nombre de neurones en sortie dépend généralement du codage adopté. Par exemple, si on est face à un problème de discrimination, chacun d'eux est généralement dédié à une classe donnée.

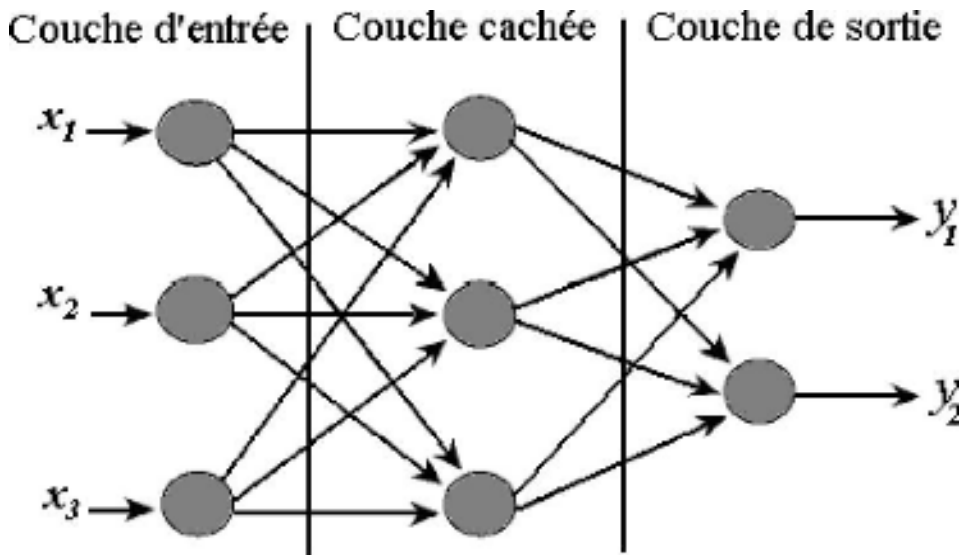


Figure II.8. Exemple d'un réseau de neurones

Les réseaux de neurones peuvent prendre le rôle d'un pure classifieur où leurs utilités résident dans leurs capacités d'apprentissage automatique ce qui leurs permet de résoudre des problèmes sans avoir besoin d'employer des règles complexes, tout en étant tolérant aux erreurs. Mais, on peut aussi les considérées pour réaliser la fusion de données **[80]** pour séparer deux populations données, à savoir les clients et les imposteurs dans notre cas.

II.6.2.3 Fusion par méthode de l'analyse discriminante linéaire (*Linear Discriminant Analysis* LDA)

L'analyse Discriminante Linéaire est utilisée pour trouver la combinaison linéaire des caractéristiques qui séparent le mieux les classes d'objet ou d'événement. Les combinaisons résultantes peuvent être employées comme classificateur linéaire, ou généralement dans la réduction de caractéristiques.

La LDA est une technique qui cherche les directions qui sont efficaces pour la discrimination entre les données. La **Figure II.9** représente un exemple de classification de deux nuages de points. L'axe principal de la LDA est l'axe de projection qui maximise la séparation entre les deux classes. Il est clair que cette projection est optimale pour la séparation des deux classes. Concrètement, pour tous les échantillons de toutes les classes, on définit deux mesures. La première mesure est la matrice de dispersion intra-classes S_w (*within-class scatter matrix*) qui est définie par :

$$S_w = \sum_{i=1}^{L} \frac{1}{n_i} \sum_{j=1}^{n_i} (x_j^i - m^i)(x_j^i - m^i)^T \qquad \textbf{(II.21).}$$

Avec x_j^i est le $j^{\text{ème}}$ échantillon de la classe i, m^i la moyenne de la classe i, L le nombre de classes et ni le nombre d'échantillons de la classe i.

La deuxième mesure est la matrice de dispersion inter-classes S_b (*between-class scatter matrix*) qui est définie par :

$$S_b = \sum_{i=1}^{L} (m^i - \overline{m})(m^i - \overline{m})^T \qquad \textbf{(II.22).}$$

Avec $\overline{m}$ la moyenne de tous les échantillons.

Le but de la LDA est de maximiser les distances interclasses tout en minimisant les distances intraclasses, ce qui revient à retrouver la matrice de transformation U_{LDA} qui maximise le critère:

$$W_{opt} = \arg\max_W \left(\frac{\left| w^T S_b w \right|}{\left| w^T S_w w \right|} \right) \quad \textbf{(II.22).}$$

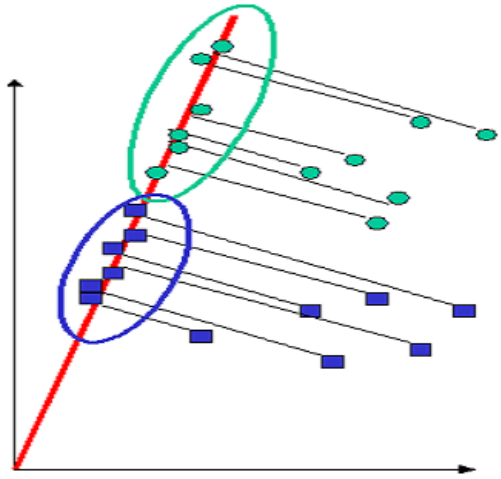


Figure II.9. Les projections de deux classes de points ("classe 1" et "classe 2") sur les axes principaux construits par la méthode LDA

Ce problème est ramené à un problème de recherche des vecteurs propres de la matrice $S_{w\text{-}1}S_b$. La matrice de transformation de LDA est les *m* premiers vecteurs propres sont donc ordonnés par ordre décroissant des valeurs propres correspondantes(U_{LDA}). Cette méthode est utilisée en fusion de données **[81]** pour distinguer entre les clients et les imposteurs.

II.7 Etapes de l'opération de fusion

Pour un niveau hiérarchique donné, l'opération de fusion s'effectue en plusieurs étapes **[82-84]**.

- **Alignement :** l'alignement ou conditionnement ou encore parfois, harmonisation, consiste à définir un espace commun, dans lequel les informations vont être projetées afin d'y être comparables. Cela veut dire que les observations ou les données sont ramenées dans un même référentiel.

- **Corrélation :** cette étape concerne la détermination des relations entre les différentes données.
- **Association ou mise en correspondance :** l'association est l'union des différentes représentations issues des informations multi-sources. Chaque mesure se trouve associée à l'entité correspondante (le résultat de l'étape de corrélation est évidemment utilisé). Cette étape permet aussi de rejeter les données aberrantes suivant un critère sur la matrice de covariance par exemple.
- **Combinaison :** seules les données obtenues après alignement et qui sont en accord avec l'étape d'association sont combinées pour obtenir une meilleure représentation de l'estimation correspondant à l'attribut avec lequel l'étape d'alignement a été réalisée.

L'auteur de **[85]** a aussi distingué en plus les notions de fusion statique et de fusion dynamique en définissant :

- **Fusion statique :** quand le résultat de l'opération de fusion est obtenu indépendamment des états antérieurs. On exploite alors uniquement les données de l'instant courant.
- **Fusion dynamique :** quand le résultat tient compte des états antérieurs. Tout processus de fusion ayant une formulation itérative rentre dans ce contexte. Cette approche peut être située au même niveau que la fusion temporelle.

II.8 Domaines d'applications de la fusion de données

La fusion de données a d'abord visé l'améliorer de la qualité des réponses aux problèmes posés par les militaires **[86]**, il y a approximativement vingt-cinq ans, mais aujourd'hui elle touche énormément de domaines. Voici quelques applications :

- **La télédétection** **[87]** est une science à part entière avec des applications s'étendant depuis le domaine civil de la surveillance jusqu'aux applications militaires. Elle permet de bénéficier de l'information fournie par des satellites d'observation de la Terre. Les données numériques de ces satellites, présentées sous forme d'images, s'avèrent particulièrement précieuses pour l'évaluation du potentiel territorial et pour la planification dans les secteurs de la forêt, de l'agriculture, de l'environnement, de la géologie et de l'aménagement du territoire. Les sondes qui acquièrent les images sont typiquement aéroportées ou spatiales. En outre, elles peuvent acquérir l'information

dans différentes bandes spectrales ou à différentes résolutions. La fusion peut également être employée pour combiner les données radar. Plusieurs applications de la fusion dans ce domaine sont décrites dans **[88]**, **[89]**, **[90]**.

- La mise au point d'un système de **détection de mines** exploite aussi l'intérêt de la fusion de données **[91]**, **[92]**.
- **La prévision météorologique** est un autre exemple d'application de la fusion de données ; l'air, les satellites, les avions et les ballons météorologiques fournissent des mesures sur l'état tridimensionnel de l'atmosphère et sur les propriétés de surface du sol et de l'océan. Au sol, des dizaines de milliers de stations mesurent les paramètres météorologiques, comme la température, le vent, la pression, etc. et les radars suivent les orages et les cellules de pluie. En mer, des bateaux et des bouées automatiques mesurent également les paramètres météorologiques, ainsi que la houle. Toutes ces informations de mesures sont traitées par des experts avec des modèles numériques et de fusion pour faire des prévisions du temps qui sont diffusées par les médias ou utilisées par certaines professions **[93-94]**.
- **La biométrie** donne lieu à plusieurs applications de fusion de données avec les différentes modalités biométriques et les systèmes multimodales **[95-99]**, identification de visages **[100-101]**, vérification de signatures **[102-104]**, reconnaissance de la parole **[105-107]**.
- **Document et écrit :** reconnaissance de chiffres **[108-114]**, reconnaissance de caractères et mots manuscrits **[115-117]**, classification des documents **[118]**.
- **Applications Médicales :** traitement d'images médicales et diagnostic médical **[119-121]**.
- **Robotique et véhicules intelligents : [122-125]**.

II.9 Conclusion

Dans ce chapitre, nous avons présenté les différentes facettes que comporte la fusion de données. On utilise la fusion de données aussi bien dans la vie quotidienne que dans les technologies les plus récentes. Il existe plusieurs topologies et niveaux de fusion dont le choix dépend de la nature des sources et de l'information.

De nombreux travaux sur la fusion de données dans les applications réelles montrent que la fusion améliore nettement les performances des systèmes de reconnaissance par rapport à

chacune des sources prises isolément.

Dans le prochain chapitre, nous allons nous attacher à décrire notre système multimodal basé sur la fusion en scores de l'empreinte digitale et la signature manuscrite cursive en ligne.

Chapitre III

Système proposé

III.1 Introduction

On peut constater de ce qui précède plusieurs limitations inhérentes des systèmes unimodaux. D'abord, au niveau de l'acquisition, le bruit cause une dégradation des performances. Ensuite, la modalité elle-même peut présenter une grande variabilité intra- classes ou une petite variabilité interclasses. Afin d'augmenter la fiabilité des systèmes biométriques et d'améliorer leurs performances, plusieurs systèmes sont combinés. Cette combinaison peut être basée sur différents systèmes de la même modalité ou sur des systèmes à base d'une modalité particulière.

Dans ce dernier cas, on parle de système biométrique multimodal. En plus de l'utilisation conjointe des modalités, les systèmes multimodaux offrent la possibilité d'une utilisation alternative. En effet, le système peut d'être configuré de telle manière à s'adapter à l'utilisateur. On peut par exemple authentifier un utilisateur avec l'empreinte, car il est facile de lui vérifier avec, tandis qu'on utilise une autre modalité pour un autre utilisateur dont les empreintes sont déformées.

Comme on a illustré dans le chapitre précédent, il existe plusieurs manières de fusionner les systèmes biométriques. La fusion peut être effectuée au niveau des capteurs, des paramètres, des scores, ou au niveau de la décision. Dans notre travail, la fusion au niveau des scores est préférée, car elle offre un meilleur compromis en termes d'informations et de simplicité de fusion **[126]**.

Le présent chapitre est consacré à la présentation du système d'authentification multimodale que nous proposons. Les différents composants de notre système (Les prétraitements appliqués, les paramètres extraits, la méthode de comparaison) ainsi que d'autres travaux avec lesquels notre travail sera comparé sont détaillés.

III.2 Architecture du système d'authentification biométrique multimodale proposé

L'architecture générale de notre système d'authentification biométrique multimodale est illustrée dans la **Figure (III.1).**

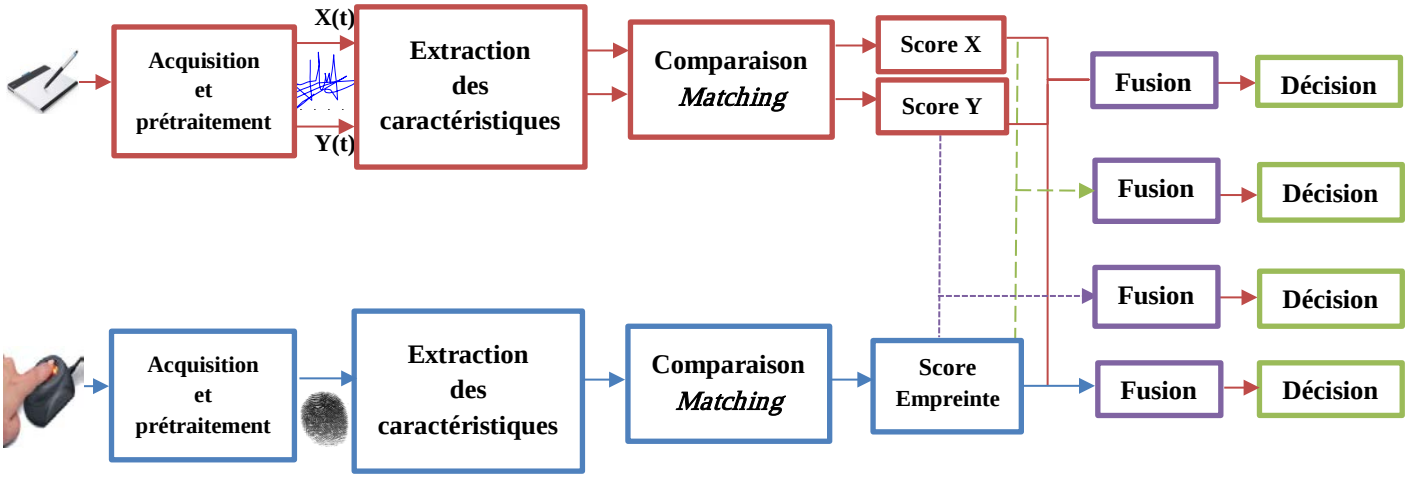


Figure III.1 : Architecture du système d'authentification biométrique multimodale proposé.

Nous avons choisi deux modalités biométriques de nature différente : une modalité morphologique et une autre comportementale en occurrence l'empreinte digitale et la signature manuscrite en ligne respectivement. Les deux systèmes sont traités séparément avant de les fusionner au niveau scores.

Dans le système d'authentification par signature, on extrait les coordonnées de la position (x(t) et y(t)) de la signature afin de leurs subir des prétraitements nécessaires avant d'extraire les paramètres discriminant à l'aide d'un algorithme original appelé la décomposition modale empirique. Ensuite vient l'étape de comparaison entre les paramètres extraits de ces coordonnées et ceux des coordonnées de la signature de référence ou deux scores de similitude sont obtenus.

Par ailleurs, dans le système d'authentification par empreinte digitale, on applique une série de prétraitements sur l'image brute de l'empreinte afin de faciliter l'opération d'extraction des paramètres (les minuties). Puis, la comparaison est effectuée entre les minuties de l'empreinte de test avec celles de l'empreinte de référence pour définir un score de similitude.

Avant d'abordée la phase de fusion, on a normalisé les scores issus de chaque système avec les trois méthodes de normalisation de scores décrites dans le chapitre précédent à savoir les méthodes Min-Max, Z-scores et TanH.

On a mise en œuvre plusieurs combinaisons de scores, en premier lieu, nous avons adopté une fusion intermodalité entre les deux scores de la signature, puis on a fusionné le score de l'empreinte digitale avec chacun des scores de la signature. Et pour terminer, on a fusionné le score de l'empreinte avec le score combiné entre les deux scores de la signature. Dans la suite, nous décrirons les différents composants de chaque système tandis que la description des phases de fusion, décision et évaluation des performances sera abordée au chapitre suivant.

III.3. Système d'authentification d'empreinte digitale

III.3.1. Généralités

L'empreinte digitale est le dessin formé par les lignes de la peau des doigts, des paumes des mains, des orteils ou de la plante des pieds. Ce dessin se forme durant la période fœtale. Il existe deux types d'empreintes: l'empreinte directe (qui laisse une marque visible) et l'empreinte latente (saleté, sueur ou autre résidu déposé sur un objet).

Elles sont uniques et immuables, elles ne se modifient donc pas au cours du temps (sauf par accident comme une brûlure par exemple). La probabilité de trouver deux empreintes digitales similaires est de 10^{-24}. Les jumeaux, par exemple, venant de la même cellule, auront des empreintes très proches, mais pas semblables.

On classe les empreintes selon un système vieux qui date d'un siècle: le système Henry. Dans ce système, le classement repose sur la topographie générale de l'empreinte digitale et permet de définir ses caractéristiques.

Les éléments qui permettent de différencier deux empreintes digitales ayant le même motif sont :

- **Les points singuliers globaux :**
  - **Noyau ou centre :** lieu de convergences des stries.
  - **Delta :** lieu de divergences des stries.

- **Les points singuliers locaux**
  - **Les minuties :** points d'irrégularité se trouvant sur les lignes capillaires. Petites imperfections dans le flot des lignes cutanées d'une empreinte digitale. Il en existe différents types (îlot, lacs, etc.)

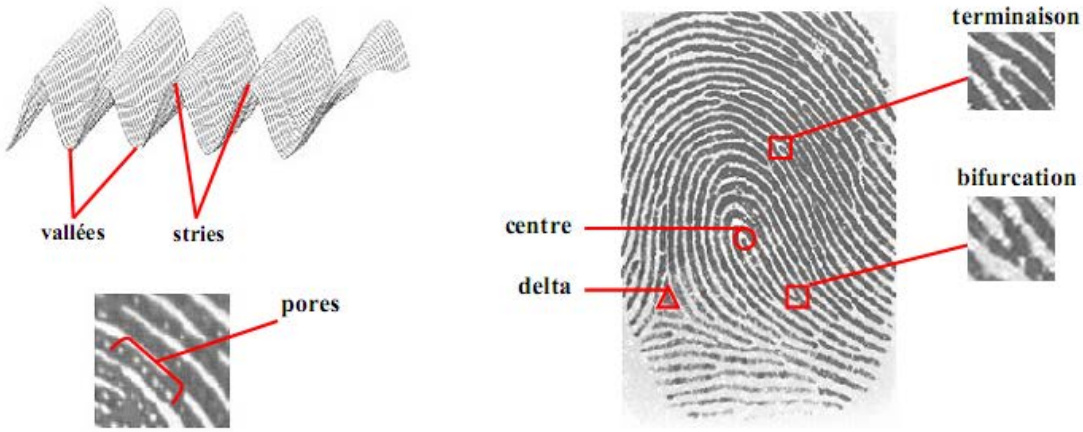


Figure III.2: Caractéristiques d'une empreinte digitale.

On peut relever jusqu'à seize types de minuties, mais dans les algorithmes on retient généralement que quatre types:

- **Terminaison à droite ou à gauche (minutie située en fin de strie)**: **Figure I-8-a**.
- **Bifurcation à droite ou à gauche (intersection de deux stries)** : **Figure I-8-b**.

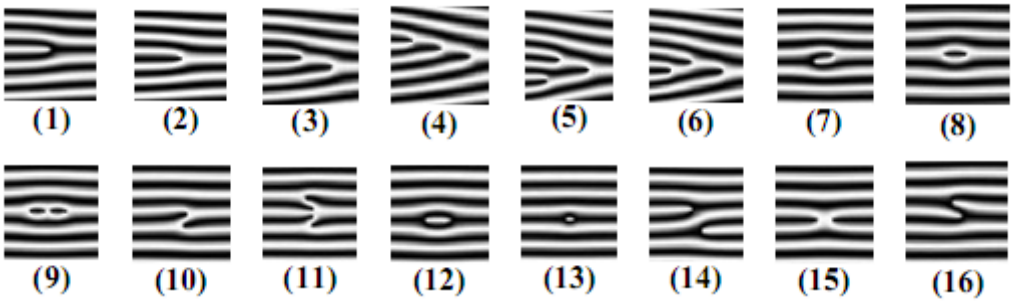
On peut citer également :

- **Île** : assimilée à deux terminaisons **: Figure III-3-d et e**.
- **Lac** : assimilé à deux bifurcations : **Figure III-3-c**.

(a) (b) (c) (d) (e)

Figure III.3: Types de minuties possibles (stries en noir): terminaison à droite ou à gauche (a), bifurcation à droite ou à gauche (b), Lac (c), Île (d) et (e).

Voici une représentation des seize (16) types de minuties existant dans les empreintes digitales:



1	**Terminaison**	**9**	**Boucle double**
2	**Bifurcation simple**	**10**	**Pont simple**
3	**Bifurcation double**	**11**	**Pont jumeaux**
4	**Bifurcation triple I**	**12**	**Intervalle**
5	**Bifurcation triple II**	**13**	**Point isolé**
6	**Bifurcation triple III**	**14**	**Traversée**
7	**Crochet**	**15**	**Croisement**
8	**Boucle simple**	**16**	**Tête bêche**

Figure III.4:Les différents types de minuties.

III.3.2. Etat de l'art

À l'heure actuelle, la reconnaissance des empreintes digitales est la méthode biométrique la plus utilisée. De diverses techniques ont été formulées par différents auteurs pour la reconnaissance de personnes par les empreintes digitales. Parmi ces techniques, on trouve celles basées sur l'extraction des minuties qui ont attirées l'intérêt de différents groupes de recherche.

Cette technique est largement adoptée parce que les minuties sont les primitives les plus uniques, les plus durables et les plus fiables d'une empreinte digitale. Ces algorithmes sont souvent conçus pour résoudre des problèmes de calcul de correspondance et de similitude. L'algorithme commence par l'acquisition de l'empreinte digitale **[127]** suivie d'une phase de prétraitement des arêtes et des vallées. Cette phase est nécessaire pour faciliter l'extraction des minuties et elle implique la segmentation d'arête, la normalisation, l'évaluation d'orientation, l'évaluation de fréquence, le filtrage, la binarization et l'amincissement **[128,129]**. Puis vient l'emploi de plusieurs algorithmes pour l'extraction des points de minuties des images amincies d'empreinte digitale **[128, 130, 131, 132]**. Plusieurs de ces algorithmes font l'extraction des points d'arête comme les bifurcations et les terminaisons **[133]**. Pendant le processus de *matching*, une similitude entre les ensembles de minuties de deux empreintes digitales est calculée par paires en comparant les descripteurs de minuties qui sont invariables à la rotation et à la taille **[127]**. D'autres travaux mettent l'accent sur les crêtes locales **[134]**, certaines études sont basées sur la position du point de singularité et son orientation **[135]**, et la détection de distance relative **[135-138]**. Certains considèrent des plateformes intégrées efficaces et à faible coût pour l'authentification **[139- 142]** alors que certains se concentrent sur les performances à l'aide de grandes bases de données **[143]** et la vitesse de reconnaître une empreinte digitale **[144]**. D'autres études mettent en œuvre la topologie en deux serveurs **[145]** ou multiserveurs **[146]**. Les techniques des systèmes embarqués tels que DSP **[147- 149]** *Field programmable gate array* (FPGA) en utilisant des réseaux de neurones **[150]** ont été employé pour des fins d'authentification d'empreinte digitales. Dans une autre étude, la méthode Delaunay Quadrangle en utilisant le code de la topologie a été utilisée pour l'authentification **[151]**. Les auteurs de **[152]** ont proposé un algorithme original basé sur la combinaison des descripteurs de minuties. Une autre approche basée sur une nouvelle distance appelée *Hilbert Scanning Distance* (HSD) a été proposé dans **[153]**. Par ailleurs, une autre philosophie basée sur les ondelettes a été élaborée par les auteurs de **[154].** Les auteurs de **[155]** fournissent une comparaison générale entre l'SVM, KNN, modélisation bayésienne et perceptrons multicouche. Carlotto et al. **[156]** emploie un modèle gaussien statistique tandis que D. Maio **[157]** propose un algorithme qui permet la localisation des minuties d'une manière plus directe en utilisant des réseaux de neurones. Dans **[158]** une approche basée sur le modèle de Markov cachée (HMM) a été proposée. Récemment, des approches basées sur la transformation **[159-160] ,** le filtre de Gabor **[161],** l'analyse en composante principale (ACP) **[162],** les coefficients de Fourrier **[163]**, la logique flou **[164]** et les empreintes 3D sans contact **[165]** ont été proposées.

III.3.3. Système proposé

Comme on a défini dans la section précédente**,** il existe deux principales approches pour séparer ou distinguer entre les empreintes digitales. La première approche, qui utilise des méthodes à base d'image, tente de faire de l'authentification basée sur les caractéristiques globales d'une image d'empreinte digitale. La seconde approche, qui est basée sur l'extraction des minuties, représente l'empreinte par ses caractéristiques locales, comme les stries et les bifurcations. Cette approche, qui a été intensivement étudiée, est également l'épine dorsale de l'actuelle disposition de produits d'authentification d'empreintes digitales. Dans notre travail, nous avons choisi d'utiliser cette approche.

Notre système d'authentification d'empreintes digitales est composé essentiellement de cinq étapes fondamentales, qui sont: L'acquisition, le prétraitement, l'analyse ou l'extraction des caractéristiques, l'apprentissage et la comparaison ou le *matching*. Voici un schéma synoptique qui donne une globalisation des étapes de notre système:

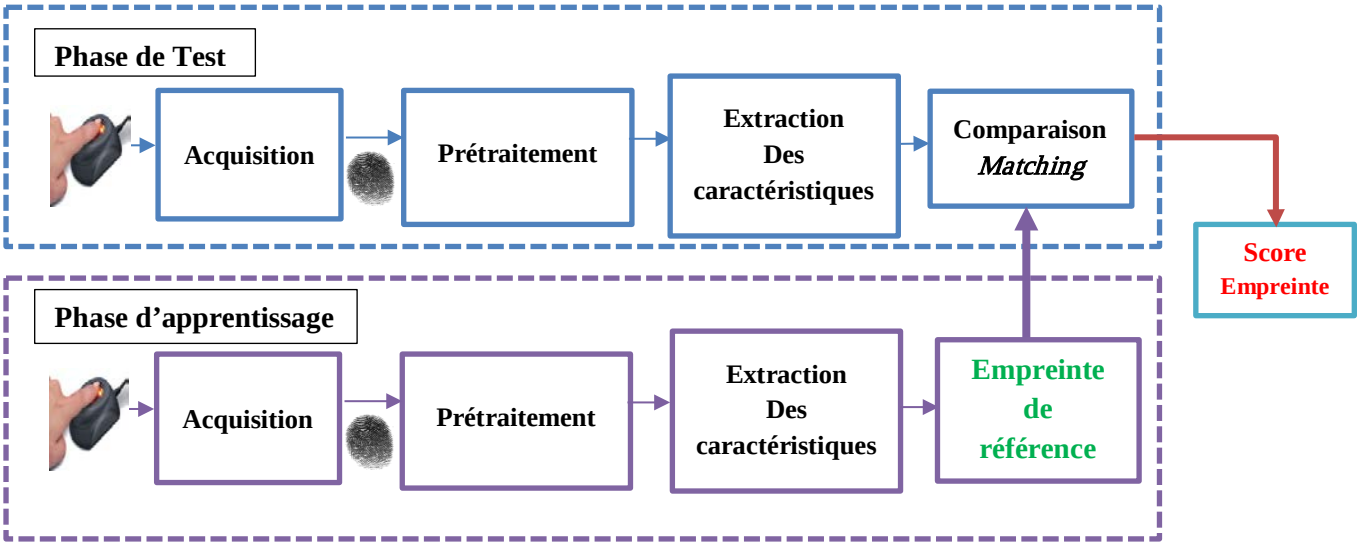


Figure III.5: Architecture générale de notre système d'authentification d'empreintes digitales.

Maintenant on va développer les étapes de ce système ainsi que les sous opérations effectuées lors chaque étape:

III.3.4. L'acquisition

Dans un système d'authentification d'empreintes digitales, l'acquisition de l'image de l'empreinte joue un rôle primordial. C'est une étape primaire dans un système de

reconnaissance qui consiste à acquérir l'image de l'empreinte digitale de départ afin de lui subir les différents traitements possibles.

Toutefois, dans notre travail, nous avons utilisé la célèbre base fournie par FVC 2004 (Fingerprint Verification Competition 2002) **[166]** ainsi que la base bimodale MCYT (empreinte et signature) **[167]** que nous allons décrire leurs caractéristiques au chapitre IV. Donc, On n'a pas effectué une acquisition au sens propre. Néanmoins, on va définir quelques concepts concernant les types de capteurs utilisés lors de l'acquisition des empreintes digitales :

III.3.4.1 Les capteurs optiques

Les capteurs optiques sont les plus largement utilisés. Ils ont une grande efficacité et une précision acceptable, sauf pour certains cas, comme quand le doigt de l'utilisateur est trop sale ou trop sec.

La méthode optique est l'une des méthodes les plus communes. Un appareil photo CCD (dispositif couplé chargé) est utilisé au cœur du capteur optique. Un appareil photo CCD se compose simplement d'une rangée de diodes sensibles légères appelées photosites. En général, le doigt est placé sur une surface en verre et l'appareil photo CCD prend la photo.

Le système CCD contient une rangée de LED (diodes électroluminescentes) qui illumine les creux et les bosses du doigt. Un prix avantageux constitue l'avantage principal des systèmes optiques tandis que leurs inconvénients sont qu'ils sont faciles à détourner. L'autre problème est celui des empreintes latentes : l'empreinte digitale du doigt précédent, qui a été placé sur le capteur peut laisser sa trace.

III.3.4.2- Les capteurs électriques-thermiques

Ce capteur mesure le différentiel de température entre les vallées de l'empreinte et l'air capturé dans les stries de l'empreinte digitale. Cette méthode donne une image d'excellente qualité même sur des empreintes de qualité médiocre telles que celles provenant de doigts secs avec peu de profondeur entre les vallées et les stries.

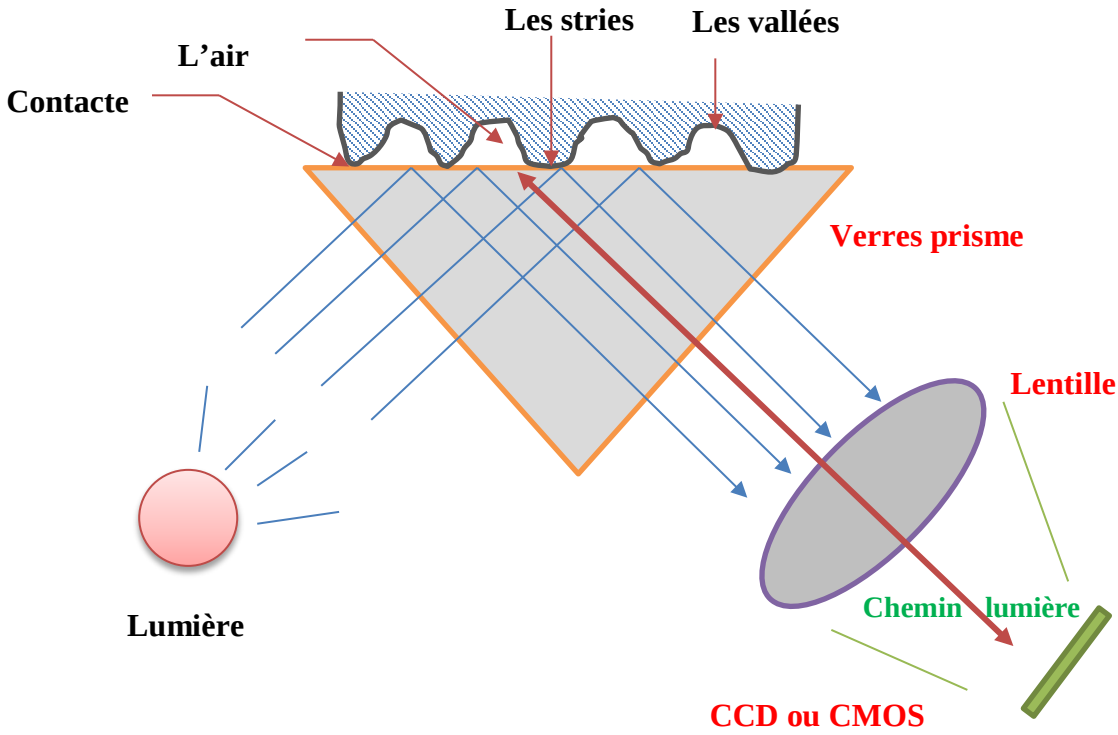


Figure III.6: Principe du capteur optique d'empreintes digitales

La technologie thermique fonctionne également dans des conditions environnementales difficiles, comme lors des températures extrêmes, de taux d'humidité ou de poussière élevé, ou de contamination d'eau.

L'avantage de cette technologie est donc la possibilité d'avoir une image de bonne qualité avec un capteur toujours propre. Son inconvénient est que la qualité de l'image dépend des compétences de l'utilisateur à savoir manipuler le capteur. Le deuxième inconvénient est le chauffage du capteur qui augmente la consommation électrique. La chaleur du capteur est nécessaire afin d'éviter un équilibre thermique entre le capteur et la surface du doigt.

III.3.4.3 Les capteurs capacitifs

La méthode capacitive est une des méthodes les plus populaires. Comme les autres capteurs, le capteur capacitif d'empreinte digitale reproduit l'image des stries et vallées qui composent une empreinte digitale. Le capteur capacitif emploie des condensateurs de courant électrique pour mesurer l'empreinte digitale. Un capteur capacitif se compose d'une rangée de

cellules minuscules. Chaque cellule inclut deux plaques conductrices recouvertes par un revêtement protecteur.

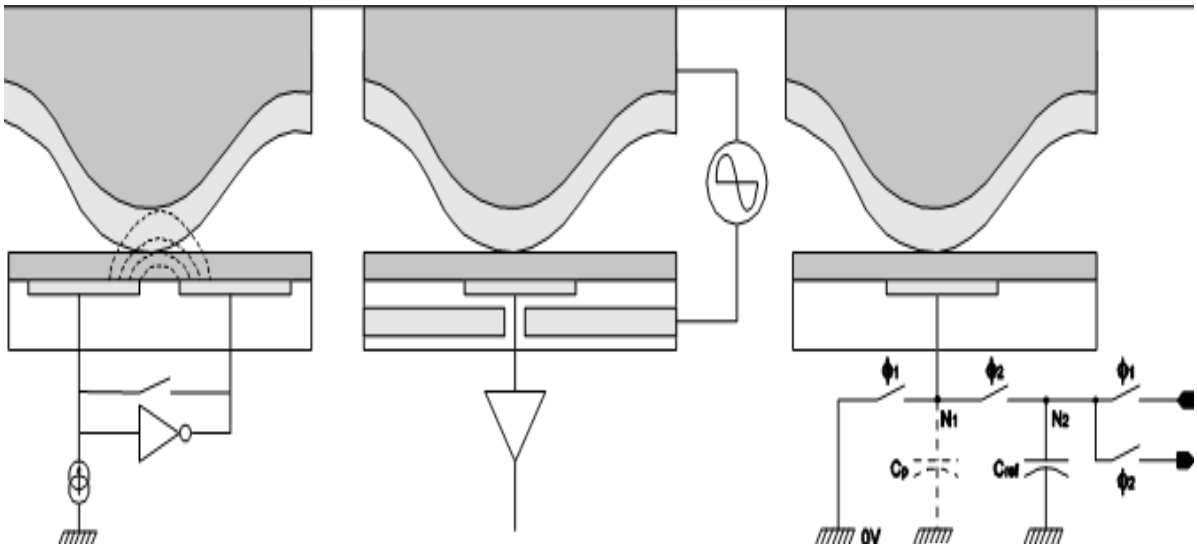


Figure III.7: Principe des capteurs capacitifs (a) capteur actif a deux électrodes (b) capteur passif à une électrode (c) capteur actif à une électrode.

L'avantage principal des capteurs capacitifs est qu'ils demandent une réelle empreinte digitale. Mais ils rencontrent des difficultés avec les doigts secs et humides. Des doigts humides rendent l'image noire, tandis que des doigts secs la rendent pâle.

III.3.4.4. Les capteurs à champ-électrique

Le capteur à champ-électrique fonctionne avec un champ-électrique et le mesure au-delà de la couche extérieure de la peau là ou l'empreinte digitale commence. La technologie du champ-électrique peut être utilisée dans des conditions extrêmes par exemple lorsque le doigt est sale ou sec.

La technologie du champ-électrique crée un champ électrique entre le doigt et le semi-conducteur adjacent qui imite la forme des stries et des vallées de la couche épidermique du doigt. Un amplificateur est utilisé pour mesurer les signaux. On parvient ainsi à une image plus claire que ce que peuvent donner les technologies optiques ou capacitives. Cette technologie permet d'obtenir des images d'empreinte digitale que d'autres technologies ne parviendraient pas à avoir.

III.3.4.5. Les capteurs sans contact

Le capteur sans contact a un fonctionnement semblable à celui du capteur optique. En général, il y a une glace optique de précision à une distance de 5 à 7 cm de l'empreinte digitale. L'empreinte digitale est mise sur un support avec une ouverture. Un des inconvénients à considérer est que la poussière et la saleté peuvent se déposer sur la vitre optique, donnant un mauvais résultat d'image. D'autre part, les empreintes digitales scannées sont sphériques ce qui amène à des algorithmes de comparaison plus complexes.

III.3.5. Le prétraitement

L'authentification d'une empreinte digitale est directement liée à la qualité de l'image obtenue au moyen du capteur. Ainsi dans la plupart des cas, un prétraitement est nécessaire pour améliorer la qualité de l'image. Le but de cette phase est de rendre l'image plus claire pour faciliter de nouvelles opérations. Ces méthodes préliminaires de prétraitement ont pour but d'augmenter le contraste entre les stries et les sillons et de relier les points rompus. Cette phase comporte plusieurs opérations d'amélioration (**Figure III.8**) comme suit:

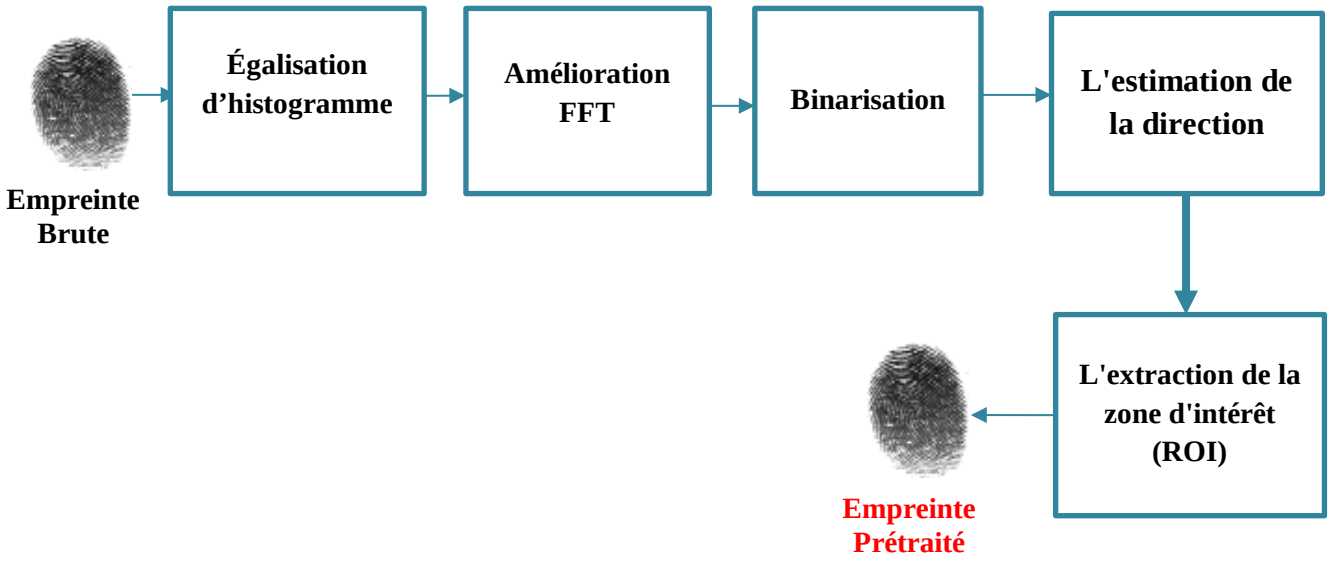
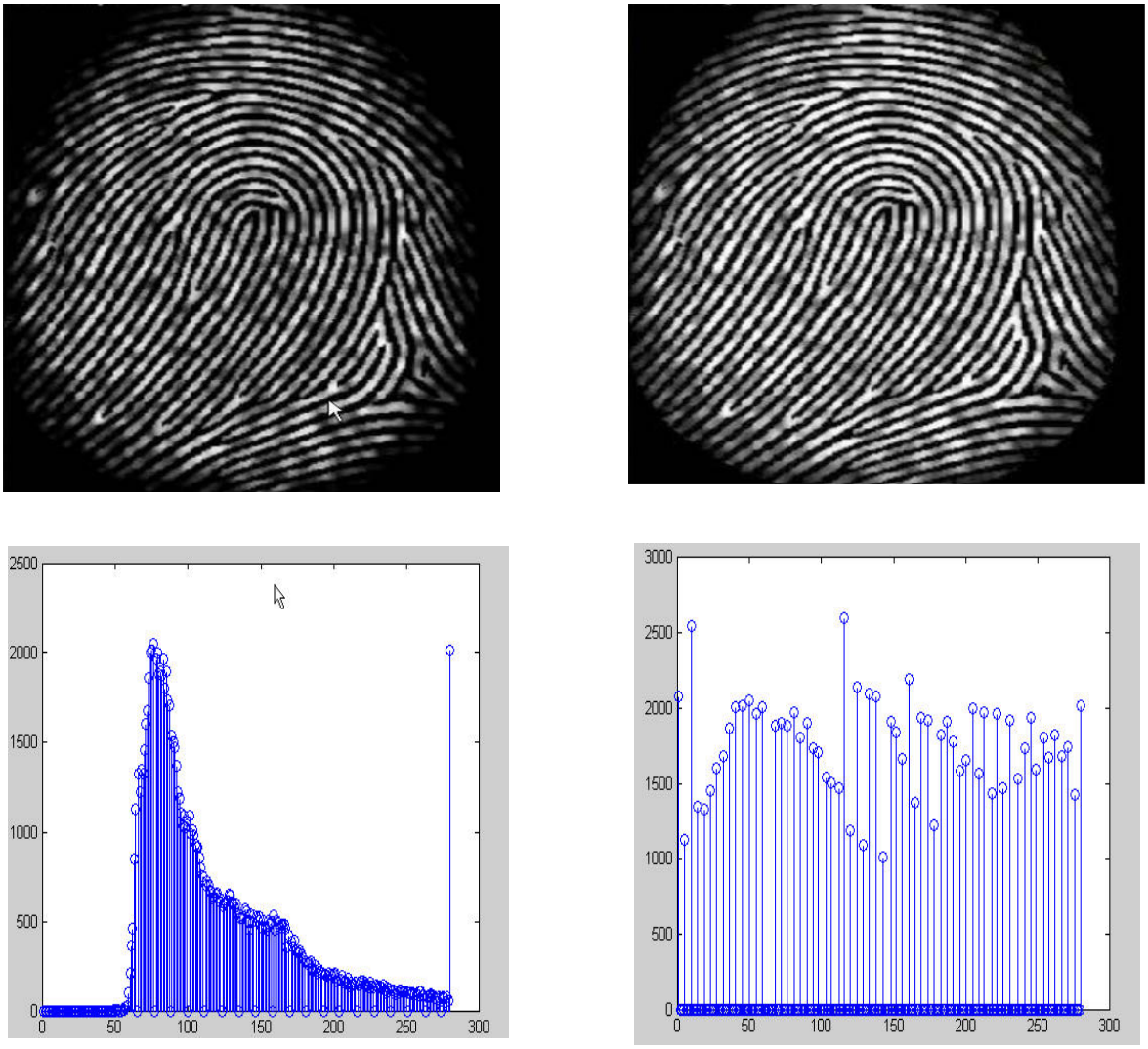


Figure III.8: Les différentes phases de prétraitement d'une empreinte digitale.

III.3.5.1 L'égalisation d'histogramme

L'égalisation d'histogramme consiste à élargir la distribution des valeurs des pixels d'une image de manière à accroître l'information de perception. L'histogramme d'une image d'empreinte digitale est de type bimodal (**Figure III.9.a**), l'histogramme après l'égalisation occupe toute la gamme de 0 à 255 et l'effet de visualisation est par conséquent amélioré (**Figure III.9.b**).



(a) **(b)**

Figure III.9: L'image de l'empreinte et son histogramme (a) avant l'égalisation (b) après l'égalisation.

III.3.5.2 Amélioration des empreintes digitales par transformée de Fourier

Nous divisons l'image en petits blocs de traitement (32 par 32 pixels) et on applique la transformée de Fourier discrète 2D selon:

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times e^{(-2j\pi\left(\frac{ux}{M}+\frac{vy}{N}\right))} \quad \textbf{(III.1)}$$

pour u = 0, 1, 2, ..., 31 et v = 0, 1, 2, ..., 31.

Afin de renforcer un bloc spécifique par ses fréquences dominantes, on multiplie la FFT du bloc par son amplitude une série de fois selon :

$$FFT = abs\left(F(u,v)\right) = \left|F(u,v)\right| \quad \textbf{(III.2)}$$

On obtient un bloc amélioré selon:

$$g(x,y) = F^{-1}\left\{F(u,v)\times\left|F(u,v)\right|^{k}\right\} \quad \textbf{(III.3)}$$

Où F^{-1} (F (u, v)) est effectuée par:

$$f(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} g(u,v) \times e^{(+2j\pi\left(\frac{ux}{M}+\frac{vy}{N}\right))} \quad \textbf{(III.4)}$$

Avec x = 0, 1, 2, ..., 31 et y = 0, 1, 2, ..., 31.

Le terme " **k**" dans la formule (**III.3**) est une constante déterminée expérimentalement. Après avoir essayé plusieurs valeurs (**Figure III.10**), nous avons choisi un k=0,45. Une meilleure valeur de **k** permet de connecter des points rompus à tort sur les stries et supprime certaines connexions parasites. Si "k" est trop élevé (**Figure III.10.d**), il peut entraîner de faux assemblages des stries. Ainsi, une terminaison pourrait devenir une bifurcation.

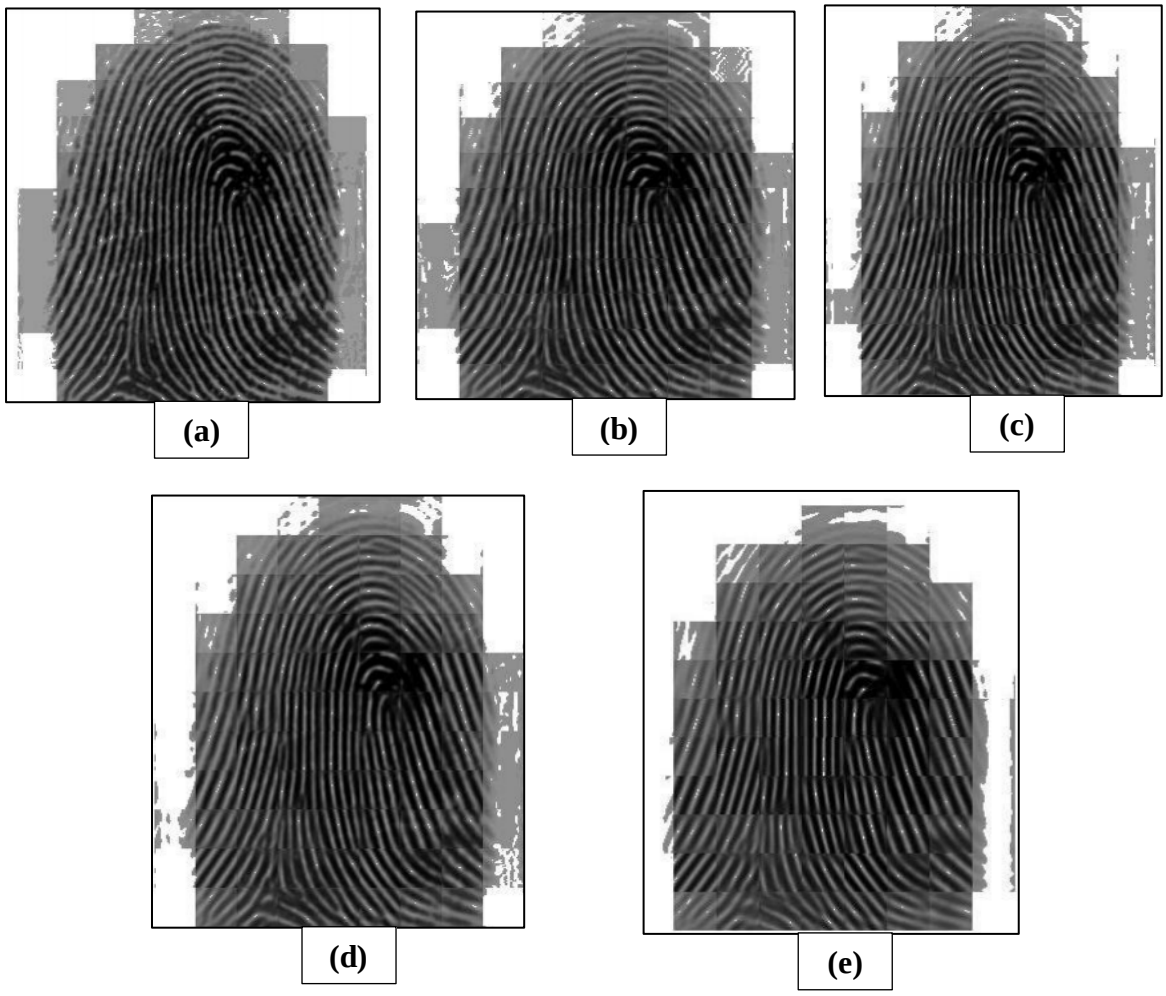


Figure III.10:L'image de l'empreinte digitale améliorée avec FFT pour plusieurs valeurs de k (a) k= 0.1 (b) k= 0.4 (c) k= 0.45 (d) k= 0.5 (a) k= 1

III.3.5.3. Binarisation image d'empreinte digitale

La binarisation d'image d'empreinte digitale consiste à transformer l'image d'empreinte digitale, qui est naturellement à 8 bits et en niveaux de gris, à une image à un seul bit avec l'attribution de la valeur "**0**" pour les stries et la valeur "**1**" pour les vallées.

Une méthode adaptative de binarisation locale est adoptée pour binariser l'image d'empreinte digitale. Cette méthode attribue la valeur **1** au pixel dont sa valeur excède la valeur de l'intensité moyenne du bloc courant (16x16) à laquelle appartient le pixel, dans le cas contraire, il prend la valeur **0**. Après avoir effectué cette opération, les stries de l'empreinte

digitale sont mises en évidence avec la couleur noire tandis que les vallées prendront la couleur blanche (**Figure III.11**).

Figure III.11: Binarisation de l'image de l'empreinte digitale

III.3.5.4. La segmentation d'images d'empreintes digitales:

Dans une image d'empreinte digitale, seule une région d'intérêt (ROI) est utile pour le processus d'authentification parce qu'elle contient les informations discriminantes. Pour extraire cette région, deux étapes sont nécessaires. La première étape consiste à l'estimation du bloc de la direction **[168]**, tandis que la seconde est effectuée à l'aide de certaines méthodes morphologiques.

III.3.5.4.1. L'estimation de la direction

L'estimation de la direction est effectuée pour chaque bloc de 16x16 de l'image d'empreinte digitale. L'algorithme est comme suit :

- On calcule les valeurs des gradients g_x et g_y le long de la direction X et Y pour chaque pixel du bloc. Deux filtres de Sobel sont utilisés pour accomplir cette tâche.
- Pour chaque bloc, on utilise la formule suivante pour obtenir le rapprochement des moindres carrés pour le bloc de direction :

$$tg2ß = 2\sum\sum(g_x \times g_y) / \sum\sum(gx^2 - gy^2) \qquad \textbf{(III.5)}$$

- Ainsi, la valeur tangente du bloc de direction est estimée à peu près de la même manière que le sens illustré par la formule suivante:

$$tg2ß = 2sin\theta\, cos\theta / (cos^2\theta - sin^2\theta) \quad \textbf{(III.6)}$$

- Après avoir fini avec l'estimation de la direction de chaque bloc, les blocs qui ne contiennent pas d'importantes informations sur les stries et les vallées sont éliminés sur la base de la formule suivante:

$$E = \{2\sum\sum(gx \times gy) + \sum\sum(gx^2 - gy^2)\} / W \times W \times \sum\sum(gx^2 + gy^2) \quad \textbf{(III.7)}$$

- Pour chaque bloc, si son niveau de certitude E est inférieur à un seuil, alors le bloc est considéré comme un élément de fond.

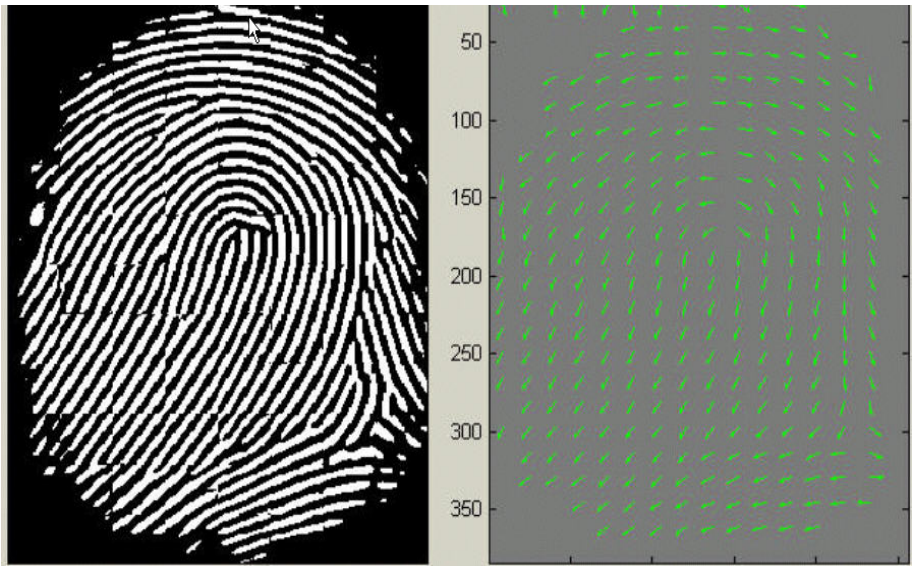


Figure III.12: Exemple de la carte directionnelle de l'empreinte digitale

III.3.5.4.2. L'extraction de la zone d'intérêt (ROI) par les opérations morphologiques

Deux opérations morphologiques appelées «l'ouverture» et «la fermeture» sont adoptées. L'opération d'ouverture (**Figure III.13.b)** fait étendre l'image et fait supprimer les pics introduits par le bruit de fond. L'opération de fermeture fait réduire l'image et élimine les petites cavités

(**Figure III.13.c)**. La région d'intérêt est obtenue après la soustraction du secteur fermé du secteur ouvert (**Figure III.13.d).**

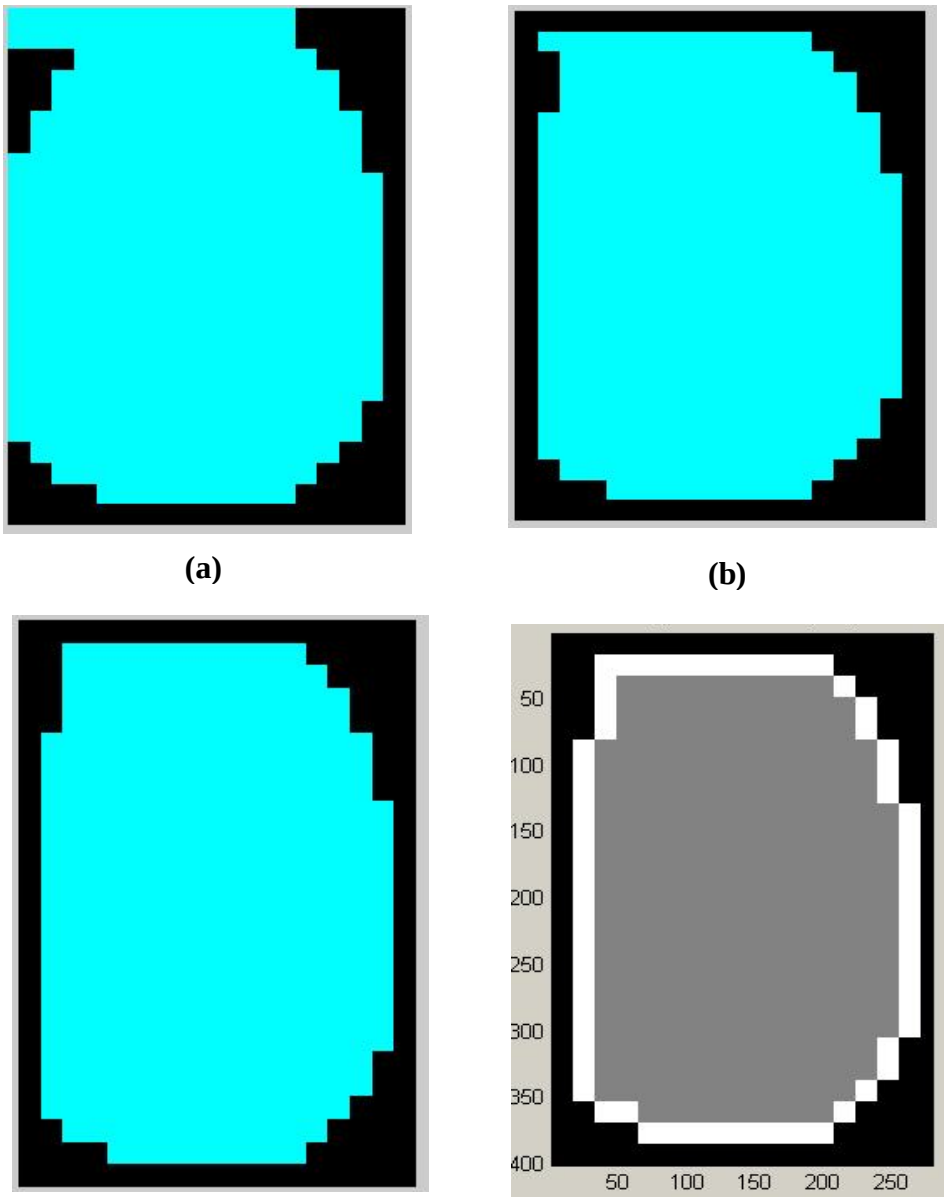


Figure III.13: Détermination de la zone d'intérêt (a) Région originale d'image d'empreinte (b) après l'opération de fermeture (c) après l'opération d'ouverture (d) la région d'intérêt de l'empreinte.

III.3.6. L'ANALYSE

III.3.6.1. Amincissement et élimination des pics et des points de pauses

L'opération d'amincissement consiste à éliminer les pixels redondants de strie en strie. Elle utilise un algorithme itératif et parallèle **[169]**. Dans chaque balayage complet de l'image

d'empreinte digitale, l'algorithme marque les pixels redondants dans chaque fenêtre d'image de taille (3x3) et supprime définitivement tous les pixels marqués après plusieurs balayages.

On utilise une méthode pour extraire les stries éclaircies directement à partir d'images d'empreintes digitales binarisées qui cherche à tracer les stries qui ont le maximum de valeur d'intensité de niveaux de gris **[170]** **(Figure III.14.a)**.

La carte amincie des stries est ensuite filtrée par deux opérations morphologiques en occurrence l'ouverture et la fermeture afin de supprimer certains points de pauses, des points isolés, des pics et crampons afin de faciliter l'étape suivante qui est l'extraction des minuties.

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

Figure III.14: (a) Amincissement de l'image d'empreinte (b) l'image d'empreinte après l'élimination des points de pauses (c) l'image d'empreinte après l'élimination des pics et crampons.

III.3.6.2. Extraction des minuties

Après avoir effectué les opérations précédentes, l'extraction des points de minuties est relativement abordable. Mais, ce n'est pas toujours une tâche facile, car on peut rencontrer au moins un cas spécial qui évoque notre prudence au cours de l'extraction des minuties.

En général, pour chaque fenêtre de 3x3, si le pixel central prend la valeur "**1**" et qu'il a exactement trois voisins qui ont comme valeur "1", alors le pixel central est considéré comme une bifurcation (**Figure III.15.a**).

Si le pixel central prend la valeur "1" et a qu'il a seulement un seul voisin qui a comme valeur "1", alors le pixel central est considéré comme une terminaison (**Figure III.15.b**).

La (**Figure III.15.c**) illustre un cas particulier de minuties qui est la branche triple. Supposons que le pixel le plus élevé a comme valeur "1" et que le pixel le plus à droite prend la valeur "1" et qu'on a un autre voisin en dehors de la fenêtre de 3x3 qui prend lui aussi la valeur "1", alors les deux pixels seront considérés comme des branches.

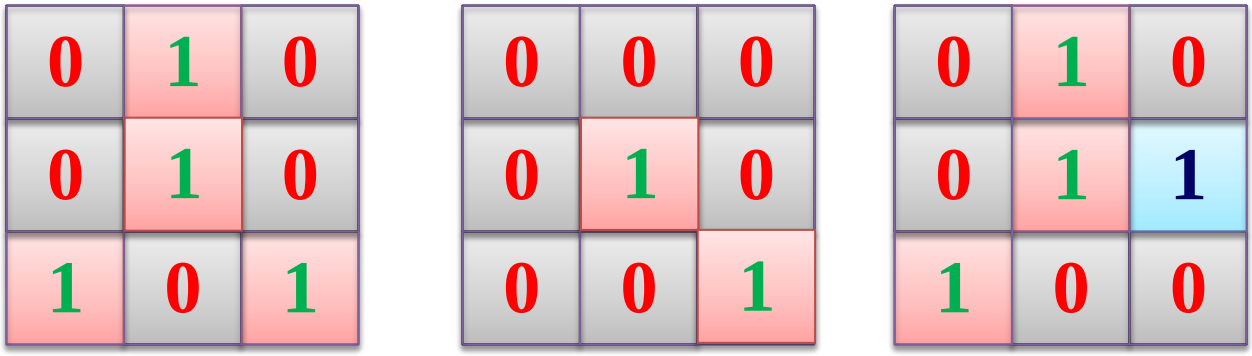


Figure III.15: Les types de minuties (a) bifurcation (b)Terminaison (c) branche triple.

Maintenant on va mieux définir le mécanisme d'extraction de minuties qui va jouer un rôle primordial pour la suite des opérations d'authentification. Considérant une fenêtre de 3x3 représenté par la **Figure III.16.**

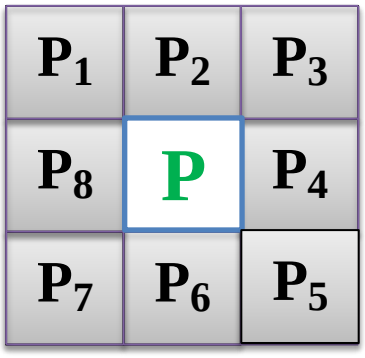


Figure III.16. Fenêtre de 3x3 d'une image d'empreinte digitale

Si on calcule le nombre de transitions divisé par 2 entre un pixel blanc et un pixel noir pour chaque point du squelette, on obtient un nombre appelé CN (*Crossing Number*) de stries partant de ce point et nous pouvons donc déterminer simplement le type d'un pixel selon :

$$CN(P) = \frac{1}{2}\sum_{i=1}^{8}\left|P_i - P_{i-1}\right| \quad avec\ P_8 = P_0 \ \ et \ \ P_i \in \{0,1\} \qquad \textbf{(III.8)}$$

Ainsi pour chaque pixel **P** appartenant à une strie (c'est-à-dire pour chaque pixel qui prend la valeur de "1"), la valeur de CN peut prendre cinq valeurs:

- **CN (P) =0** : dans ce cas il s'agit d'un pixel isolé et nous n'en tenons pas compte, car même si ce type de minutie existe, il est très rare et à ce stade du traitement il est probablement dû à un résidu de bruit.
- **CN (P)=1** : dans ce cas nous avons à faire à une minutie de type terminaison.
- **CN (P)=2** : c'est le cas le plus courant, le pixel se situe sur une strie, il n'y a pas de minutie.
- **CN (P)=3** : nous sommes en présence d'une bifurcation triple.
- **CN (P)=4** : nous sommes en présence d'une bifurcation quadruple. Ce type de minutie étant assez rare il est probablement dû au bruit que nous l'ignorons.

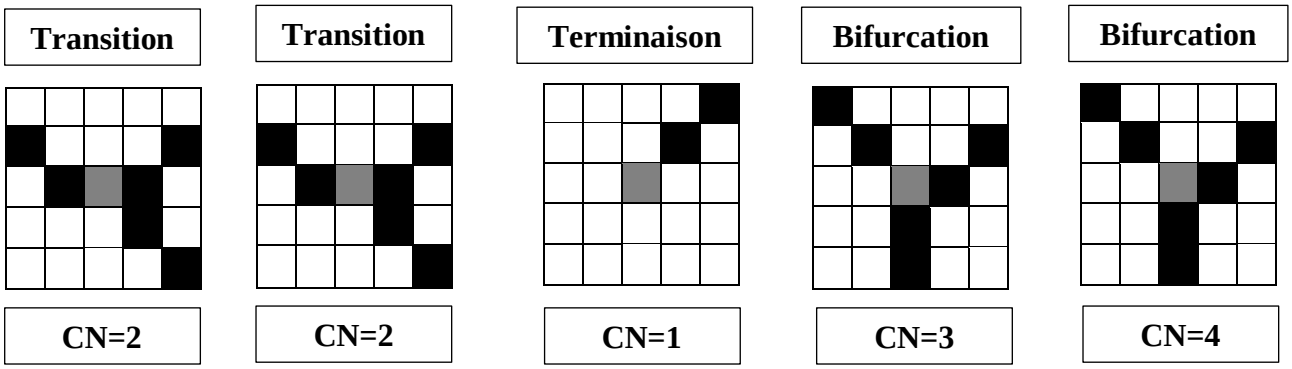


Figure III.17: Exemples de détermination du type de minutie en fonction du calcul du nombre CN.

Bien que l'utilisation du nombre CN facilite grandement la détection des minuties, elle provoque aussi la détection d'un très grand nombre de minuties (quelques centaines). Un traitement supplémentaire est nécessaire pour éliminer le plus de fausses minuties possibles.

III.3.6.3.L'élimination des fausses minuties

L'objectif de ce processus est d'éliminer au maximum les fausses minuties tout en conservant les vraies détectées. Pour cela, on utilise des considérations empiriques basées sur le fait que la distance entre deux minuties voisines est toujours supérieure à un certain seuil. En effet, pratiquement, il est extrêmement rare de trouver deux vraies minuties très proches, par contre on a quasiment toujours une concentration locale de plusieurs fausses minuties.

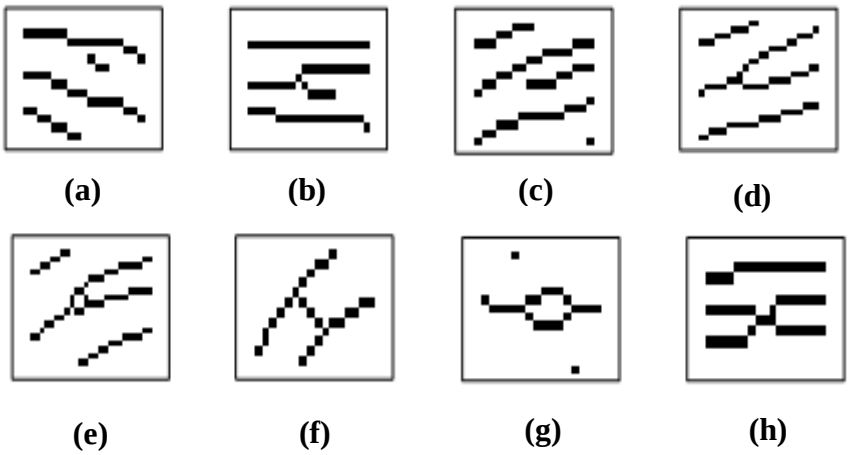


Figure III.18: Exemples de minuties détectées (a)segment trop court (b)branche parasite (c)vraie terminaison (d) vraie bifurcation (e) triangle (f)pont (g) îlot (h)segment trop court.

III.3.6.3.1- Le traitement des terminaisons détectées

Lorsque l'on détecte un point $T(X_T, Y_T)$ candidate pour le titre de terminaison (CN (P)=1), on vérifie d'abord si celui-ci se situe au bord de l'image, car la très grande majorité des fausses terminaisons se situent au bord de l'image . Ceci permet d'éliminer de nombreuses fausses terminaisons, car les lignes du squelette qui s'arrêtent au bord de l'image provoquent la détection de fausses terminaisons.

Le découpage en blocs défini au cours de la segmentation de l'image a permis de diviser l'image en deux sous-ensembles: la zone d'intérêt contenant l'information de l'empreinte et son complément qui correspond au bord de l'image et que nous notons **S**. Si il existe un bloc adjacent au bloc contenant $T(X_T, Y_T)$,et appartenant à S, alors on considère que $T(X_T, Y_T)$ est une fausse terminaison et on l'élimine. Cette simple considération permet d'éliminer plus de trois quarts des fausses terminaisons détectées.

Pour les terminaisons restantes **T** on parcourt la strie qui lui est associée sur une distance maximum K_1 avec: $K_1 = \overline{d} = (d_{min} + d_{min}) = 9$ *pixels* jusqu'à atteindre le point À($d = TA \leq K_1$) (**Figure III.19**). Nous considérons deux cas de fausses terminaisons:

- $d < K_1$ et CN (P)=3 : on détecte une bifurcation avant d'avoir parcouru la distance maximum . On est dans le cas d'une branche parasite, le point $T(X_T, Y_T)$ et la bifurcation "A" sont considérés comme des fausses minuties.
- d< K1 et CN (P)=1: on détecte une terminaison avant d'avoir parcouru la distance maximum. On est dans le cas d'un segment trop court. Alors le point $T(X_T, Y_T)$ et la terminaison "**A**" sont considérés comme de fausses terminaisons.
- Dans tous les autres cas, T (XT, YT) est validée en tant que vraie terminaison.

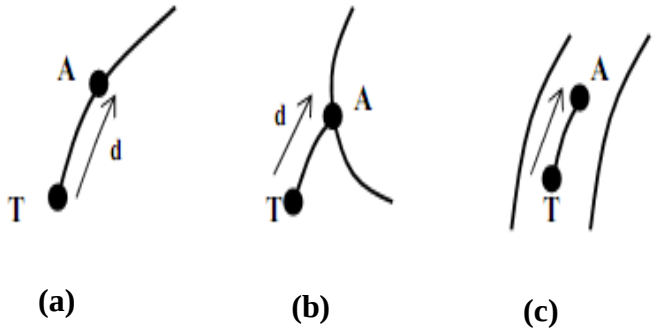


Figure III.19: Validation des terminaisons détectées (a) cas d'une vraie terminaison, (b)branche parasite, (c) segment trop court.

III.3.6.3.2- Le traitement des bifurcations détectées

Lorsqu'on détecte un point B candidat pour le titre de bifurcation (CN (B)=3), on parcourt les trois stries qui lui sont associées sur une distance maximum de K jusqu'à atteindre trois points A1, A2 et A3 (**Figure III.20**). Plusieurs cas peuvent se produire et ils sont traités dans l'ordre suivant:

- $d < K_1$, $d < K_2$, $d < K_3$ la zone circulaire de centre B et de rayon K_1 contient au moins quatre minuties. On considère alors que nous sommes dans une zone très bruitée (regroupement important) et que B est une fausse bifurcation.

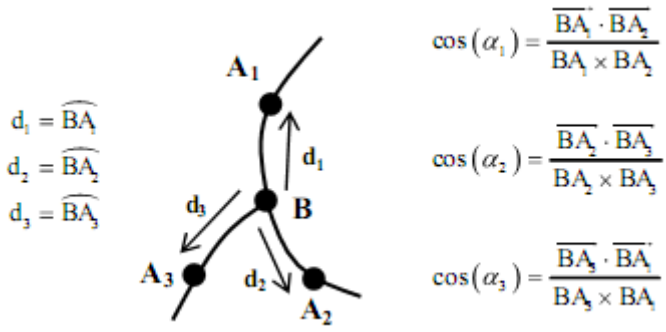
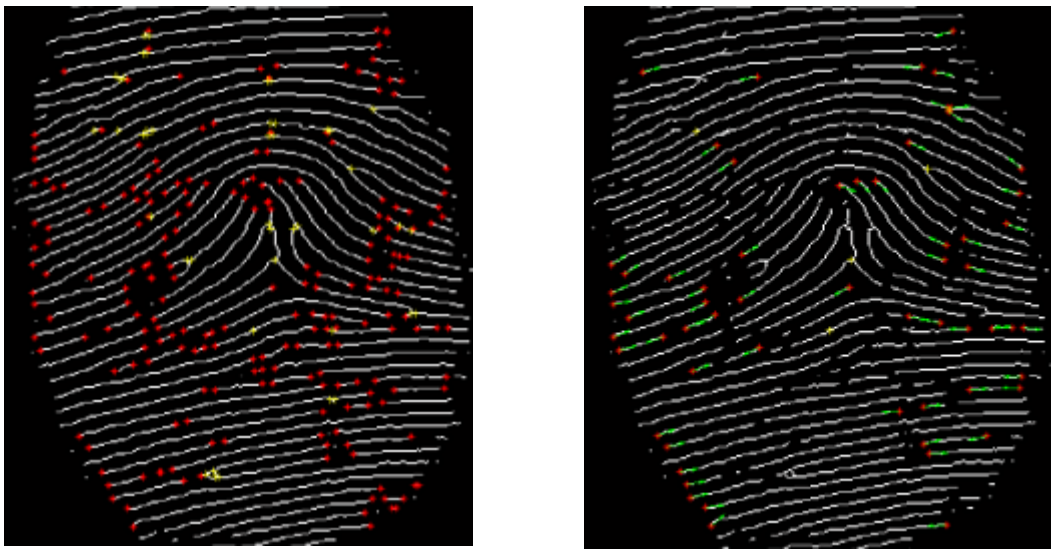


Figure III.20: Définitions associées à une bifurcation lors de la phase de validation.

- CN (A_1)=1, CN (A_2)=1, CN (A_3)=1 : au moins une des stries mène à une terminaison. On est dans le cas d'une branche parasite, le point B et les terminaisons atteints ne sont pas validés.
- $A_1 = A_2$ ou $A_2 = A_3$ ou $A_3 = A_1$: deux des stries mènent au même point. On est dans le cas d'un îlot (**Figure III.18.g**), le point B et la bifurcation atteinte ne sont pas validés.
- Nous avons deux des stries qui mènent à deux bifurcations **A1** et **A2** (**CN (A_1) =3, CN (A_2)=3**). Dans ce cas, on calcule la différence angulaire $\boldsymbol{\alpha_1}$ ainsi que la distance $\left\|\overline{A_1A_2}\right\|$ entre les deux bifurcations rencontrées. Si les conditions $\left|\cos(\alpha_1)\right| \succ \cos(\frac{\pi}{4})$ et $\left\|\overline{A_1A_2}\right\| \leq \lambda$ (**B** correspond à la distance inter-strie locale du bloc contenant **B**) sont réunies, alors on est dans le cas d'un triangle (**Figure III.18.e**) et on considère que **B** est une vraie bifurcation tandis que **A1** et **A2** sont des fausses.
- Une seule des stries mène à une bifurcation **A1** (**CN (A_1) =3**). On calcule les différences angulaires $\boldsymbol{\alpha_1}$ et $\boldsymbol{\alpha_2}$ ainsi que la distance entre **A1** et **B**. Si $\left|\cos(\alpha_2)\right| \succ \cos(\frac{\pi}{4}), \left|\cos(\alpha_1)\right| \succ \cos(\frac{\pi}{4})$ et $\left|BA_1\right| \leq \lambda$, alors on est dans le cas d'un pont (**Figure III.18.f**) et **A1** et **B** sont considérés comme de fausses minuties.
- Dans tous les autres cas, le point B est validé en tant que vraie bifurcation.

La figure suivante illustre un exemple du processus d'extraction des minuties ainsi que la phase d'élimination des fausses terminaisons et bifurcations :



(a) **(b)**

Figure III.21: Processus d'extraction des minuties (a) extraction générale des minuties (b) élimination des fausses terminaisons et bifurcations.

III.3.7. Apprentissage et sauvegarde du fichier paramètres

La phase d'apprentissage consiste à définir l'empreinte de référence. Dans notre cas la première empreinte de chaque utilisateur est considérée comme empreinte de référence. Cette dernière va subir toutes les étapes de prétraitement et d'analyse décrites précédemment et on sauvegarde ainsi son fichier paramètres qui correspond à l'information utile contenue dans l'image qui est nécessaire à l'authentification. Dans notre cas il s'agit de la liste des minuties détectées et validées associées avec leurs caractéristiques. Pour chaque minutie détectée et validée, on extrait trois caractéristiques :

- Le type de minutie: bifurcation ou terminaison (1 bit).
- La position de la minutie dans l'image: coordonnées (x, y) (2 octets).
- La direction du bloc local associé à la strie: θ (2 octets).

Après la validation des minuties, on dispose donc d'un fichier paramètres **S** comportant **N** minuties valides.

$$S = \left\{ M_i = (x_i, y_i, \theta_i, t_i) \middle| i \in [1 \ldots N] \right\} \quad \|S\| = N \qquad \textbf{(III.9)}$$

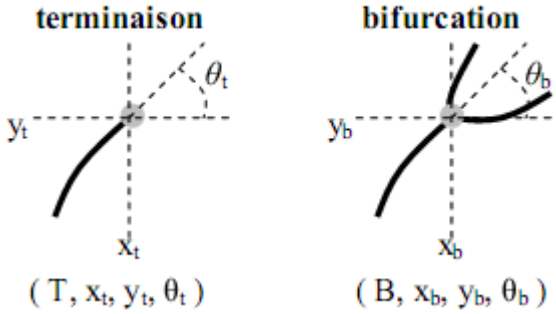


Figure III.22: Les caractéristiques extraites d'une minutie.

III.3.8.La comparaison

Après avoir effectué toutes les étapes de traitement précédentes ainsi que la désignation de l'empreinte de référence, on va faire une comparaison entre le fichier paramètres de l'empreinte candidate à l'authentification et celui de l'empreinte de référence (**Figure III.22**).

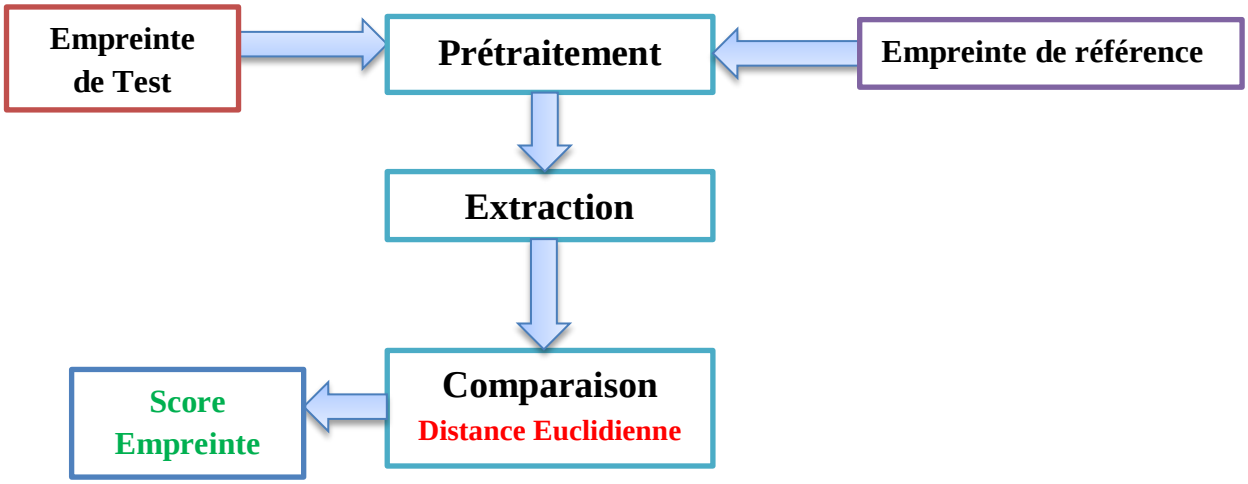


Figure III.23: Schéma général du processus de comparaison d'empreintes.

Étant donné $\mathbf{S_{ref}}$ **(i)** le fichier paramètres de l'empreinte référence du i^{éme} utilisateur et $\mathbf{S_{test}}$ **(i)** le fichier paramètres de l'empreinte de test du i^{éme} utilisateur. Les scores empreintes $\mathbf{S_{emp}}$ sont obtenus en utilisant la distance Euclidienne selon :

$$S_{emp} = \frac{1}{I}\sqrt{\sum_{i=1}^{I}(S_{refi} - S_{testi})^2} \qquad \textbf{(III.10)}$$

Cette différence cherche à faire déterminer un score qui représente le nombre de pairs de minuties identiques par rapport au nombre de minuties totales.

III.4. Système d'authentification de signatures manuscrite en ligne

La signature est l'une des tâches les plus personnelles et les plus uniques que l'être humain peut accomplir. Cette modalité biométrique comportementale est depuis longtemps le moyen le plus utilisé pour authentifier les documents, les personnes et les transactions bancaires et financières. Les systèmes de vérification des signatures manuscrites se rangent dans deux catégories selon le mode d'acquisition des données : hors ligne **[171]** et en ligne **[172]**. Le problème d'authentification des signatures manuscrites peut être approché selon deux types de méthodes : probabilistes (analytique) et structurelles. En conséquence, deux méthodologies peuvent être distinguées : méthodes globales **[173-177]** et méthodes locales **[178-180]**. Les méthodes globales consistent à authentifier une signature par l'extraction de ses caractéristiques globales telles que la vitesse moyenne, le temps global de la signature et le rapport (taille/largeur) de la signature, qui sont considérés comme des informations générales puisqu'elles ne sont pas très précises. En d'autres termes, un paramètre global contient peu d'information sans être très distinctif. Pour enrichir la quantité de l'information, l'approche globale doit généralement extraire plus de paramètres globaux (environ de 50 à 100) pour atteindre des performances acceptables. L'avantage des approches globales résident dans le faîte que toutes les signatures sont représentées par des vecteurs de la même longueur.

À la différence des méthodes globales, les méthodes locales visent à extraire plusieurs paramètres dans chaque point de la signature. La signature est finalement représentée par des vecteurs de grandes dimensions. Dans un système de vérification de signatures en ligne, les individus sont d'abord enregistrés en fournissant des échantillons de signatures définies comme des signatures de référence **[173]**. Dans un tel système, l'ordre chronologique des coordonnées des points issu de la tablette est bien connu ce qui permet de dégager les paramètres dynamiques spécifiques à la signature telle que la vitesse, la longueur du tracé et l'angle d'inclinaison.

III.4.1. Système proposé

Dans le système d'authentification de signatures manuscrit en ligne proposé, on extrait les cinq premières signatures de chaque utilisateur afin de les employer dans la phase d'apprentissage. Puis, quand un utilisateur prétendant être un client particulier du système présente sa signature pour l'authentification, elle sera comparée à sa signature de référence. Après cette comparaison, un score mesurant la similitude entre les deux signatures est fourni.

Le diagramme de notre système proposé est illustré par le diagramme de la **Figure III.24**. Notre système est séparé en deux blocs : un bloc de test et un bloc d'apprentissage. On doit noter que les opérations de prétraitement des signatures sont identiques pour les deux blocs considérés. Les phases principales composant ces deux blocs sont décrites dans ce que suit :

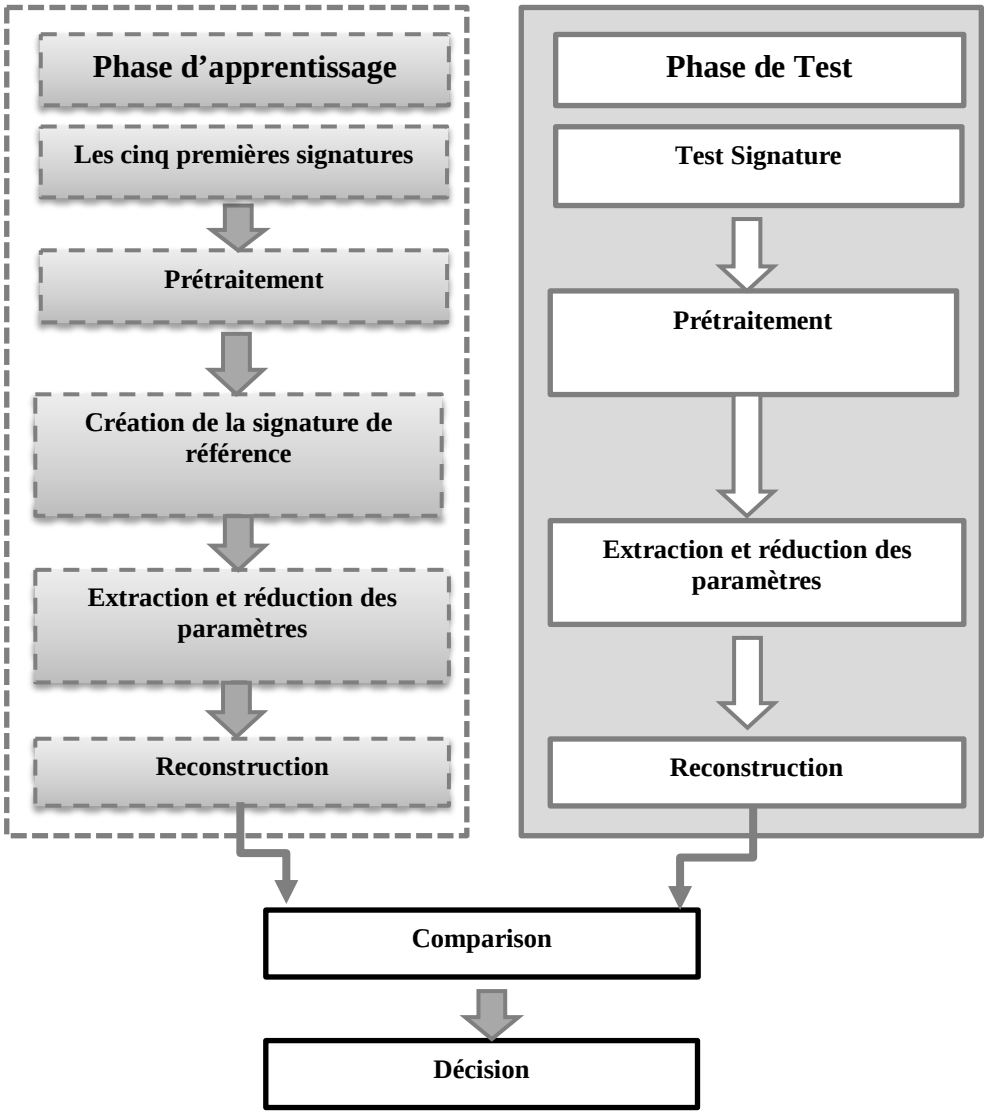


Figure III.24: Schéma général de notre système d'authentification de signature en ligne proposé.

III.4.2. Acquisition et prétraitement

La base de signatures utilisée dans ce travail est la base « **task1** » issue de la "First International Signature Verification Competition (SVC2004)" **[181]** ainsi que la base bimodale MCYT (empreinte et signature) **[167]** que nous allons décrire leurs caractéristiques au chapitre IV.

Le prétraitement est destiné à éliminer le bruit introduit lors de l'acquisition ainsi que la redondance de l'information. Cette opération consiste à éliminer le bruit d'écriture et la redondance d'information. Cette étape se compose de deux grandes sous-étapes importantes qui sont le filtrage et la normalisation. L'étape de filtrage repose sur l'utilisation de deux filtres : un filtre Gaussien et un filtre en distance. Une fois cette étape est achevée, elle est suivie par une étape de normalisation qui consiste à rendre toutes les signatures standard en tailles, en positons et en longueurs.

III.4.2.1. Filtre Gaussien

Ce filtre enlève les tremblements involontaires pendant le processus d'acquisition (**Figure III.25.b**) et peut être réalisé à l'aide d'un filtre gaussien unidimensionnel dans chacune des directions x et y selon :

$$x_f(t) = \sum_{i=-2\sigma}^{2\sigma} M_i * x(t+i) \qquad \textbf{(III.11)}$$

$$y_f(t) = \sum_{i=-2\sigma}^{2\sigma} M_i * y(t+i) \qquad \textbf{(III.12)}$$

Avec:

$$M_i = \frac{e^{-\frac{i^2}{2\sigma^2}}}{\sum_{j=-2\sigma}^{2\sigma} e^{-\frac{j^2}{2\sigma^2}}} \qquad \textbf{(III.13)}$$

Les expériences menées dans **[182]** affirment que les basses fréquences d'une signature sont les plus significatives. En effet, ces expériences prouvent que l'application d'un filtre avec une fréquence de coupure de 10 HZ préserve plus de 90% de la puissance de la signature. Ce filtre élimine les oscillations involontaires et fait le lissage de la signature tout en préservant sa structure globale.

III.4.2.2. Filtre en distance

Ce filtre est utilisé pour échantillonner la signature tout en gardant sa forme générale (**Figure III.25.c**). Ce filtre fonctionne comme suit :

Soit Pi (Xi, Yi) un point d'une signature, nous considérons tous les prochains points P_{i+1}, P_{i+2}, ... P_{i+k} jusqu'à trouver le point qui satisfait les critères suivants :

$$|X_i - X_k| \geq d \qquad \text{Ou} \qquad |Y_i - Y_k| \geq d \qquad \textbf{(III.14)}$$

Alors le point P_k est considéré comme le prochain point de P_i et tous les points intermédiaires entre P_i et P_k sont éliminés. Où "d " est un seuil de distance déterminé expérimentalement et égal à 0.3 millimètre. Ce seuil a une influence sur les performances de notre système. Ce que nous allons démontrer au chapitre V.

III.4.2.3. Normalisation en position

Pour normaliser une signature en position, l'approche qui consiste à aligner les signatures par leurs centres de la gravité **[183]** est adoptée. Pour effectuer cette opération entre deux signatures, on doit tout d'abord calculer les deux centres de gravité des deux signatures comme suit:

$$G_x = \frac{1}{N}\sum_{i=1}^{N} X_i \qquad \textbf{(III.15)}$$

$$G_y = \frac{1}{N}\sum_{i=1}^{N} Y_i \qquad \textbf{(III.16)}$$

Où N est le nombre de points de la signature.

Puis, on va glisser la signature de test pour la superposer sur la signature de référence (**Figure III.25.d**).

III.4.2.4. Normalisation en taille

La normalisation en taille, qui consiste à rendre toutes les signatures incluses dans une boîte de taille fixe, est donnée par :

$$x = \frac{x}{\sqrt{\sum_{i=1}^{n} x_i^{\,2} + y_i^{\,2}}} \qquad \textbf{(III.17)}$$

$$y = \frac{y}{\sqrt{\sum_{i=1}^{n} x_i^{\,2} + y_i^{\,2}}} \qquad \textbf{(III.18)}$$

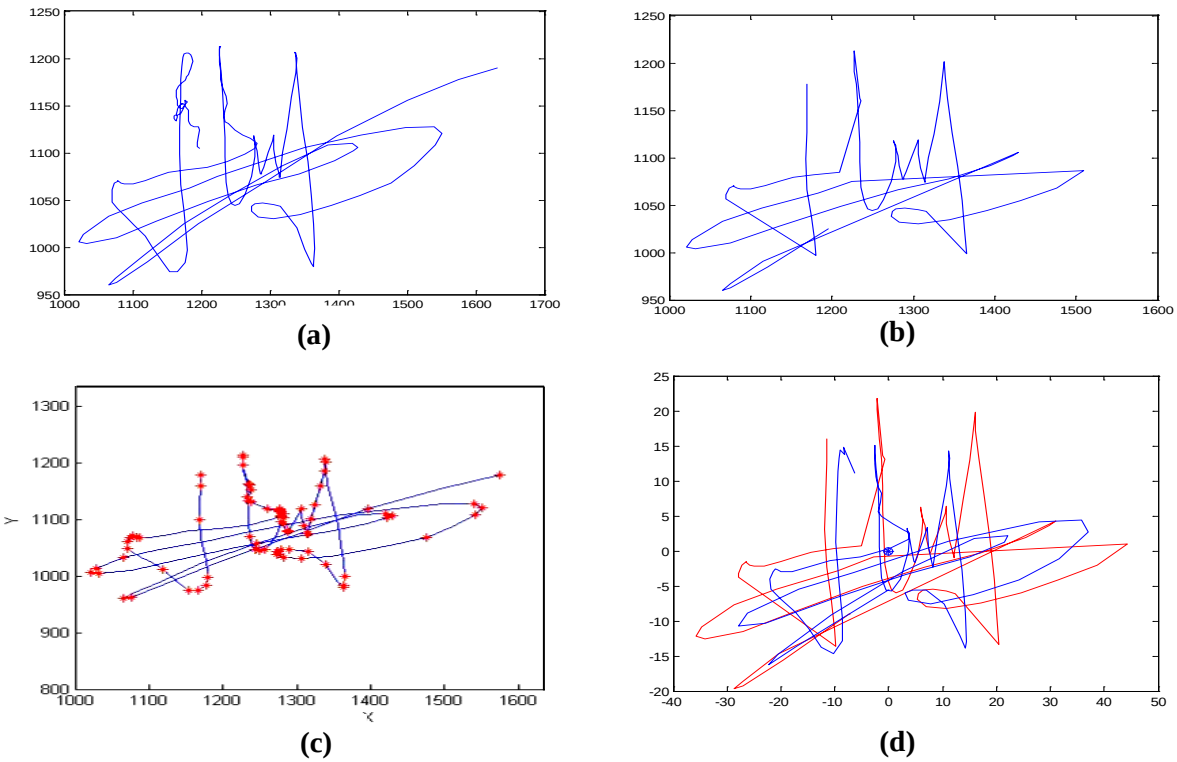


Figure III.25 : (a) La signature brute (b) La signature après filtrage Gaussien (c) la signature après filtrage en distance (d) Superposition de deux signatures par leur centre de gravité.

III.4.2.5. Normalisation en longueur

Cette opération ne conserve que quelques points importants de la signature. L'intérêt ici est multiple: elle permet de réduire la longueur de la signature et, par conséquent, d'accélérer le traitement. Elle permet aussi de diminuer l'espace de stockage requis pour chaque utilisateur.

Comme la taille et la position, la longueur d'une signature change en conséquence. Cette opération vise à rendre toutes les signatures avec le même nombre d'échantillons. Pour effectuer cette opération, nous avons essayé différentes techniques d'interpolation comme l'interpolation linéaire et l'interpolation polynomiale, mais nous avons opté pour l'interpolation bilinéaire **[184]** à cause de sa simplicité et de son succès dans le cas de deux variables. Cette dernière peut être interprétée comme étant une succession de deux interpolations linéaires, une dans chaque sens **[185]**. La longueur de la signature de référence est choisie comme longueur de référence et toutes les autres signatures sont interpolées afin d'avoir le même nombre d'échantillons comme celle de la référence.

Cette opération est très bénéfique pour le processus d'authentification, en particulier pour notre algorithme d'extraction de caractéristiques qui est conçu pour prendre des signatures avec la même longueur.

La figure suivante illustre x (t) de la signature de référence avec celui de cinq signatures d'un utilisateur avant et après la phase de normalisation

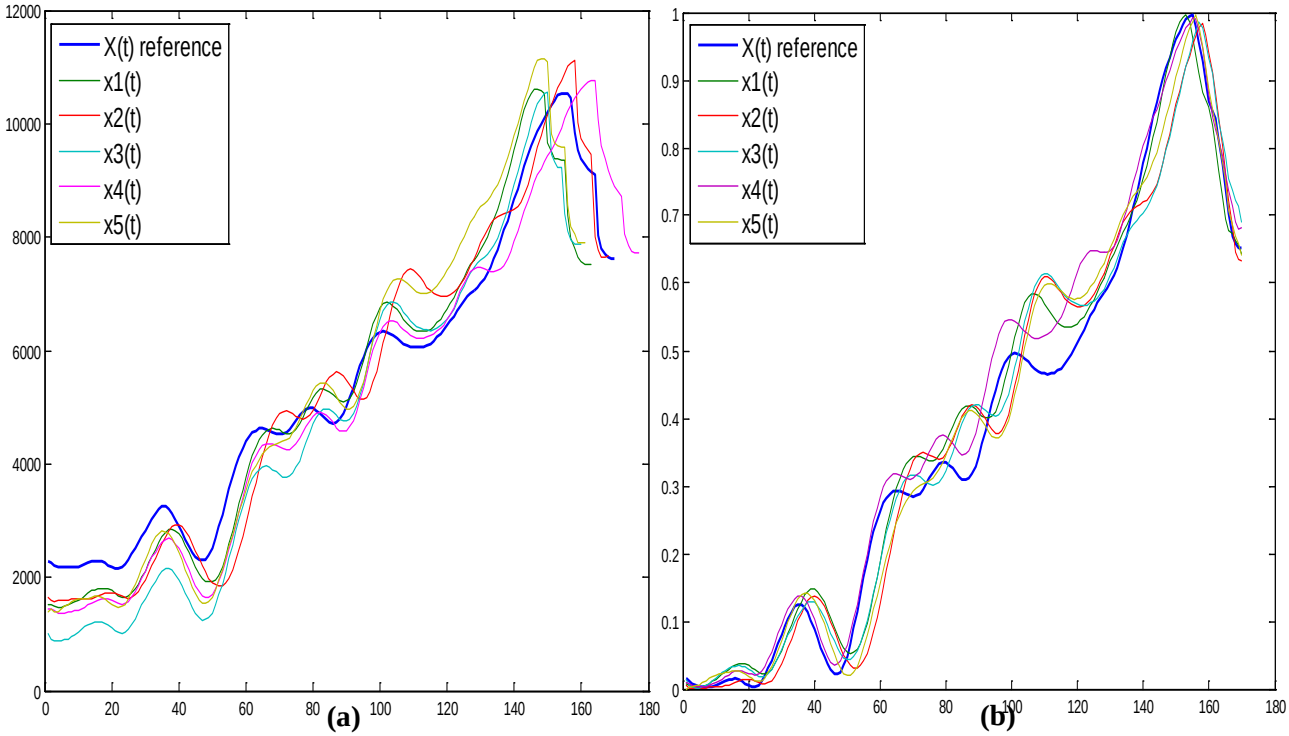


Figure III.26: x (t) de la signature de référence et des cinq signatures d'un utilisateur (a) avant la phase de normalisation (b) après la phase de normalisation.

III.4.3. L'apprentissage

Cette étape vise à créer le profil d'un utilisateur. Au cours de cette phase, les cinq premières signatures de chaque utilisateur de nos deux bases de données (SVC 2004 et MCYT-100) sont destinées pour la définition de la signature de référence, tandis que les autres signatures sont utilisées comme des signatures de test. Tout d'abord, ces cinq signatures sont filtrées et normalisées **(cf. section III.4.2)** .On doit noter que lors de l'application de l'interpolation bilinéaire, la longueur d'interpolation utilisée est la longueur moyenne de ces cinq signatures **(cf section III.4.2.5).**

Puis, après la phase de prétraitement, la signature de référence est calculée à partir de ces cinq signatures. Étant donné les cinq premières signatures [S1 (x1, y1) ... S5 (x5, y5)] d'un utilisateur qui a subi les opérations de prétraitement décrites précédemment, la signature de référence de cet utilisateur est définie par l'expression suivante:

$$S_{ref} = \frac{S_1 + S_2 + S_3 + S_4 + S_5}{5} \qquad \textbf{(III.20)}$$

La figure suivante montre comment la signature de référence est obtenue à partir des cinq premières signatures d'un utilisateur selon le dernier concept.

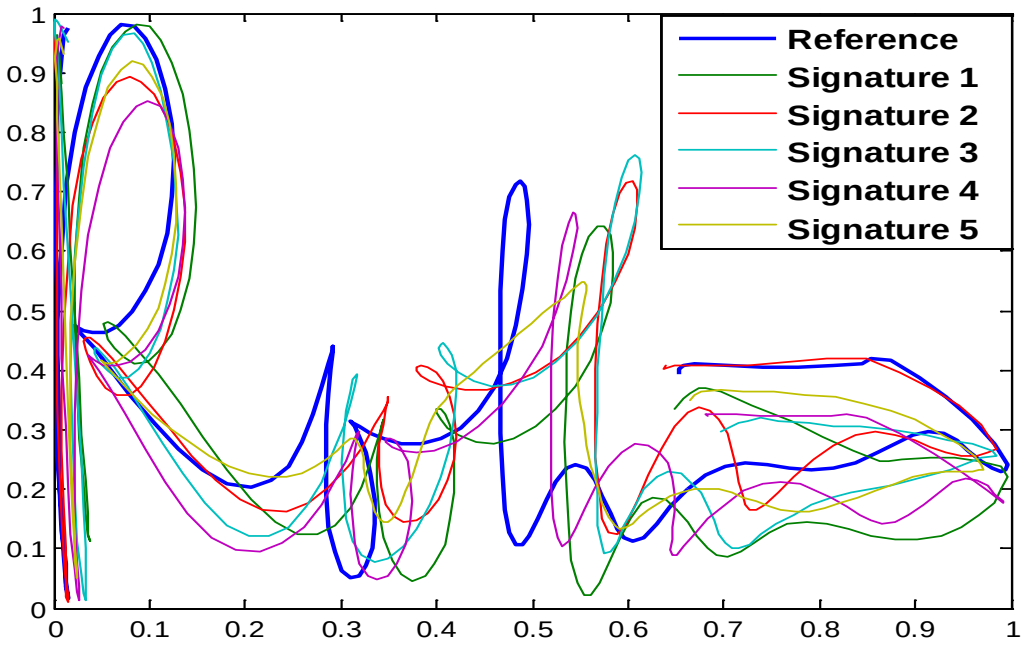


Figure III.27: La signature de référence

III.4.4. La phase de test

Ce processus vise à vérifier l'identité d'un utilisateur. Après avoir franchir les étapes de prétraitement et d'extraction de paramètres, la signature de test sera comparée à celle de référence afin de déterminer si elle est authentique ou pas. La comparaison est effectuée à l'aide de la distance Euclidienne qui donnera un score de similitude entre les deux signatures. Dans la prochaine section, le procédé destiné à l'extraction des paramètres d'une signature par l'approche EMD est présenté.

III.4.4. 1. Extraction des paramètres d'une signature par l'approche EMD

La décomposition modale empirique (***empirical mode decomposition EMD***) est une approche adaptative d'analyse temps-fréquence conçue pour les signaux non linéaires et non stationnaires **[186]**. L'EMD décompose un signal en un nombre fini de composants AM-FM appelés les fonctions intrinsèques de mode (***intrinsic mode functions IMFs***) utilisant un processus de tamisage (*shifting process*). L'extraction de ces modes permet de comprendre le contenu fréquentiel du signal.

L'approche d'EMD montre son efficacité comparant à d'autres approches de décomposition de signaux telles que la transformation en ondelettes discrète (DWT) **[187]**. Elle a beaucoup d'avantages tels qu'être une approche adaptative, non paramétrique et locale qui n'exige aucune connaissance antérieure du signal, et qui n'emploie aucune fonction prédéterminée.

En raison de ces avantages, la décomposition modale empirique (EMD) a fait l'objet de plusieurs travaux dans plusieurs domaines. Au début, l'EMD a été employé pour des applications géophysiques **[188]**, mais plus tard, elle a été introduite dans la science de l'ingénierie où plusieurs travaux ont été menés. L'EMD a été également employé en reconnaissance des formes et plus particulièrement pour les modalités biométriques comme une méthode de décomposition pour l'iris **[189]** et pour le visage **[190]**. Elle a été prolongée pour s'adapter aux données bidimensionnelles ou elle a été appliquée pour faire du traitement d'images **[191-193]** et l'analyse de la texture **[194]**. Dans le domaine du traitement des signaux, la méthode d'EMD a été utilisée comme étant un filtre **[195-196]** et pour détecter et analyser les signaux **[197-198]**. La décomposition modale empirique a été également employée pour analyser les séquences impulsionnelles des radars **[199]**.

La signature manuscrite en ligne est représentée par un ensemble de signaux numériques en fonction du temps. Les paramètres obtenus dépendent du type de dispositif d'acquisition de la signature. Les paramètres basiques obtenus directement du dispositif d'acquisition sont : la forme de la signature, représentée par les coordonnées (abscisse x(t) et ordonnée y(t)) du stylo à chaque point d'acquisition. À partir de ces deux paramètres de base, plusieurs autres paramètres, représentant les caractéristiques dynamiques qui augmentent la discrimination entre les signatures, peuvent être extraits. Dans notre cas, nous avons utilisé le concept de la décomposition modale empirique (EMD) pour extraire d'autres paramètres pouvant discriminer les signatures entre elles.

III.4.4.2.Obtention des IMFs: l'algorithme EMD

Étant donné un signal monodimensionnel S(t), Les étapes suivantes montrent comment les IMFs sont calculés. À noter que chaque IMF doit satisfaire deux conditions nécessaires: la première est que le nombre d'extrema et passages par zéro doivent soit être identiques ou ne diffèrent que par un. Le second est que la valeur moyenne entre les deux enveloppes (supérieur et inférieur) est nulle à tout moment.

Étape 1. Initialisation : x(t)= S(t), i=j = 1

Étape 2. Trouver tous les maxima et minima locaux du signal $x_{j-1}(t)$

Étape 3. Génération de l'enveloppe supérieure E_{up} en utilisant la *spline cubique interpolation* des maxima locaux et l'enveloppe inférieure E_{low} en utilisant la *spline cubique interpolation* des minima locaux.

Étape 4. Calcul de l'enveloppe moyenne E_{j-1} selon l'expression suivante:

$$E_{j-1} = \frac{(E_{up} + E_{low})}{2} \qquad \textbf{(III.21)}$$

Étape 5. Soustraire l'enveloppe moyenne E_{j-1} du signal original:

$$x_j(t) = x_{j-1}(t) - E_{j-1} \qquad \textbf{(III.22)}$$

Étape 6. Répétez les étapes de 2 à 5 avec j = j+1 jusqu'à $x_j(t)$ sera un IMF.

Étape 7. On met $Imf_i(t)=x_j(t)$ et nous calculons le résidu $r_i(t)$:

$$r_i(t) = r_{i-1}(t) - Imf_i(t) \qquad \textbf{(III.23)}$$

Étape 8. Répétez les étapes de 2 à 7 avec i=i+1 jusqu'à $r_i(t)$ soit monotone.

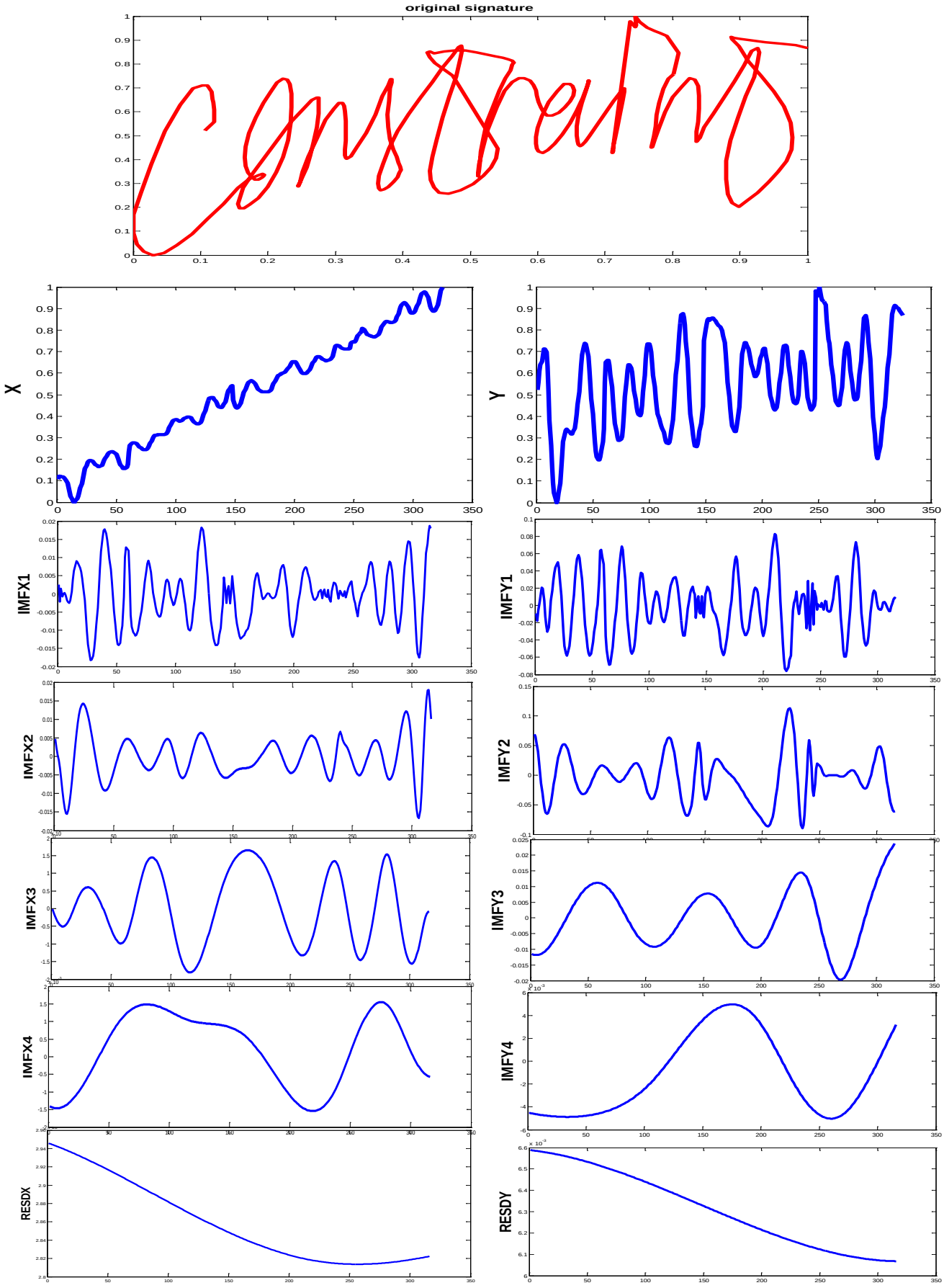
À un certain moment, un critère d'arrêt (SD) est défini afin d'assurer la convergence de l'algorithme itératif. L'arrêt aura lieu lorsque la différence entre deux itérations consécutives est sous un seuil selon l'expression suivante:

$$SD = \sum \left| E_{j-1}(t) \right| \leq \varepsilon \qquad \textbf{(III.24)}$$

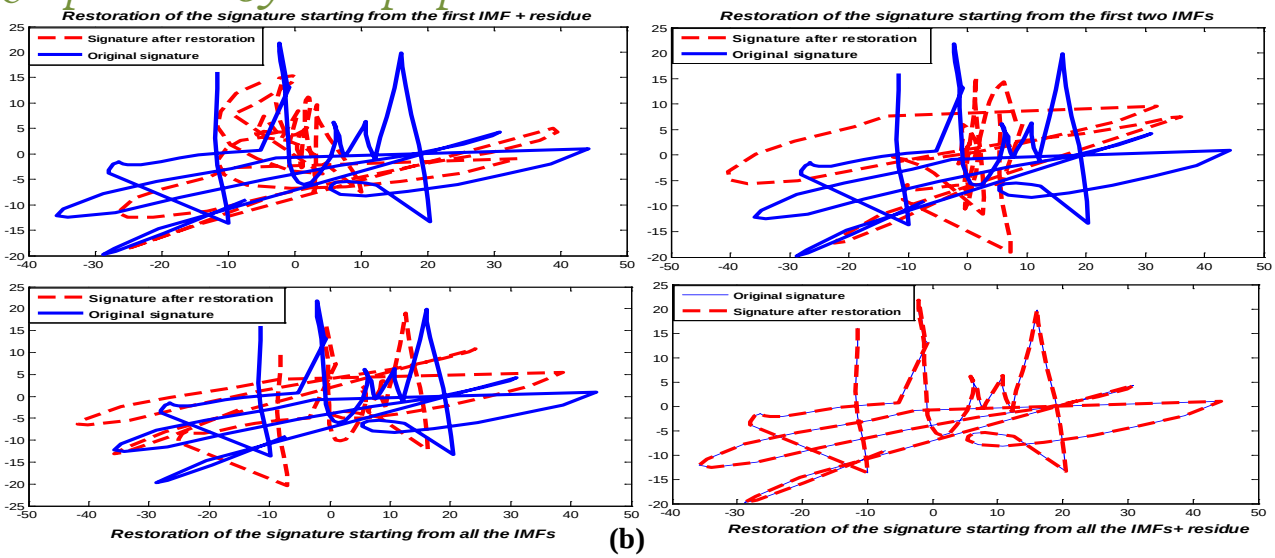
ε est pris généralement entre 0,2 et 0,3 **[200]**. Dans notre cas, le critère d'arrêt est réglé à 0,2 **[201]**. Ce critère affecte l'EMD et, par conséquent, tout le processus d'authentification. En ce sens, si on considère une valeur de SD trop faible, un nombre important d'IMF sera obtenu dont certains d'entre eux ne sont pas significatifs pour nous tandis que les itérations seront très longues. Dans le cas contraire, si on prend une grande valeur de SD, la séparation entre les modes intrinsèques ne sera pas une tâche possible. On note que le premier et le dernier IMFs contiennent respectivement la fréquence d'oscillation plus faible et la plus élevée, tandis que le résidu représente la composante continue du signal. Une fois que la décomposition est terminée, S(t) peut être écrit de la manière suivante:

$$S(t) = r(t) + \sum_{i=1}^{n} Imf_i(t) \qquad \textbf{(III.25)}$$

Comme nous l'avons mentionné, la signature manuscrite en ligne est représentée par les coordonnées x(t) et y(t) du stylo en chaque point d'acquisition. La décomposition modale empirique de ces deux signaux permet de caractériser une signature par de nouveaux paramètres qui sont les IMFs des signaux x(t) et y(t). Ces paramètres sont regroupés dans un vecteur Vemd= [IMFx, IMFy]. Nous pouvons ainsi décomposer et reconstruire une signature à partir de ces nouveaux paramètres. La reconstruction peut être une reconstruction parfaite (obtenue à partir de la somme de tous les IMFs), rapprochée (somme de quelques IMFs) ou pondérée (somme de quelques IMFs pondérées). Les poids de pondération sont déterminés expérimentalement. Nous focalisons la suite de notre travail sur le cas de la reconstruction d'une signature à partir de la somme de tous ces IMFs. La **Figure III.28** illustre un exemple de la décomposition et la reconstruction d'une signature par l'EMD.


original signature
X
Y
IMFX1
IMFY1
IMFX2
IMFY2
IMFX3
IMFY3
IMFX4
IMFY4
RESDX
RESDY

(a)



(b)

Figure III.28: (a) Décomposition d'une signature par l'EMD (b) Reconstruction d'une signature à partir de combinaison entre IMFs.

III.4.4.3.Réduction de l'espace de représentation des paramètres

Le vecteur paramètres Vemd défini précédemment ne peut être utilisé pour caractériser une signature à cause de son volume important. Pour pallier ce problème, nous avons défini un nouveau vecteur (VemdN) composé uniquement des maximas et des minimas des IMFs. L'algorithme d'extraction de ces extrema est le même que celui utilisé dans **[202]**, qui comprend une procédure de suppression de faux extrema. Le nouveau vecteur caractérisant une signature est : VemdN =[EXTREMAIMFx,EXTREMAIMFy]. Ce vecteur nous permet de reconstruire le signal original d'une manière approchée par une technique d'interpolation choisie (*Spline cubique* pour notre cas). La **Figure III.29** illustre le principe de reconstruction par VemdN.

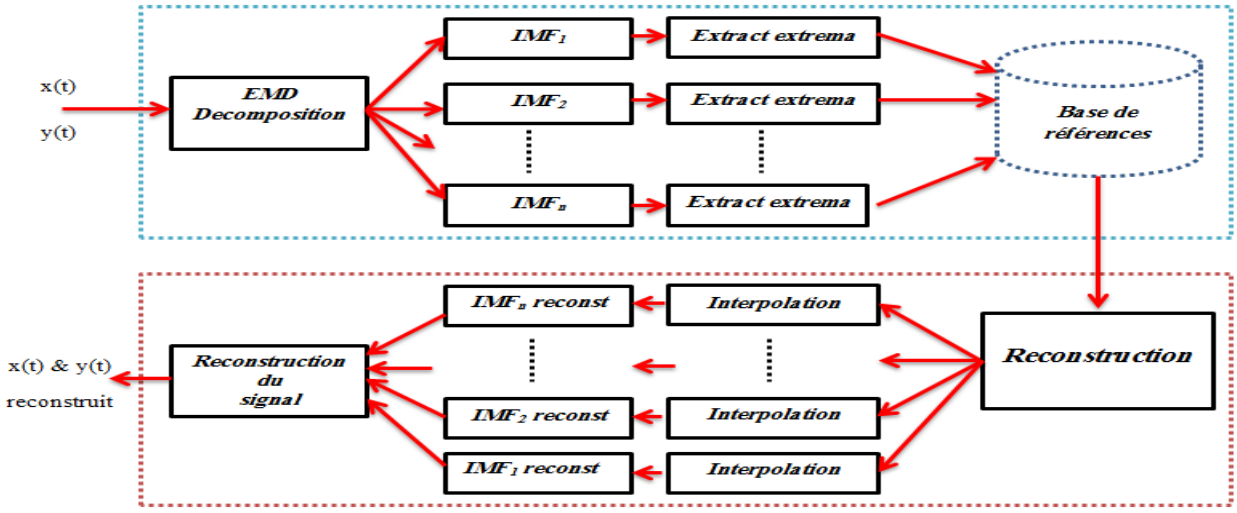
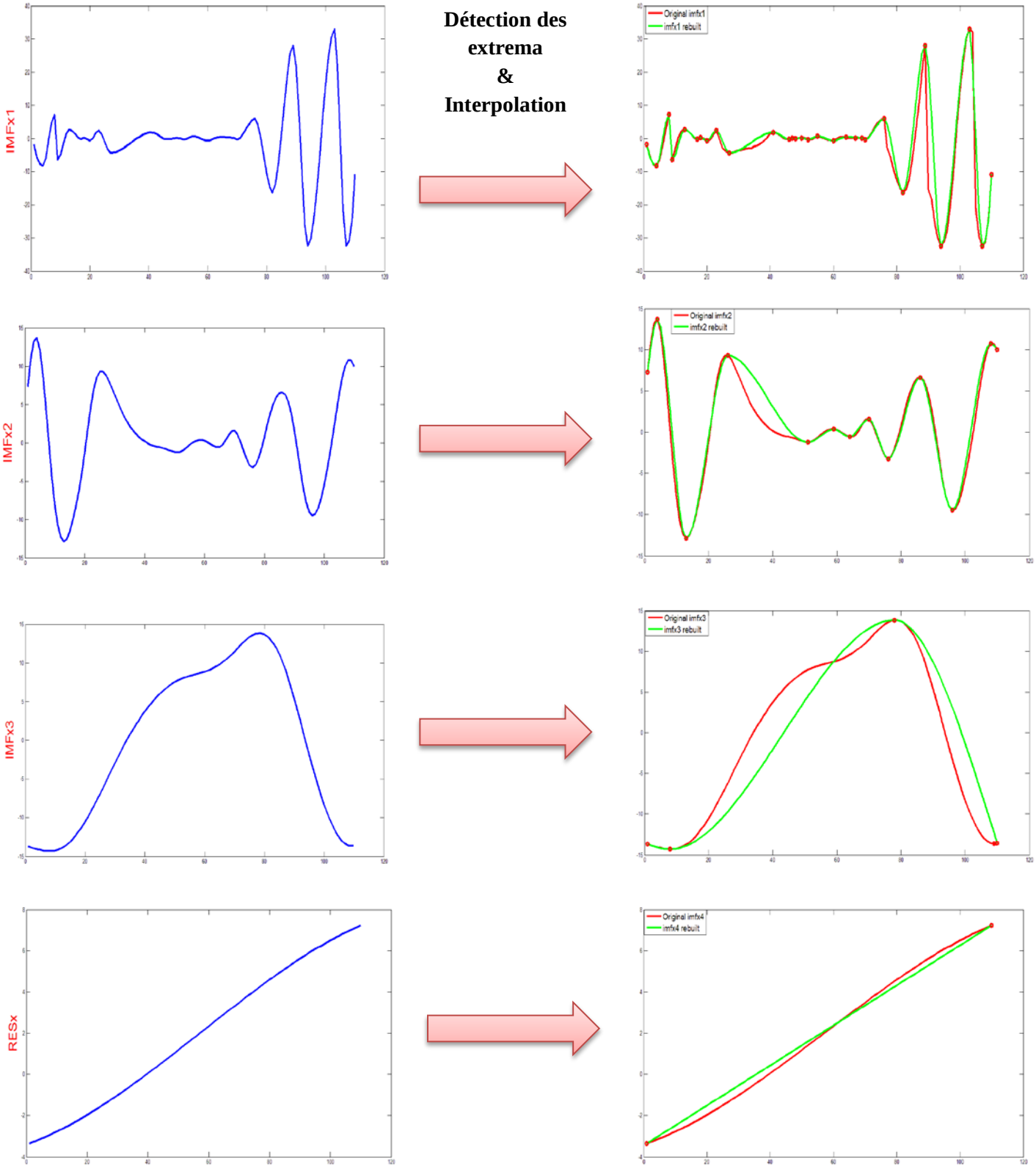
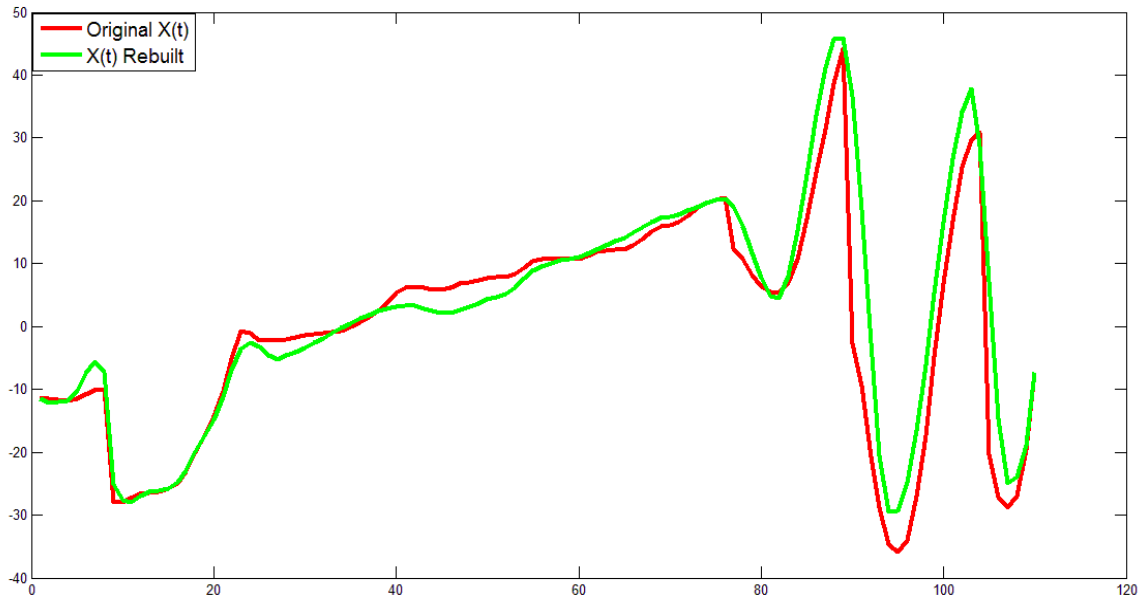


Figure III.29: Principe de reconstruction d'une signature par les extremas d'IMFs

La figure **III.30** illustre un exemple de reconstruction de x (t) à partir des extrema de ces IMFs.



(a) **(b)**



(c)

Figure III.30 : Exemple de reconstruction de x(t) à partir des extrema de ces IMFs : (a) Les IMFs du signal x(t) (b) interpolation des Extrema (courbe rouge) (c) reconstruction de x(t) à partir des extrema des IMFs (courbe rouge).

III.4.5. La comparaison

Cette phase cherche à dégager un score de comparaison entre une signature candidate à l'authentification et celle de référence d'un utilisateur.

La comparaison s'effectue par le calcul de la distance Euclidienne entre la signature test et référence reconstruite à partir de VemdN. Les points suivants constituent la partie essentielle de notre contribution au niveau du bloc de comparaison :

1. Présentation des bases de données des signatures.
2. Associer à chaque signature de la base un vecteur VemdN destiné à reconstruire une signature à partir de ses extrema (cf section **III.4.4.3**).
3. Obtenir la signature de test reconstruite d'une manière approchée par *spline cubique* interpolation à partir des extrema stocké dans VemdN .
4. Obtenir la signature de référence et sa signature reconstruite.
5. Calculer de la distance Euclidienne entre la signature de test et de référence reconstruite à partir de leur extrema: si T désigne une signature de test d'un tel utilisateur et R

indique sa signature de référence, la distance Euclidienne entre la signature de test et celle de référence est définie par:

$$D(T,\ R) = \sqrt{\sum (T - R)^2} \qquad \textbf{(III.26)}$$

III.5. Conclusion

La signature manuscrite en ligne et l'empreinte digitale sont deux modalités biométriques de nature différente, la première est comportementale alors que la deuxième et morphologique. Cette différence s'avère très bénéfique lorsque ces deux modalités sont fusionnées parce elle permet de caractériser une personne de façon très subjective et très complémentaire. Dans ce chapitre, nous avons fait un tour d'horizon des étapes de notre système proposé de fusion entre l'empreinte digitale et la signature manuscrite en ligne. Nous avons aussi défini chaque système (empreinte et signature) de façon séparée. Les méthodes principales associées à chaque phase de notre système ainsi que leurs déroulements sont décrites dans ce chapitre avec une grande précision. Le chapitre suivant sera consacré à la présentation des mécanismes de fusion et de décision ainsi que la description des bases de données utilisées dans notre travail.

Chapitre IV

Validation et concrétisation de la démarche adoptée

IV.1 Introduction

L'idée de combiner des informations venant de plusieurs sources et portant sur un même phénomène est une idée très simple qui vient naturellement à l'esprit. Nous faisons souvent cette combinaison dans notre vie quotidienne. Par exemple, un expert humain reçoit l'information de plusieurs sources d'entrée, l'assimile et propose des conclusions. Cependant, il faut différencier entre le terme combinaison d'informations et fusion d'informations d'une part et entre le terme fusion de données d'autre part. En fait, l'idée principale de la fusion de données est de combiner différentes informations relatives à un problème, les informations fusionnées pouvant être de natures très variées et provenant de plusieurs sources. Ces informations peuvent être des données provenant de sources différentes ou bien présentant des caractéristiques différentes, extraites des mêmes données initiales comme c'est le cas pour nos deux modalités biométriques en occurrence l'empreinte digitale et la signature manuscrite en ligne. Pour cette raison on trouve souvent dans la littérature le terme fusion d'information au lieu de fusion de données. Il y a eu plusieurs définitions du terme fusion d'information. En effet, le terme est souvent confondu avec le terme fusion de données. En outre, il a été suggéré d'utiliser le terme combinaison d'informations dans un sens beaucoup plus large que la fusion d'informations. En tout cas, ces termes définissent tout processus impliquant une opération mathématique effectuée sur au moins deux sources d'information. Ces définitions sont dissociées intentionnellement et offrent différentes interprétations. La combinaison n'est pas définie comme un terme opposé à la fusion. Elle est simplement plus générale, elle est utilisée souvent pour décrire des processus et des méthodes d'une manière générale, sans tenir compte des détails. L'intégration peut jouer un rôle semblable bien qu'elle se réfère implicitement davantage à la concaténation (c.-à-d. augmentant le vecteur d'observations) qu'à l'extraction d'information pertinente.

Dans ce chapitre nous allons nous focaliser sur les détails liés à la méthode de fusion adoptée. De plus, nous présenterons des descriptions sur les bases de données utilisées lors de la validation et concrétisation de la démarche adoptée. Enfin, nous illustrons le protocole d'évaluation ainsi que les règles de décision.

IV.2. Méthode de fusion en scores adoptée

L'architecture générale de notre démarche de fusion en scores adoptée est illustrée dans la **Figure (IV.1).**

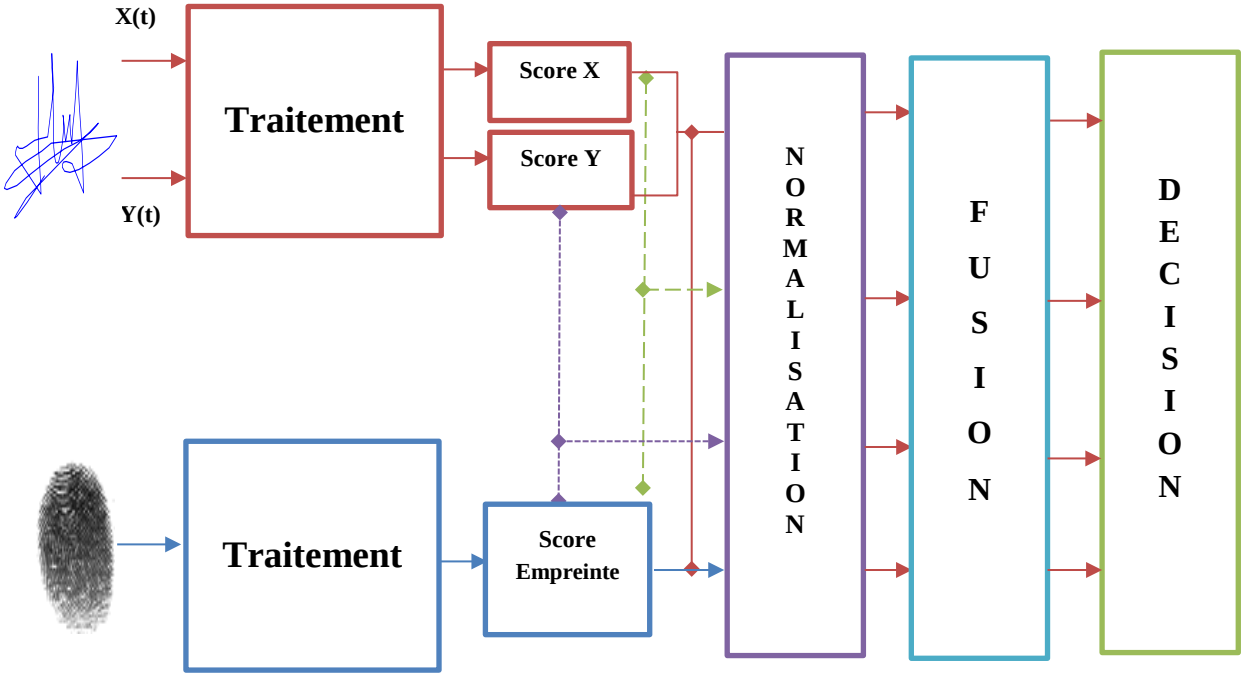


Figure IV.1 : Architecture du système d'authentification biométrique multimodale proposé.

Comme on peut constater sur la figure, nous avons considéré plusieurs combinaisons de fusions. Après avoir subi les différents traitements décrits au chapitre précédent, les scores de chaque système sont d'abord normalisés avant d'aborder l'étape de fusion. On a essayé trois types de méthodes de normalisation (Min-Max , Z-score, Tanh) pour le but de considérer l'ampleur d'une méthode ou d'une autre sur les performances de notre système.

Une fois normalisés, les scores sont prêts pour être fusionnés. On a effectué quatre combinaisons de fusion. Premièrement, on a réalisé une fusion intermodalité entre deux caractéristiques provenant de la même modalité (x(t) et y(t) de la signature manuscrite), puis on

s'est focalisé sur la fusion multimodale ou on a fusionné le score de l'empreinte avec chacun des scores de la signature de façon séparée avant de faire une fusion de tous les scores à la fois.

Notre méthode de fusion se base sur une règle de somme pondérée. La somme pondérée est une combinaison convexe des scores. Cette méthode cherche à attribuer des poids à chaque score en fonction de sa fiabilité. Les poids sont estimés en fonction de l'influence du score sur les performances finales du système.

Après avoir été introduite par **Zadeh (1963)** **[203]** , la somme pondérée a été mentionnée en évidence dans la littérature. Elle a été utilisée pour fusionner des modalités biométriques telles que la signature manuscrite en ligne **[204]**, l'iris et le visage **[205]**.

Le plus grand avantage de cette méthode est sa simplicité et son cout de calcul très faible.

Soit S_1,…..S_k les scores issue de la comparaison des différents vecteurs paramètres de nos modalités. Le score de fusion est donné par :

$$S = \sum_{i=1}^{K} w_i S_i \qquad \textbf{(IV.1)}$$

Où w_i sont les poids associés à chaque type de modalité. Ces poids représentent le degré de fiabilité des modalités. Si les poids sont tous égaux, nous nous ramenons au cas du principe du vote majoritaire. L'estimation des poids et donc de la fiabilité peut se faire selon plusieurs critères **[206]**.

Dans notre travail, on a choisi la méthode qui les calcule à partir des erreurs (EER) de chaque système comme suit **[207]**:

$$w_i = \frac{EER_i}{\sum_{m=1}^{N} EER_m} \qquad \textbf{(IV.2)}$$

Notons que $0 \le w_i \le 1$, $\sum w_i = 1$ et que les poids sont inversement proportionnels. Ainsi, plus la modalité est discriminante, plus son poids est important et vice versa.

Dans notre cas, pour chacune des quatre combinaisons proposées, nous allons calculer les poids de la somme pondérée en fonction des performances de chaque sous-système de façon séparé.

IV.3. Base de données utilisée

Comme nous avons énoncé au paravent, nous avons mené nos tests sur trois bases de données, une base de signatures manuscrites en ligne (**SVC 2004**[181]), une base d'empreintes digitales (**FVC2004** [166]) et une base bimodale composée d'empreintes et signatures (**MCYT-100**[167]). Dans ce qui va suivre, nous allons décrire chacune de ces bases en donnant leurs caractéristiques et leurs façons d'acquisition :

IV.3.1 Base de signatures en ligne SVC 2004

La base **SVC2004** pour *First International Signature Verification Competition* est une base de données de signatures en ligne issue d'une compétition de vérification. La **SVC2004** se compose de deux bases de signatures séparées. On a considéré la première base dans notre travail.

Cette base de données appelée "**task1**" contient des signatures recueillies à partir de quarante utilisateurs. Pour des raisons de sécurité, ces utilisateurs ne fournissent pas leurs vraies signatures utilisées lors de leurs vies quotidiennes, mais de nouvelles signatures dont il l'on pratiquer plusieurs fois. Pour chaque utilisateur, il y a 20 signatures authentiques et 20 signatures imitées provenant d'au moins quatre autres personnes. Les imitateurs peuvent voir toutes les signatures authentiques et peuvent aussi s'entrainer à les imiter à plusieurs tentatives jusqu'au moment où ils sont confiants de les avoir maitrisées.

Chaque fichier de signature fournit: les coordonnées x et y, le temps, le levé de plume, l'azimut, l'altitude et la pression. Les signatures sont acquises dynamiquement au moyen d'une tablette à digitaliser de type WACOM Intuos Tablet.

En outre, la plupart des signatures de cette base sont en l'anglais ou en Chinois. Bien que la plupart des signataires soient des Chinois, on trouve un bon nombre d'entre eux qui utilisent

des signatures anglaises dans leurs vies quotidiennes. La figure suivante illustre quelques exemples de signatures de cette base de données.

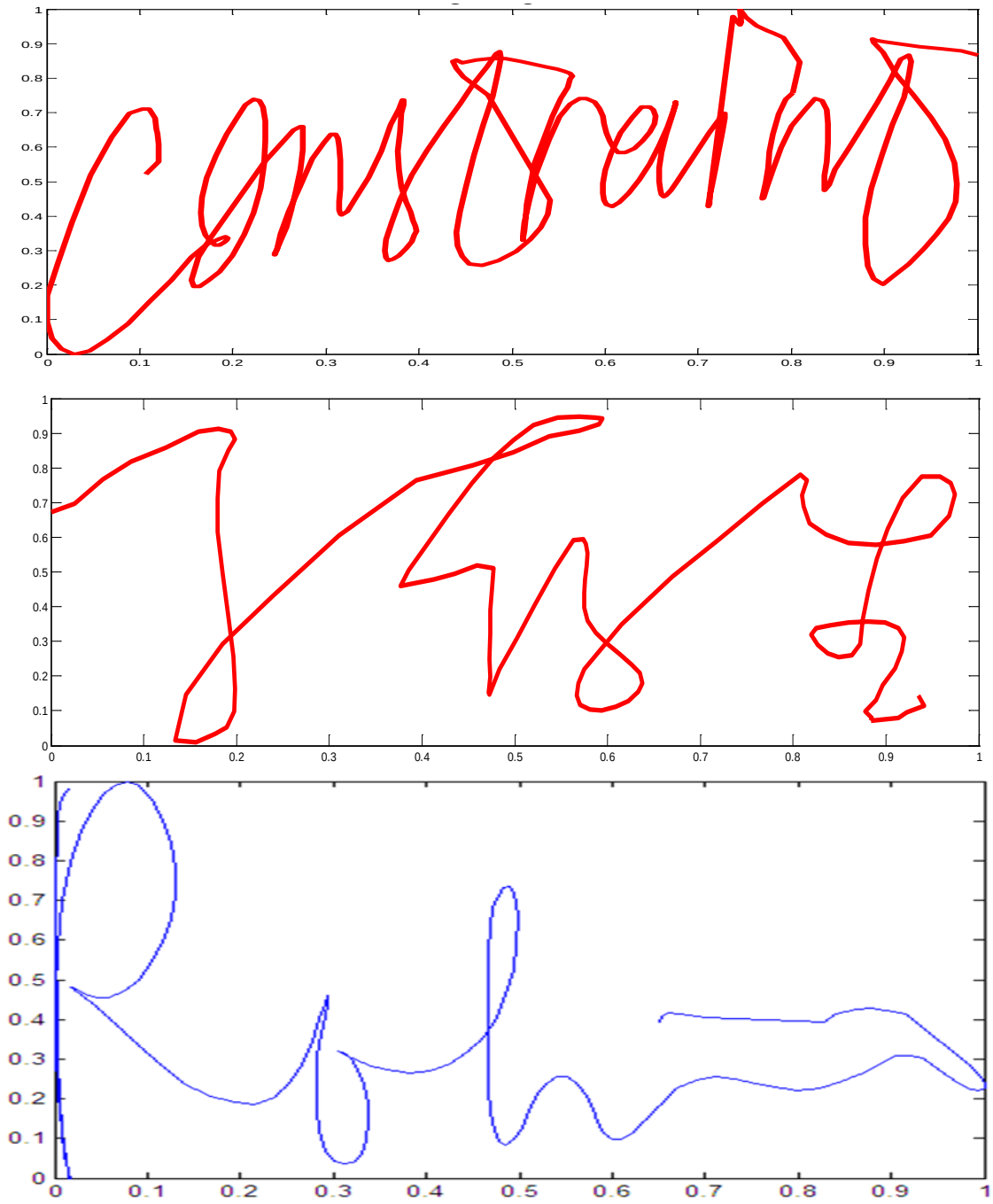


Figure IV.2: Exemples de signatures de la base de données SVC 2004.

IV.3.2 Base d'empreintes digitales FVC 2004

La base **FVC2004** pour *the third international Fingerprint Verification Competition* est une base de données d'empreintes digitales issue d'une compétition de vérification. La **FVC 2004** contient trois bases réelles et une synthétique. Dans notre travail, on a pris la première base appelée « DB1 » comme base de test.

Cette base a été acquise au moyen d'un capteur optique de type *CrossMatch V300* avec une résolution de 500 dpi. Les images acquissent des empreintes digitales sont de taille 640×480 et provenant de trente étudiants volontaires (24 ans de moyenne d'âge). Chaque volontaire a été invité à présenter son empreinte en trois sessions distinctes, avec au moins un temps de deux semaines séparant chaque session. Aucun effort n'a été fourni pour contrôler la qualité d'image ni pour nettoyer le capteur.

Dans chaque session, quatre impressions sont acquises de chacun des quatre doigts de chaque volontaire. Enfin d'acquisition, cette base contient un recueil de 120 doigts avec 12 impressions par doigt (1440 impressions) provenant de 30 volontaires. La figure suivante illustre quelques exemples de signatures de cette base de données.

Figure IV.3: Exemples d'empreintes de la base de données FVC 2004.

IV.3.3 La base bimodale MCYT-100 (Empreinte et signatures)

La base MCYT-100 est une base de données biométrique bimodale qui contient à la fois des signatures manuscrites et des empreintes digitales proposées par " *Biometric Recognition Group - ATVS* "de l'université de Madrid.

La base de signature manuscrite en ligne a été acquise à l'aide d'une tablette graphique WACOM modèle INTUOS A6 USB. La résolution de la tablette est de 2540 lignes par pouce, avec une précision de ± 0,25 mm. Elle a une surface active de 127 x 97 mm avec une fréquence d'échantillonnage de 100 Hz. Cet appareil peut enregistrer à chaque échantillon les coordonnées x et y de la signature, la pression, l'azimut et l'altitude. Chaque utilisateur fournit 25 signatures authentiques accompagnées de 25 imitations produites par 5 autres utilisateurs. Ces imposteurs imitent les signatures authentiques en observant leurs images statiques puis ils entrainent à leurs reproductions plusieurs fois (au moins 10 fois) jusqu'ils soient sure de les avoir maitrisées. Enfin cette base contient 2500 signatures authentiques et 2500 imitations issues de 100 utilisateurs.

Quant à la base d'empreinte digitale, elle a été acquise au moyen de deux capteurs. Le premier est un capteur capacitif de modèle 100SC avec une résolution de 500 dpi . Le deuxième est un capteur optique de modèle *UareU* qui possède la même résolution que son antécédent. L'image de sortie de l'empreinte est de 300×300 pixels et 256 ×400 pixels pour le premier et le deuxième capteur respectivement. Le processus d'acquisition d'empreinte digitale de cette base est accompli sous la surveillance attentive d'un opérateur.10 échantillons d'empreintes sont acquise pour chaque utilisateur. Chaque échantillon est acquis 12 fois dans le but de permettre d'évaluer les systèmes dans différentes conditions d'acquisition comme suit :

- 3 échantillons avec une basse résolution.
- 3 échantillons avec une moyenne résolution
- 6 échantillons avec une haute résolution.

Par conséquent, chaque individu fournit un nombre total de 240 images d'empreinte digitale à la base de données (10 échantillons × 12 d'impression/échantillons × 2 capteurs). La figure suivante illustre un exemple de données contenu dans cette base de données bimodale.

(a)

(b)

Figure IV.4: Exemples de données de la base bimodale MCYT-100 (a) Empreintes digitales (b) signatures manuscrites en ligne.

IV.4. Protocole d'évaluation et de décision

Les métriques présentées dans la littérature pour évaluer les performances d'un système biométrique sont efficaces et complètes. Après avoir dégagé et normalisé les scores de chaque modalité, ces derniers vont être confrontés à l'étape de décision ou leurs performances sont évaluées.

Comme nous l'avons décrit au chapitre I, lorsqu'un système fonctionne en mode authentification, celui-ci peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejet (*false rejection*). Comme il peut accepter un imposteur et on parle dans ce second cas de fausse acceptation (*false acceptance*). La performance de notre système de fusion multimodale se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et a son taux de fausse acceptation (False Acceptance Rate ou FAR) et aussi au taux d'erreur égal (EER). Note algorithme d'évaluation et décision est comme suit :

- Soit H_0 l'hypothèse que le score S provient d'un imposteur
- Soit H_1 l'hypothèse que le score S provient d'un utilisateur authentique. Il faut donc choisir l'hypothèse la plus probable.
- On considère que le score S provient d'un utilisateur authentique si $P(H_1/S) > P(H_0/S)$. En appliquant la loi de Bayes on obtient :

$$\frac{P(S/H_1)P(H_1)}{P(S)} > \frac{P(S/H_0)P(H_0)}{P(S)} \qquad \textbf{(IV.3)}$$

Et donc :

$$\frac{P(S/H_1)}{P(S/H_0)} > \frac{P(H_0)}{P(H_1)} \qquad \textbf{(IV.4)}$$

Comme les valeurs de $P(H_0)$ et $P(H_1)$ qui représentent respectivement la probabilité pour qu'un imposteur ou un utilisateur authentique essayent d'accéder au système sont des

valeurs difficilement estimables, on compare alors le taux de vraisemblance (*likelihood ratio*) $\frac{P(S/H_1)}{P(S/H_0)}$ à un seuil θ appelé seuil de décision.

Nous avons représenté sur la **Figure IV.5** la distribution hypothétique des taux de vraisemblance qu'obtiendraient les utilisateurs authentiques et les imposteurs de l'une des combinaisons de fusion de notre système proposé. Idéalement, le système devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Plus le seuil de décision θ est bas, plus le système acceptera d'utilisateurs authentiques, mais plus il acceptera aussi d'imposteurs. Inversement, plus le seuil de décision θ est élevé, plus le système rejettera d'imposteurs, mais plus il rejettera aussi d'utilisateurs légitimes.

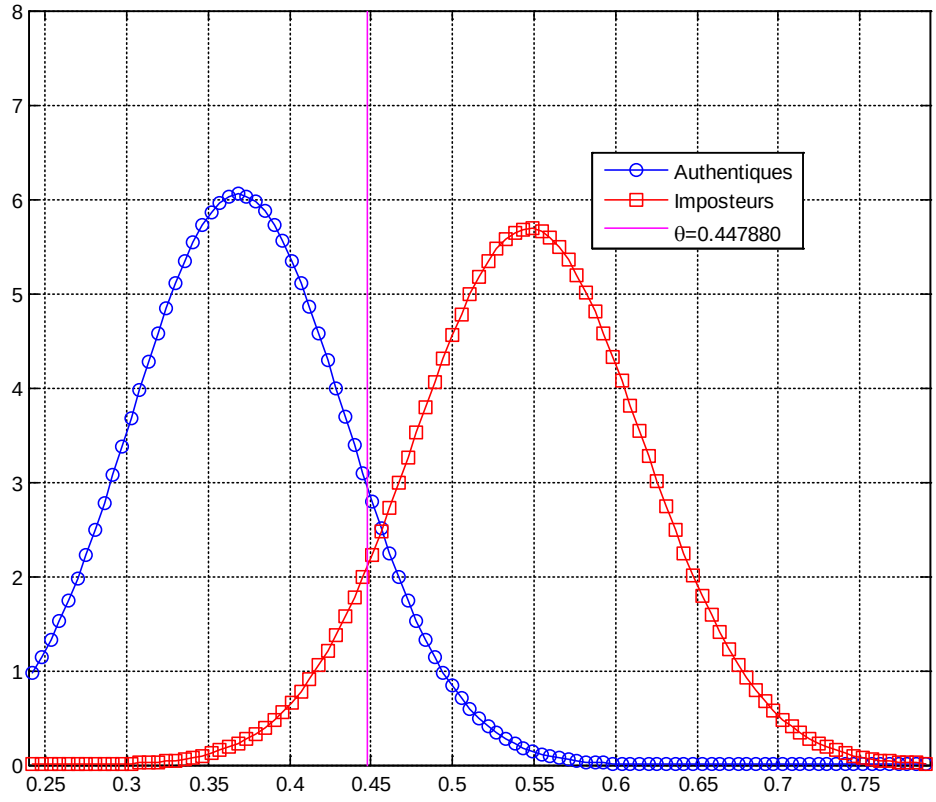


Figure IV.5: Distributions des taux de vraisemblance des utilisateurs authentiques et des imposteurs d'une combinaison de fusion de notre système multimodale

Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps.

Pour évaluer notre système multimodal, nous avons utilisé la courbe dite DET (*Detection error tradeoff*), représentée à la **Figure IV.6**, qui permet de représenter graphiquement les performances de notre système pour des différentes valeurs de θ. Notre système est évalué en matière de taux d'erreur égal (Equal Error Rate ou EER) qui correspond au point où le FAR et FRR sont égaux, ce qui équivalant graphiquement à l'intersection de la courbe DET avec la première bissectrice.

Ce type d'erreur est fréquemment utilisé pour donner un aperçu de la performance d'un système biométrique. Le seuil θ doit donc être ajuste en fonction de l'application ciblée : haute sécurité, basse sécurité ou un compromis entre les deux. Dans notre cas, on va s'intéresser au dernier type tout en variant le seuil de décision et calculer à chaque fois les valeurs du FAR et le FRR jusqu'à atteindre le seuil de compromis entre le FFR et le FAR.

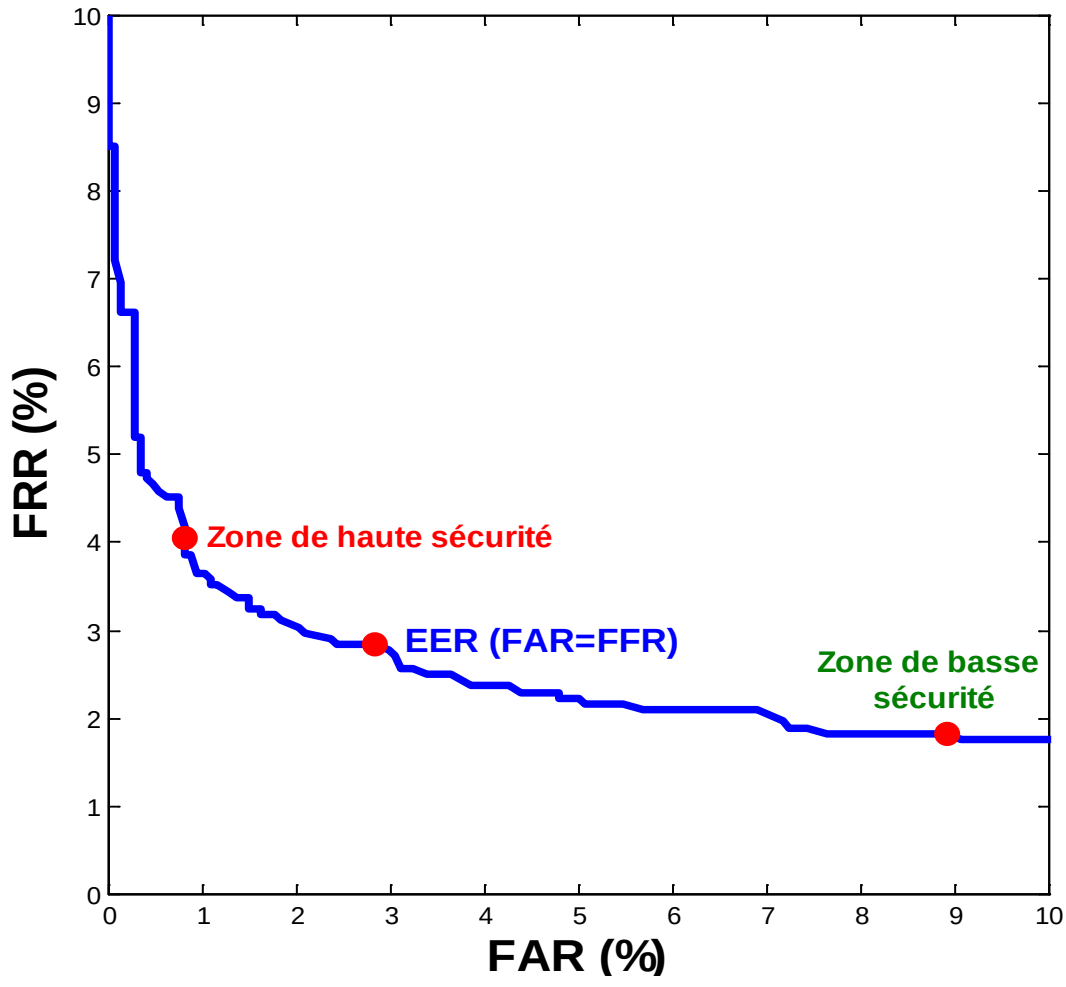


Figure IV.6: Les zones de sécurité dans la courbe DET

IV.5. Conclusion

Dans le présent chapitre, nous avons expliqué notre méthode adoptée de fusion en scores de l'empreinte digitale et la signature manuscrite en ligne. Nous avons opté pour une approche à la fois simple, efficace et qui ne nécessite pas beaucoup de calcul. Nous avons aussi présenté les caractéristiques des bases de données utilisées pour valider et concrétiser la démarche adoptée. Nous avons choisi des bases connues par la communauté scientifique afin de donner plus d'ampleur à notre travail. Enfin, on a illustré les mécanismes d'évaluation et de décision. On a opté pour une décision bayésienne alors qu'on a calculé trois types d'erreurs (FFR, FAR, EER).

Dans le chapitre suivant, nous allons présenter les performances de notre système biométrique multimodal.

Chapitre V

Résultats expérimentaux

V.1 Introduction

La multimodalité est une alternative qui permet d'améliorer de manière systématique la performance d'un système biométrique. Par performance, nous entendons à la fois la précision du système, mais aussi son efficacité, plus particulièrement. En effet, les systèmes biométriques unimodaux font en général des erreurs différentes, alors il est possible de tirer parti de cette complémentarité offerte par la multimodalité afin d'améliorer la performance du système.

Malgré les avantages des systèmes biométriques par rapport aux systèmes traditionnels, ils sont vulnérables à des attaques spécifiques qui peuvent dégrader considérablement leurs fonctionnalités et l'intérêt d'employer de tels systèmes. Ainsi, l'évaluation de la sécurité des systèmes biométriques est devenue indispensable pour garantir l'opérationnalité de ces systèmes.

Le présent chapitre est consacré à la présentation des tests effectués et les résultats obtenus. Nous étudions les performances des deux systèmes (empreintes et signatures) de façon séparée avant de présenter les résultats de nos combinaisons de fusion. En outre, notre système sera comparé par rapport aux travaux de ceux qui ont travaillé sur les mêmes bases de données utilisées.

Une étude de l'apport de la normalisation des scores selon les différentes méthodes introduites dans le chapitre II, ainsi que l'influence du prétraitement sur les performances du système est réalisée. Les performances du système sont évaluées en termes de taux d'égale erreur (*Equal Error Rate ou EER*) qui indique le point où les taux des fausses acceptations et des faux rejets sont égaux. L'implémentation des différents algorithmes de notre système ainsi que le déroulement de tous les tests sont faits sous **Matlab**.

V.2 Fusion intermodalité des signatures manuscrites en ligne

V.2.1. Impacte du filtrage sur les performances du système d'authentification des signatures manuscrites en ligne

L'utilisation des filtres pour représenter la signature manuscrite en ligne avec seulement un certain nombre de points influence de façon considérable sur les performances du système. Le but ici est de réduire au maximum le nombre de points d'une signature tout en gardant les taux d'erreurs au plus bas possible. En d'autres termes, nous devons trouver un compromis entre ces deux facteurs pour préserver la forme générale des signatures tout en gardant les performances du système au plus haut niveau possible. Dans notre cas, cette étude est menée afin de choisir un seuil approprié à notre filtre de distance et montrer son influence sur les performances du système. Des expériences ont été effectuées selon le procédé suivant : dans un premier temps, nous étudions l'effet du seuil "d" de notre filtre en distance sur la variation de l'EER. Pour cela, nous avons évalué notre système en prenant différentes valeurs de ce seuil sur l'ensemble des signatures de la base SVC 2004. Les résultats sont représentés sur la **Figure V.1** sous forme de courbes DET:

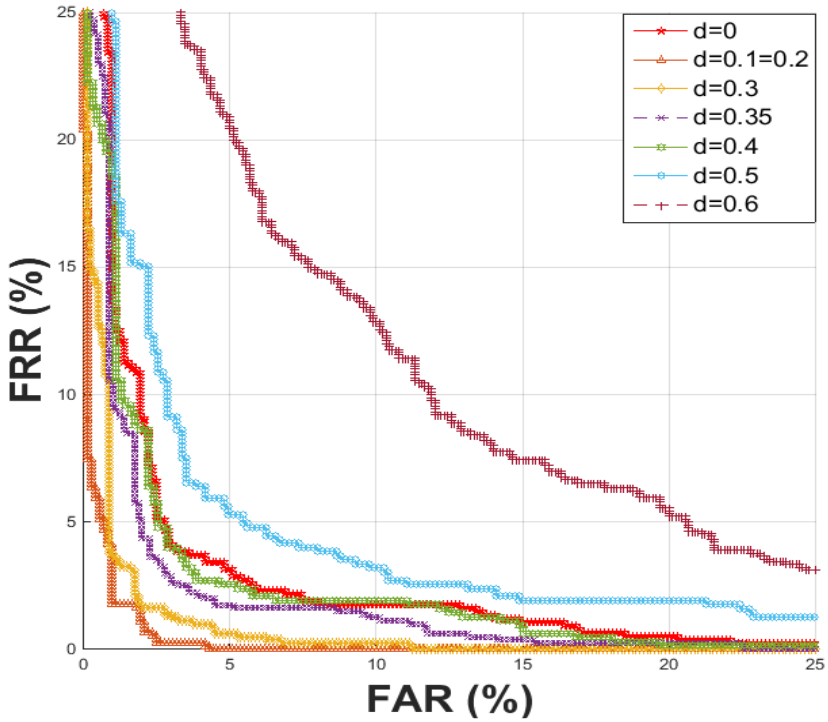


Figure V.1. Évaluation de notre système d'authentification de signatures manuscrites en ligne avec différentes valeurs du seuil " d ".

Ensuite, nous avons déterminé le nombre moyen d'échantillons et on a défini deux types de rapport : le premier est « **le rapport de réduction d'échantillons (SR)** » et le second est défini comme le rapport entre l'EER et le SR. Les résultats sont résumés dans le tableau suivant :

La valeur du seuil d	EER (%)	Le nombre moyen d'échantillons (nombre arrondi)	Le rapport de réduction d'échantillons (le nombre d'échantillons avant le filtrage / le nombre d'échantillons après le filtrage)	Le rapport M=(EER/SR)
0	3.72%	292	1	3.72
0.1	1.79%	262	1.114	1.60
0.2	1.79%	241	1.211	1.47
0.3	1.83%	176	1.659	1.110
0.35	2.88%	147	1.986	1.45
0.4	3.52%	125	2.336	1.506
0.5	5.28%	112	2.607	2.025
0.6	11.33%	93	3.139	3.609

Tableau V.1: Effets de la valeur du seuil "d" sur les performances du système.

Les résultats du tableau montrent que la meilleure valeur seuil est d=0.3. En fait, c'est pour cette valeur qu'on obtient la meilleure valeur du rapport " M ". Par conséquent le compromis est satisfait.

V.2.2. Evaluation de la fusion inter-modalité des signatures manuscrites en ligne

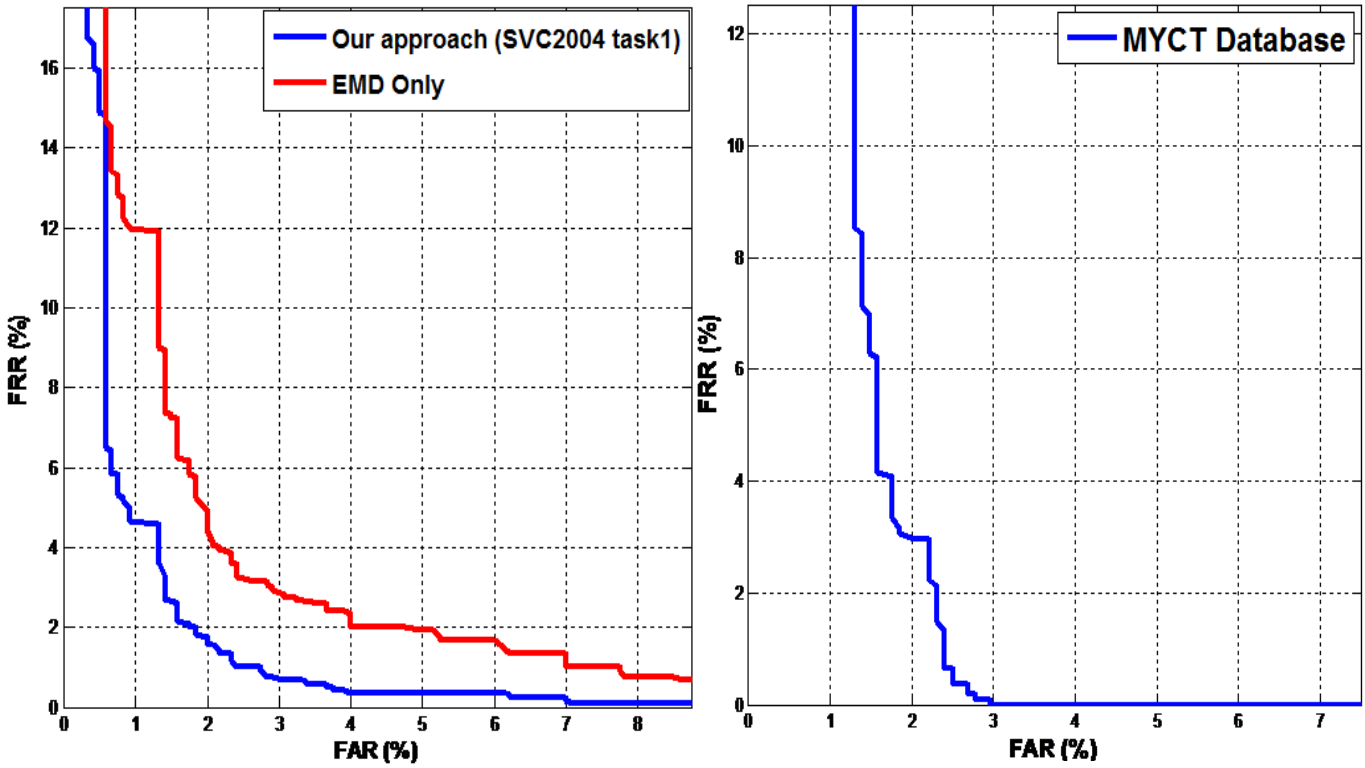
Ce type de fusion est très utilisé dans les systèmes d'authentification de signatures manuscrites en ligne. **N**ous avons effectué ce type de fusion pour deux raisons essentielles.

La première est de considérer l'effet et les performances d'une fusion à partir de deux caractéristiques qui proviennent de la même modalité. La deuxième est de voir l'impact de la décomposition modale empirique sur la signature manuscrite en ligne. Cette méthode originale, que nous l'avons appliquée pour la première fois **[208]** à porter ces fruits pour cette modalité.

Dans ce cas, nous avons utilisé la méthode du Min-Max pour normaliser les scores X et les scores Y et nous avons attribué des poids égaux lors de l'application de la somme pondérée comme méthode de fusion.

Notre système est évalué en termes de taux d'erreur égal (EER). Le système proposé a été testé sur deux bases de données en occurrence la base SVC 2004 et la base MCYT-100 où un EER de 1.83% et de 2.23% est obtenu pour chaque base de données respectivement.

La **Figure V.2** montre les courbes DET (*detection error tradeoff*) pour chaque ensemble de données.



(a) **(b)**

Figure V.2. Les courbes DET (*detection error tradeoff*) de notre système proposé d'authentification de signatures manuscrites en ligne (a) Pour la base SVC 2004 (b) Pour la base MCYT-100.

Comme on peut constater sur la **Figure V.2**, nous avons également évalué notre système en employant l'approche d'EMD sans extraction d'extrema sur la base SVC2004 « task1 » comme décrite dans (**section III.4.4.2**) dans le but de présenter les avantages de la méthode adoptée. En effet, notre approche diminue le temps de calcul et permet aussi de gagner en espace mémoire. En outre, elle a réduit au maximum les taux d'erreur en comparaison avec ceux obtenus par l'EMD sans extraction d'extrema. Ce fait indique bien la validité de notre choix.

Nous avons comparé nos résultats à ceux obtenus par d'autres travaux qui avaient utilisé les mêmes bases de données.

Le **Tableau V.2** et le **Tableau V.3** récapitulent leurs performances en termes de taux d'erreur égal (EER). Les résultats obtenus montrent l'efficacité de l'approche adoptée en comparaison à d'autres qui ont utilisé les mêmes bases de données.

Méthodes	EER (%)
DTW **[209]**	6.69
HMM **[210]**	6.90
SVM **[211]**	6.84
Mellin transform + MFCC **[184]**	3
EMD sans extraction extrema	2.92
EMD avec extraction d'extrema (notre approche)	**1.83**

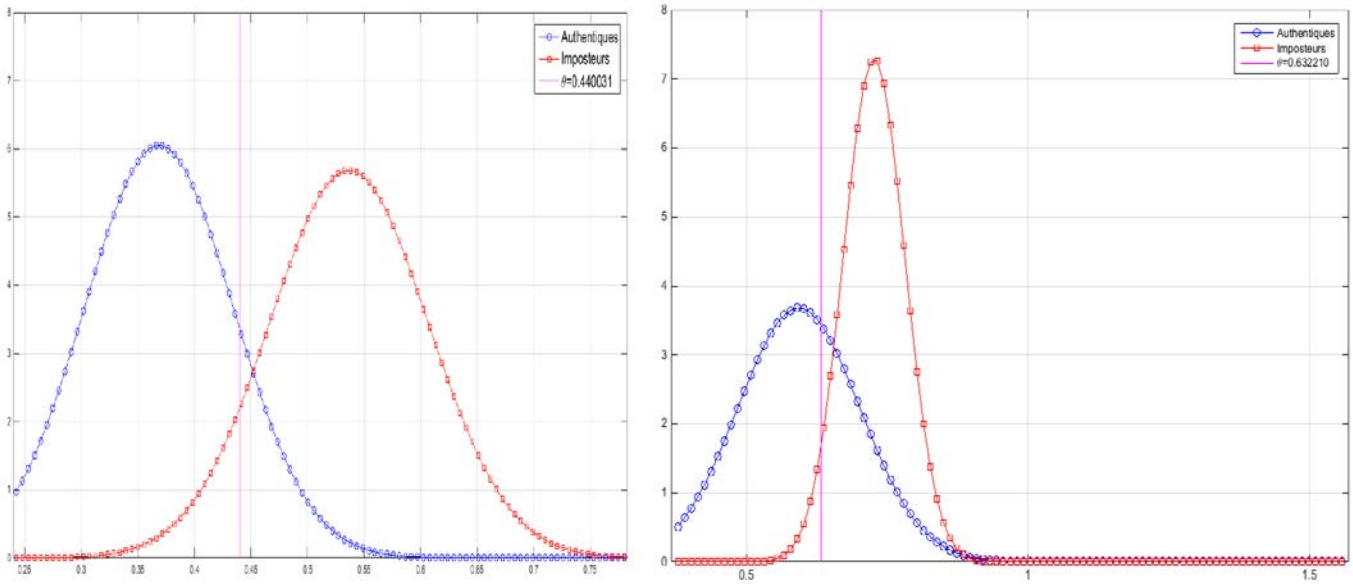
Tableau V.2: Comparaison de nos performances en termes d'EER sur la base SVC2004 "tâche 1" base de données.

Méthodes	EER (%)
[212]	5
[213]	4
[214]	3.5
[215]	3.37
Notre méthode	**2.23**

Tableau V.3: Comparaison de nos performances en termes d'EER sur la base MCYT-100.

V.3 Évaluation de notre système unimodal d'authentification d'empreinte digitale

Comme nous avons énoncé au paravent, nous avons utilisé la base FVC 2004 ainsi que la base MCYT-100 pour tester les performances de notre système d'authentification d'empreintes digitales. Les expériences montrent que notre système peut différencier entre les paires de minuties authentiques et ceux des imposteurs à un certain niveau de confiance. Les systèmes unimodaux ont des performances acceptables si on les utilise pour des applications à un niveau de sécurité bas, mais dans le cas où la sécurité est primordiale, ces systèmes sont présentent des limitations. En outre, leurs performances peuvent certainement s'améliorer en faisant appel à la multimodalité. La figure suivante illustre la distribution des scores authentiques et imposteurs de notre système d'authentification d'empreintes digitales en utilisant les deux bases de données citées au-dessus. La normalisation des scores a été effectuée avec la méthode du Min-Max.



(a) **(b)**

Figure V.3. La distribution des scores authentiques et imposteurs de notre système proposé d'authentification d'empreintes digitales (a) Pour la base FVC 2004 (b) Pour la base MCYT-100.

On peut constater sur la figure ci-dessus qu'il existe deux distributions qui se chevauchent partiellement : la courbe bleue dont les scores sont principalement situés dans la partie gauche et la courbe rouge dont les scores sont principalement situés sur le côté droit de la courbe. Cela indique que notre algorithme est capable de différencier entre les empreintes

digitales en fixant une bonne valeur de seuil de décision. La **Figure V.4** montre les courbes DET (*detection error tradeoff*) pour chaque base de données où on a obtenu un EER de 2.50% et 2.91 % pour la base FVC2004 et MCYT-100 respectivement .

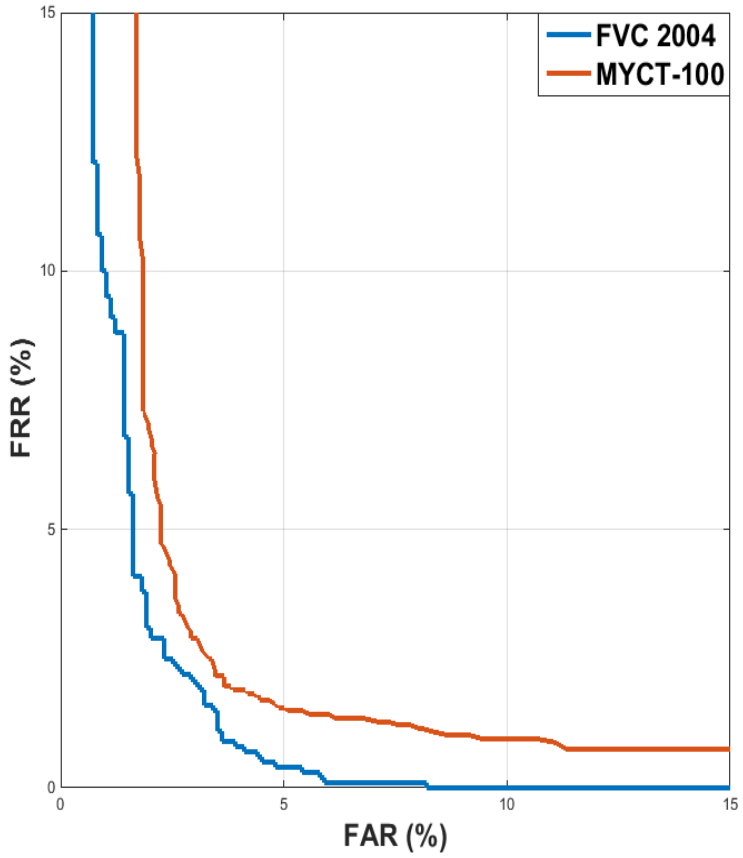


Figure V.4. Les courbes DET (*detection error tradeoff*) de notre système proposé d'authentification d'empreinte digitale pour les bases FVC 2004 et MCYT-100.

V.4. Evaluation de notre système multimodal d'authentification de signatures manuscrites en ligne et d'empreinte digitale

Les systèmes d'authentification multimodale, qui fusionnent les informations de plusieurs sources biométriques au niveau des scores, ont gagné plus d'espace dans le domaine de la sécurité et plus précisément dans le domaine de la reconnaissance et de vérification de l'identité des personnes, ce, en raison de leur capacité à surmonter les limites de la biométrie unimodale comme la non-universalité des traits biométriques, le bruit au niveau des capteurs biométriques et la grande variation intra-utilisateur ... etc.

Nous avons conçu un système à base de deux modalités de nature différente l'une comportementale et l'autre morphologique afin de distinguer l'impact de ce choix sur les

performances du système en premier lieu. Plusieurs combinaisons de fusion ont été essayées par notre système dans le but de définir la meilleure combinaison possible en termes de performances bien évidemment.

Les deux premières expériences de fusion consistent à combiner le score issu du système d'authentification d'empreinte digitale avec chacun des scores du système d'authentification de signature manuscrite en ligne (Score de x(t) et score de y(t)) respectivement. Nous avons testé notre système à l'aide de trois méthodes de normalisation (Min-Max, Z-score, TanH) et nous avons appliqué la somme pondérée comme méthode de fusion (**cf.chapitre IV**). Les deux figures suivantes démontrent les résultats obtenus après la fusion du score empreinte avec celui de x(t) et de y(t) respectivement à travers le graphe DET. Les tests ont été menés sur la base bimodale MCYT-100 avec trois méthodes de normalisation (Min-Max, Z-score, TanH) et sans normalisation :

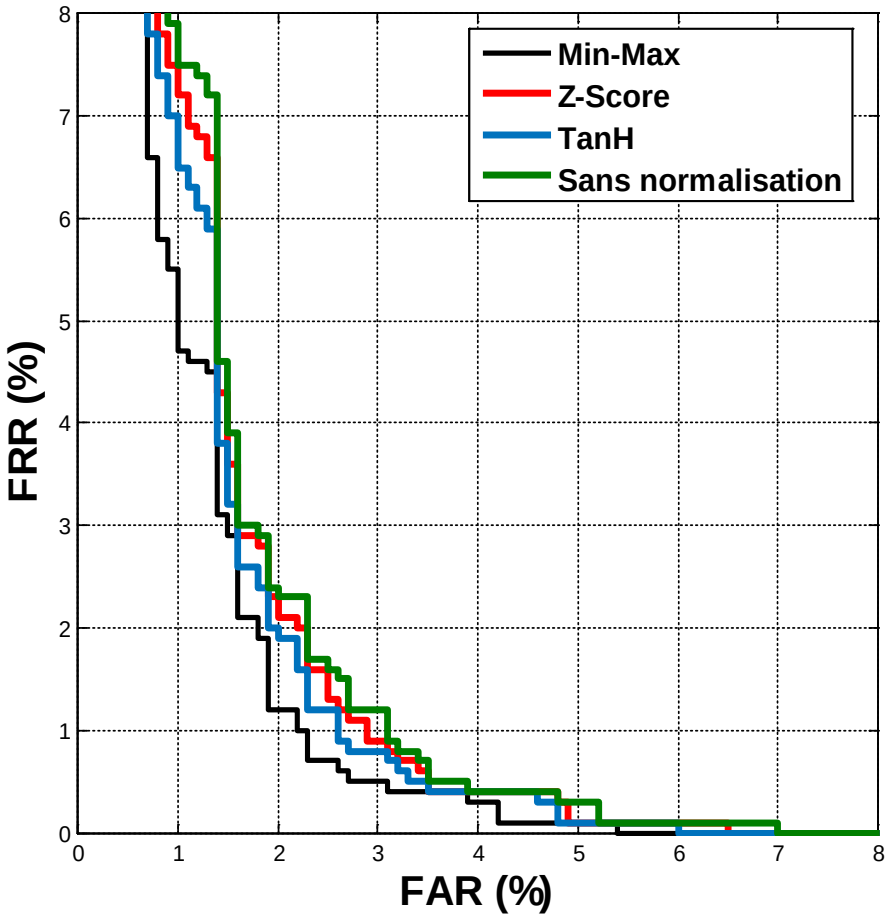


Figure V.5. Les courbes DET (*detection error tradeoff*) de la fusion entre le score empreinte et le score de x(t) de la signature manuscrite en ligne pour les bases MCYT-100.

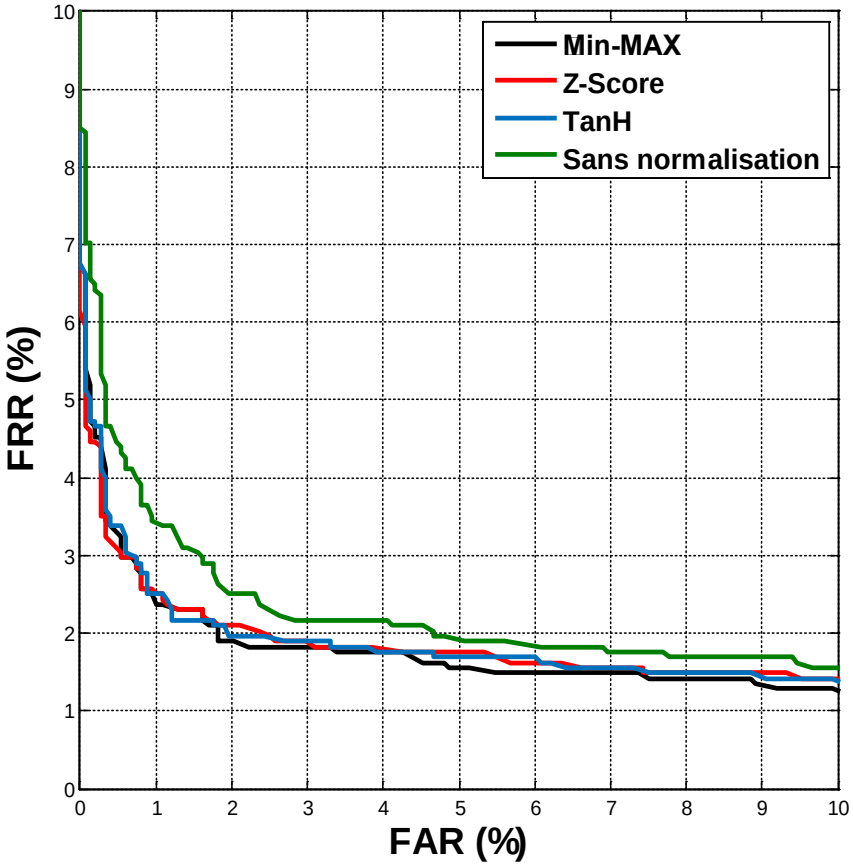


Figure V.6. Les courbes DET (*detection error tradeoff*) de la fusion entre le score empreinte et le score de y(t) de la signature manuscrite en ligne pour les bases MCYT-100.

Le tableau suivant récapitule nos résultats obtenus après avoir effectué les deux combinaisons de fusion citée au-dessus et avec plusieurs types de normalisation en matière d'EER :

Méthode de normalisation / Méthode de fusion	EER %			
	MIN-MAX	**Z-SCORE**	**TANH**	**Sans normalisation**
Score Empreinte et Score x(t)	**1.90**	**2.10**	**2.00**	**2.30**
Score Empreinte et Score y(t)	**1.89**	**2.09**	**1.96**	**2.36**

Tableau V.4: Résultats obtenus après les deux opérations de fusion en termes d'EER sur la base MCYT-100.

La décision d'accepter ou de rejeter un utilisateur est basée sur le score d'authentification. Cette décision peut être améliorée en normalisant les scores. Cela est confirmé par nos résultats parce que l'impact de la normalisation sur nos performances est

primordial. Comme on peut le constaté dans le **Tableau V.4**, les taux d'erreurs sont top proche entre eux avec une marche d'avance pour la méthode du Min-Max qui confirme sa réputation pour les scores biométriques due à sa simplicité et sa robustesse. Les taux d'erreurs obtenus sont très encourageants par rapport à ceux obtenus avec les systèmes unimodaux.

La dernière combinaison de fusion de notre système consiste à combiner le score issu du système d'authentification d'empreinte avec celui issu du système d'authentification de signature manuscrite en ligne. En fait, dans ce cas, nous allons fusionner la globalité de nos deux modalités biométriques contrairement au cas précédent où nous avons pris qu'une partie de notre modalité comportementale en occurrence la signature manuscrite en ligne. Comme pour les deux précédentes opérations de fusion, nos tests ont été menés sur la base bimodale MCYT-100 avec trois méthodes de normalisation (Min-Max, Z-score, TanH) et sans normalisation. La comparaison entre les résultats obtenus sans normalisation, avec les trois méthodes de normalisation de notre système est illustrée sous forme de courbe DET dans la **Figure V.7**.

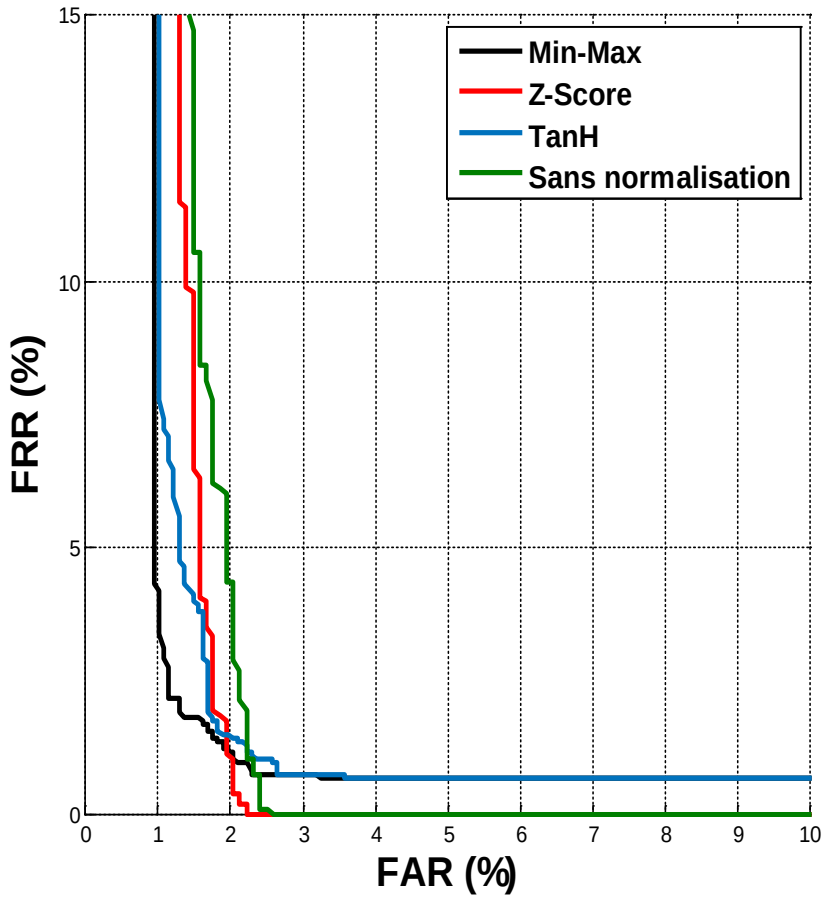


Figure V.7. Les courbes DET la fusion entre l'empreinte digitale et la signature manuscrite en ligne les bases MCYT-100.

Le tableau suivant résume nos résultats obtenus après avoir fusionné la globalité de nos deux modalités biométriques (l'empreinte et la signature) avec plusieurs types de normalisation en termes d'EER :

Méthode de normalisation / Méthode de fusion	EER %			
	MIN-MAX	**Z-SCORE**	**TANH**	**Sans normalisation**
Empreinte et signature	**1.69**	**1.85**	**1.76**	**2.16**

Tableau V.5: Résultats obtenus après la fusion entre l'empreinte et la signature en termes d'EER sur la base MCYT-100.

D'après le **Tableau V.5** et la **Figure V.6**, nous remarquons que la normalisation avec la méthode du Min-Max améliore la décision dans tous les cas de figure. De plus, on a obtenu un taux d'EER de 1.69 % ce qui constitue un réel succès pour notre système. Ce succès est réalisé à l'aide de la contribution de plusieurs facteurs : en premier lieu l'efficacité des deux algorithmes d'extraction des caractéristiques (l'approche structurelle pour les empreintes digitales et la décomposition modale empirique EMD pour la signature manuscrite en ligne) ainsi que le choix de la méthode de normalisation et de fusion adoptée par notre système. Le tableau suivant résume tous nos meilleurs résultats obtenus sur la base MCYT-100. L'amélioration est très perceptible. En effet, nous avons pu apporter une amélioration significative des taux d'erreur qui ont chuté de 2.91 % à 1.69 %.

Systèmes	**EER(%)**
Systèmes d'authentification de signature manuscrite en ligne	**2.23**
Systèmes d'authentification d'empreinte digitale	**2.91**
Fusion entre l'empreinte et x(t) de la signature	**1.90**
Fusion entre l'empreinte et y(t) de la signature	**1.89**
Fusion entre l'empreinte et la signature	**1.69**

Tableau V.6: Résumé des résultats obtenus en termes d'EER sur la base de données MCYT-100.

V.5.Conclusion

Dans ce chapitre, nous avons présenté les tests effectués et les résultats obtenus par notre système d'authentification biométrique multimodale basés sur la fusion en score d'empreinte digitale et signature manuscrite en ligne. Nous avons commencé par présenter les performances de nos deux modalités séparément avant d'effectuer plusieurs combinaisons de fusion entre nos deux modalités considérées. Nous avons aussi réalisé une étude de la normalisation des scores et son impact sur les performances de notre système. Notre système de fusion montre de bonnes performances. Le meilleur résultat est obtenu en fusionnant la globalité de nos deux modalités biométriques où on a obtenu un EER de 1.69 % en normalisant les scores selon la méthode du Min-Max. Ainsi, notre système de fusion est beaucoup plus performant en comparaison aux systèmes unimodaux illustrés dans notre travail.

Conclusion générale

Cette étude nous a permis de valider la faisabilité d'un système biométrique multimodal par la fusion de deux modalités biométriques : l'empreinte digitale, et la signature manuscrite cursive en ligne.

En suivant un protocole de test d'évaluation basé sur des méthodes de normalisation et de fusion en scores (somme pondérée des deux modalités biométriques), nous avons démontré que la démarche adoptée a fourni d'excellents résultats en termes de taux d'égale erreur(EER), et qu'elle est capable de gérer des situations délicates, en particulier lorsque les systèmes unimodaux ne permettent pas d'effectuer une bonne reconnaissance justifiant ainsi la nécessité de fusionner plusieurs modalités biométriques.

En perspective, il est souhaitable sinon indispensable de réaliser ce système bimodal sur des composants électroniques de type FPGA pour respecter les contraintes d'encombrement et de traitement en temps réel, et d'ajouter un module destiné à la sécurisation des données biométriques.

Bibliographie

[1] A. K. Jain, A. Ross, Introduction to Biometrics, in: handbook of biometrics, Springer, 2008.

[2] Jain A., Pankanti, S., Prabhakar S., Hong L., Ross, A., “Biometrics: a grand challenge”, Proceedings of International Conference on Pattern Recognition, Cambridge, United Kingdom, vol. 2, pp. 935–942, 2004.

[3] Dorizzi B., Le roux les jardins J., Lamadelaine P., Guerrier C., La Biométrie: Techniques et usages, Techniques de l’ingénieur, vol. SI1, no. H5530, pp. 1–26, 2004.

[4] Dorizzi B., Les taux d’erreurs dans le recours aux identifiants biométriques, dans l’Identification biométrique, CEHAN A., PIAZZA P., Editions de la maison des sciences de l’Homme, 2011.

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

[6] Kai Cao; Jain, A.K., "Learning Fingerprint Reconstruction: From Minutiae to Image," in Information Forensics and Security, IEEE Transactions on, vol.10, no.1, pp.104-117, Jan. 2015.

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

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

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

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

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

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

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

[14] Ee Ping Ong; Yanwu Xu; Wong, D.W.K.; Jiang Liu, "Retina verification using a combined points and edges approach," in Image Processing (ICIP), 2015 IEEE International Conference on , pp.2720-2724, 27-30 Sept. 2015.

[15] Kunxia Wang; Ning An; Bing Nan Li; Yanyong Zhang; Lian Li, "Speech Emotion Recognition Using Fourier Parameters," in Affective Computing, IEEE Transactions on , vol.6, no.1, pp.69-75, 2015

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

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

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

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

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

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

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

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

[24] Nait-ali A., “Beyond classical biometrics: when using hidden biometrics to identify individuals”, 3rd European Workshop on Visual Information Processing, Invited paper, Paris, pp. 241–256, 4–6 July, 2011.

[25] Nait-ali A., “Hidden biometrics: towards using biosignals and biomedical images for security applications”, 7th international Workshop on Systems, Signal Processing and their Applications, Invited paper, Tipaza, pp. 352–356, 2011.

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

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

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

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

[30] Wang Y., Plataniotis K., Hatzinakos D., “Integrating analytic and appearance attributes for human identification from ECG signal”, Proceedings of Biometrics Symposiums (BSYM ’06), Baltimore, MD, USA, September 2006.

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

[32] Nait-ali A., Fournier R., “Signal and Image Processing for Biometrics”, John Wiley & Sons, ISBN 978-1-84821-385-2, 2012.

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

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

[35] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez, et al, The Multi-Scenario Multi-Environment BioSecure Multimodal Database (BMDB), IEEE Transactions on Analysis, vol. 32, no. 6, pp. 1097-1111 , June 2010.

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

[37] James P. Egan., Signal detection theory and ROC-analysis. by Academic Press, New York, 1975.

[38] A. Martin, G. Doddington, T. Kamm, M. Ordowski, and M. Przybocki, The DET curve in assessment of detection task performance. In the 5th European Conference on Speech Communication and Technology, 1997.

[39] J. Bhatnagar and A. Kumar. On estimating performance indices for biometric identification. Pattern Recognition, Vol. 42, pp.1803-1815, 2009.

[40] D. Faraggi and B. Reiser, Estimation of the area under the ROC curve. Statistics in medicine, Vol.21, pp.3093–3106, 2002.

[41] E. Lefevre, Fusion adaptée d'informations conflictuelles dans le cadre de la théorie de l'évidence, application au diagnostic médical. Thèse, INSA de Rouen. 2001.

[42] C. Rouchouze, Fusion de données : exemples Défense et axes de recherche, Traitement du signal. Vol. 11(6), pp. 459-464. 1994.

[43] E. S. Bigün, Josef Bigün, Benoît Duc, and S. Fischer. Expert conciliation for multi modal person authentication systems by bayesian statistics. In AVBPA 97 : Proceedings of the First International Conference on Audioand Video-Based Biometric Person Authentication, pp: 291-300, London, UK, 1997. Springer-Verlag.

[44] Karthik Nandakumar. Multibiometric Systems: Fusion Strategies and Template Security. PhD thesis, Michigan State University, 2008

[45] Faundez-Zanuy, M., "Data fusion in biometrics," in Aerospace and Electronic Systems Magazine, IEEE , vol.20, no.1, pp.34-38, Jan. 2005.

[46] K. Nandakumar. Integration of Multiple Cues in Biometric Systems. Master's thesis, Michigan State University, May 2005.

[47] Dijana Petrovska-Delacrétaz, Gérard Chollet, Bernadette Dorizzi « *Guide to Biometric Reference Systems and Performance Evaluation* »; Springer ISBN: 978-1-84800-291-3; 2009.

[48] L. Gader B. Forester, M. Ganzberger, A. Gillies, B. Mictchell, M. Whalen and T. Yocum, Recognition of handwritten digits using template and model matching. Pattern Recognition, Vol. 24(5), pp. 421-431, 1991.

[49] L. Prevost, C. Michel-Sendis, A. Moises, L. Oudot, M. Milgram. Combining model-based and discriminative classifiers : application to handwritten character recognition. In 7th International Conference on Document Analysis and Recognition, Vol. 1, pp. 31-35, 2003.

[50] A. Rahman and M. Fairhurst, Multiple classifieur design combination strategies for character recognition: a review. Journal Document Analysis and Recognition JDAR, pp. 166-194. 2003.

[51] R. Sabourin, G. Genest and F. Preteux , Offline signature verification by local granulometric size distributions. IEEE Trans. PAMI 19(8), pp. 976-988, 1997.

[52] Y.S. Huang and C.Y. Suen, A method of combining multiple experts for the recognition of unconstranined handwritten numerals. IEEE Trans. PAMI, Vol.17(1), pp. 90-94, 1995.

[53] P. Gader, M. Mohamed and J. Keller, Fusion of handwritten word classifiers.Pattern Recognition Letters, Vol. 17, pp. 577-584, 1996.

[54] J. Kim, K. Kim, C. Nadal and C. Suen, A methodology of combining HMM and MLP classifiers for cursive word recognition. International Conference on Document Analysis and Recognition (ICDAR), Vol. 2, pp. 319-322, 2000.

[55] H.K. Zouari, Contribution à l'évaluation des méthodes de combinaison parallèle de classifieurs par simulation. Thèse, Université de Rouen, 2004

[56] B. Gosselin, Cooperation of multilayer perceptron classifiers. 8th Workshop on Circuits, Systems and Signal Processing, pp. 187-190, Mierlo, Pays-Bas, 1997.

[57] A. Bellili, M. Gilloux and P. Gallinari, Reconnaissance de chiffres manuscrits par un système hybride MLP-SVM. In 13eme Congrés Francophone AFRIF- AFIA de Reconnaissance des formes et d'Intelligence Artificielle (RFIA'02), Vol. 3, pp. 761-769, Angers, France, 2002.

[58] M.G. Oxenham, D.J. Kewley, M. J. Nelson, "Measure" of information for multi-level data fusion , SPIE, Vol. 2755, pp.271-282, 1996.

[59] V.B.Dasarathy,«Sensor fusion potential exploitation-innovative architecture and illustrative applications »,*Proc.ofIEEE*,Vol.85,pp.24-39,1997.

[60] K. Sasidhar, V. L. Kakulapati, K. Ramakrishna, and K. K. Rao, "Multimodal biometric systems—study to improve accuracy and performance," International Journal of Computer Science and Engineering Survey, vol. 1, no. 2, pp. 54–60, 2010.

[61] R. Giot and C. Rosenberger, "Genetic programming for multibiometrics," Expert Systems with Applications, vol. 39, no. 2, pp.1837–1847, 2012.

[62] Y.F. Yao, X.Y. Jing, and H.S. Wong, "Face and palmprint feature level fusion for single sample biometrics recognition", Neurocomputing 70, 1582–1588 (2007).

[63] R. N. Kankrale and S. D. Sapkal, "Template level concatenation of iris and fingerprint in multimodal biometric identification systems," International Journal of Electronics, Communication & Soft Computing Science & Engineering, pp. 29–36, 2012.

[64] P. Verlinde, P. Druyts, G. Cholet, and M. Acheroy, "Applying Bayes based classifiers for decision fusion in a multi-modal identity verification system," In : Proceedings of International Symposium on Pattern Recognition, February 1999.

[65] J. Fierrez-Aguilar, J. Ortega-Garcia, and J. Gonzalez-Rodriguez, "Fusion strategies in multimodal biometric verification," in Proceedings of the IEEE Intetrnational Conference on Multimedia and Expo (ICME '03), pp. 5–8, 2003.

[66] A. Ross. Multibiometrics. In Stan Z. Li and Anil K. Jain, editors,Encyclopedia of Biometrics, pages 967–973. Springer US, 2009.

[67] Dijana Petrovska-Delacrétaz, Gérard Chollet, Bernadette Dorizzi « Guide to Biometric Reference Systems and Performance Evaluation »; Springer ISBN: 978-1-84800-291-3; 2009.

[68] Anthony Lum,"Fingerprint Recognition"Pattern Recognition. Vol. 05, N° 2, pp. 72–85, June1999.

[69] L.A. Zadeh. Fuzzy sets, Information Control, Vol. 8, pp: 338–353,1965.

[70] Bengherabi M., Mezai L., Harizi F., Cheriet M., Guessoum A, «Face recognition based on 2DPCA, DIAPCA and DIA2DPCA in DCT domain », The 5th International Multi-Conference on Systems, Signals and Devices, IEEE SSD, Amman, Jordan, July 20-23, 2008.

[71] M. Sugeno, Fuzzy measures and fuzzy integrals A survey, in Fuzzy Automata and Decision Processes, M. M. Gupta, G. N. Saridis, and B. R. Gaines, Eds. Amsterdam, The Netherlands: North Holland,,pp: 89–102, 1977.

[72] T. Murofushi and M. Sugeno, An interpretation of fuzzy measures and the Choquet integral as an integral with respect to a fuzzy measure. Fuzzy Sets Syst. vol. 29, pp: 201–227, 1988.

[73] A. Shukla et al, Towards Hybrid and Adaptive Computing, SCI 307, Chapter 18 : Multimodal Biometric Systems,pp: 401–418, Springer-Verlag Berlin Heidelberg 2010.

[74] C. Cortes and V. Vapnick. Support-vector networks, Machine Learning, 20(3), pp 273–297, 1995.

[75] M Belahcene, A Ouamane, M Boumehrez et A Benakcha, «Authentification de visages par les transformations de Hough et Gabor associées à EFM et SVM pour la classification», Intelligence artificielle, Université MUNDIAPOLIS Casablanca, 2011.

[76] Pascual Ejarque, Javier Hernado, David Hernando, and David Gómez, Eigenfeatures and Supervectors in Feature and Score Fusion for SVM Face and Speaker Verification, BioID_MultiComm2009, LNCS 5707, pp:81-88, Springer-Verlag Berlin Heidelberg 2009.

[77] Dakshina Ranjan Kisku, Phalguni Gupta, and Jamuna Kanta Sing, Fusion of Multiple Matchers Using SVM for Offline Signature Identification. Springer-Verlag Berlin Heidelberg, pp. 201–208, 2009. 2009

[78] Mireia Farrús, Pascual Ejarque, Andrey Temko, and Javier Hernando. Histogram Equalization in SVM Multimodal Person Verification. Springer-Verlag Berlin Heidelberg, pp: 819–827, 2007.

[79] J. Hérault, B. Ans, and C. Jutten. Circuits neuronaux à synapses modifiables: Décodage de messages composites par apprentissage non supervisé. In Comptes Rendus de l'Académie des Sciences, pages 299(III–13) :525–528, 1984.

[80] P. Buyssens. Utilisation de réseaux de neurones convolutionels pour la reconnaissance faciale multimodale. Télécom & Management SudParis, Evry (ex INT), November 2008

[81] Christophe Moulin, Christine Largeron, Cecile Barat, Mathias Gery, Christophe Ducottet, Apprentissage par analyse linéaire discriminante des paramètres de fusion pour la recherche d'information multimédia texte-image. Livre : Extraction et gestion des connaissances (EGC'2012), Jan 2012, Bordeaux, France. HermannEditions, RNTI-E-23, pp.357-368, 2012.

[82] M.G. Oxenham, D.J. Kewley, M. J. Nelson, "Measure of information for multi-level data fusion" , SPIE, Vol. 2755, pp.271-282, 1996.

[83] D. Hall, J. L. Linas, "An introduction to multisensor data fusion", Proc. IEEE,Vol 85(1), pp.6-23, 1997.

[84] L. Wald, Data fusion, Definition and architectures, Fusion of images of different spatial resolutions. Presses de l'Ecole des Mines Paris, 2002.

[85] M. Oussalah. Fusion de données par la théorie des possibilités, application à la localisation d'un robot mobile. Thèse, Université d'Evry Val d'Essonne (EVE), 1998.

[86] L.Valet, G. Mauris and Ph. Bolon. A statistical overview of recent literature in information fusion. In Proceeding 3rd International Confrerence Fusion 2000, Paris, July 2000, pp. MOC3-22-29, IEEE catalog, 2000.

[87] C. Elachi, Introduction to the physics and techniques of remote sensing, in: J.A. Kong (Series Ed.), Wiley Series in Remote Sensing, 1987.

[88] S.B. Serpico and F. Roli, Classification of multisensor remote sensing images by structured neural networks. IEEE Trans. Geosci. Remote Sensing 33 (3), pp.562–578, 1995.

[89] C. Pohl, and J.L. Van Genderen, Multisensor image fusion in remote sensing:Concepts, methods and applications. International Journal of Remote Sensing Vol.19(5), pp. 823–854, 1998.

[90] L.Bruzzone, D.F.PrietoandS.B.Serpico,A neural statistical approach to multitemporal and multisensory and multisource remote sensing image classification.*IEEETrans.Geosci.RemoteSensing*Vol.37(3),pp.1350–1359,1999.

[91] F. Cremer, J.G.M. Schavemaker, E. den Breejen, K. Schutte, "Detection of anti-personal land-mines using sensor-fusion techniques," in : T. Windeatt, J. O'Brien (Eds.), Proceedings of EuroFusion 99. International Conf. on Data Fusion, Stratford Upon Avon, UK, pp. 159-166, 1999.

[92] F. Cremer, K. Schutte, J. G. M. Schavemaker and E. den Breejen, "A comparison of decision-level sensor-fusion methods for anti-personal landmine detection," Information Fusion,, vol. 2(3), pp.187-208, Sep 2001.

[93] X. Dai and S. Khorram, "Data fusion using artificial neural networks: a case study on multitemporal change analysis," Computers, Environment and Urban Systems, Vol. 23(1), pp.19-31, January 1999.

[94] T. Warren Liao, Damin Li, Two applications of the fuzzy k-ppv algorithm,Fuzzy sets and systems Vol. 92, 1997, pp. 289-303.

[95] S. Garcia-Salicetti, C. Beumier, G. Chollet, B. Dorizzi, J.L. les Jardins, J.Lunter, Y. Ni, D. Petrovska-Delacrétaz, BIOMET : A multimodal person authentication database including face, voice, fingerprint, hand and signature modalities, Lecture Notes in Computer Science, Publisher: Springer-Verlag GmbH, Vol. 2688 / 2003, pp. 845-853, 2003.

[96] K-A, Toh, W. Xiong, W-Y, Yau, X. Jiang, Combining fingerprint and Hand geometry verification decisions, Lecture Notes in Computer Science, Publisher: Springer-Verlag BmbH, Vol. 2688/2003, pp. 688-696, 2003.

[97] Guiyu Feng, Kaifeng Dong, Dewen Hu and David Zhang. When Faces Are Combined with Palmprints: A Novel Biometric Fusion Strategy. Lecture Notes in Computer Science, Volume 3072 / 2004, Proceedings of First International Conference on Biometric Authentication:, ICBA'2004, Hong Kong, China, pp. 701 – 707, July 15-17, 2004.

[98] A. Kumar, D.C.M. Wong, H.C. Shen, A.K. Jain. Personal Verification Using Palmprint and Hand Geometry Biometric. Lecture Notes in Computer Science Publisher: Springer-Verlag GmbH Vol. 2688 / 2003. Chapter: pp. 668-678,2003.

[99] M.G.K. Ong, T. Connie, A.T.B. Jin, A single-sensor hand geometry and palmprint verification system, Proc. of ACM SIGMM Workshop on Biometrics Methods and Applications, pp. 100-106, Berkley, California, USA, 2003.

[100] B.Achermann,H.Bunke,Combination of classifiers on the decision level for face recognition.Technical report,University of Bern,1996.

[101] R. Brunelli, D. Falavigna, Person identification using multiple cues, IEEE Trans. on PAMI, Vol. 17(10), pp. 955-966, 1995.

[102] E. Zois and V. Anastassopoulos, Fusion of correlated decisions for writer verification. Pattern Recognition, Vol. 32, pp. 1821-1823, 1999.

[103] M. Sabourin et G. Genest. Coopération de classifieurs pour la vérification automatique des signatures. In 3eme Colloque National sur l'Ecrit et le Document, pp. 89-98, Rouen, 1994.

[104]R. Bajaj and S. Chaudhury, Signature verification using multiple neural classifiers. Pattern Recognition, Vol. 30(1), pp. 1–7, 1997.

[105]C. Chibelushi, J. Mason and F. Deravi, Integration of acoustic and visual speech for speaker recognition, Eurospeech, pp. 157-160, 1993.

[106] K. Yu, X. Jiang, H. Bunke, Combining acoustic and visual classifiers for the recognition of spoken sentences, Int. Conf. in Pattern Recognition (ICPR), Vol. 2, pp. 491-498, Barcelona, 2000.

[107] K.Chen,L.Wang,H.Chi,Methodsofcombiningmultipleclassifierswith different features and their applications to text-independent speaker identification. Pattern Recognition and Artificialintelligence,Vol.11(3),pp.417-445,1997.

[108] S. Beiraghi, M. Ahmadi, M. Shridhar, M. Ahmed, Application of fuzzy integrals in fusion of classifiers for low error rate handwritten numerals recognition. In Int. Conf. in Pattern Recognition, 2000.

[109] J. Cao, M. Ahmadi, M. Shridhar, Fusion of classifiers with fuzzy integrals. Int.Conf. in Document Analysis and Recognition (ICDAR'95), 1995.

[110] L. Cordella, P. Foggia, C. Sansone, F. Tortorella, M. Vento, Optimizing the error/reject trade-off for a multi-expert system using the baysian combining rule. In Advances in Pattern Recognition, pp. 716-725, 1998.

[111] G. Dimauro, S. Impedovo, G. Pirlo, and S. Rizzo, Multiple experts; a new methodology for the evaluation of the combination processes. pp. 131-136,1995.

[112] R. Duin, D.M.J. Tax, Classifier conditional posterior probabilities. Advances in Pattern Recognition, Vol. 1451, pp. 611-619, 1998.,

[113] L. Heutte, Reconnaissance de caractère manuscrits : application à la lecture automatique des chèques et des enveloppes postales, Thèse, Université de Rouen, 1994.

[114] L. Xu, A. Krzyzak and C.Y. Suen, Methods of combining multiple classifiers and their applications to handwriting recognition. IEEE Transactions on Systems, Man and Cybernetics, Vol. 22(3), pp. 418–435, 1992.

[115] C. Nadal, R. Legault, and C.Y. Suen, "Complementary Algorithms for the Recognition of Totally Unconstrained Handwritten Numerals," in Proc. 10th Int. conf. Pattern Recognition., Vol. A, pp. 434-449, June 1990.

[116] T.K. Ho, J.J. Hull and S.N. Srihari, Decision combination in multiple classifier systems. IEEE Trans. PAMI, Vol. 16, pp. 66–75, 1994.

[117] P. Gader, M. Mohamed and J. Keller, Fusion of handwritten word classifiers.Pattern Recognition Letters, Vol. 17, pp. 577-584, 1996.

[118] Y. Li, A. Jain, Classification of text documents, The computer Journal, Vol. 41(8), pp. 537-546, 1998..

[119] R. Klette, P. Zamperoni, Handbook of Image Processing Operators, Ed. Wiley 1994.

[120]I .Bloch,"Some Aspects of Demspter-Shafer Evidence Theory for Classification of Multi-Modality Medical Images Taking Partial Volume EffectintoAccount, PatternRecognitionLetters,vol.17,905-919,1996.

[121] A. Dromigny-Badin. Fusion d'images par la théorie de l'évidence en vue d'applications médicales et industrielles. Thèse, INSA de Lyon, 1998.

[122] D. Dubois and H. Prade, "Combination of fuzzy information in the framework of possibility theory". Data Fusion in Robotics and Machine Intelligence, pp.481–505, 1991.

[123]M. Abidi and R. Gonzales, Editors, Data Fusion in Robotics and Machine Intelligence, Academic Press, New York, 1992.

[124] P.V. Palacharla, "A pattern recognition approach to data fusion in Intelligent Vehicle Highway Systems., Transportation Research Part A: Policy and Practice, Vol. 31(1), pp. 64-65, Jan 1997.

[125] L. Jetto, S. Longhi and D. Vitali. Localization of a wheeled mobile robot by sensor data fusion based on a fuzzy logic adapted Kalman filter, Control Engineering Practice, Vol. 7(6), pp. 763-771, 1999.

[126] K. Nandakumar, Y. Chen, S. C. Dass, A. Jain, Likelihood Ratio-Based Biometric Score Fusion, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 30, no. 2, pp. 342-347, February 2008.

[127] A. K. Jain, F. Jianjiang and N. Karthik, "Fingerprint Matching", IEEE Computer Society, **(2010),** pp. 36-44.

[128] T. Raymond, "Fingerprint Image Enhancement and Minutiae Extraction", PhD Thesis Submitted to School of Computer Science and Software Engineering, University of Western Australia, **(2003)**.

[129] G. B. Iwasokun, O. C. Akinyokun, B. K. Alese and O. Olabode, "Fingerprint Image Enhancement: Segmentation to Thinning", International Journal of Advanced Computer Science and Applications (IJACSA), Indian, vol. 3, no. 1, **(2012).**

[130] G. B. Iwasokun, O. C. Akinyokun, B. K. Alese and O. Olabode, "A Modified Approach to Crossing Number and Post-Processing Algorithms for Fingerprint Minutiae Extraction and Validation", IMS Manthan International Journal of Computer Science and Technology, Indian, vol. 6, Issue 1, (2011), pp. 1-9.

[131] L. Hong, Y. Wau and A. J. Anil, "Fingerprint image enhancement: Algorithm and performance evaluation", Pattern Recognition and Image Processing Laboratory, Department of Computer Science, Michigan State University, (2006), pp. 1-30.

[132] G. B. Iwasokun, O. C. Akinyokun, B. K. Alese and O. Olabode, "Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation", International Journal of Computer Science and Security, Malaysia, vol. 5, Issue 4, (2011), pp. 414- 424.

[133] L. Yount, "Forensic Science", From Fibres to Thumbprints' Chelsea House Publisher, (2007).

[134] K A. Nagaty,"An Energy-Based Fingerprint Matching System",Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE.

[135] C. Militello, V. Conti, F. Sorbello,S. Vitabile,"A Novel Embedded Fingerprints Authentication SystemBased on Singularity Points",International Conference on Complex, Intelligent and Software Intensive Systems,0-7695-3109-1/08 2008 IEEE.

[136] G. S. Ng, X. Tang, D. Shi "Adjacent Orientation Vector Based Fingerprint Minutiae Matching System", Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04) 1051-4651/04 , IEEE

[137] Wang Yuan,Yao Lixiu, Zhou Fuqiang,"A Real Time Fingerprint Recognition System Based OnNovel Fingerprint Matching Strategy",1-4244-1135-1/07/2007 IEEE.

[138] Bifari, E.N.; Elrefaei, L.A."Automated Fingerprint Identification System Based on Weighted Feature Points Matching Algorithm", 978-1-4799-3080-7114/2014,IEEE

[139] Fan Wang, Zhengyong Huang, Hui Yu, Xiaohua Tian, Xinbing Wang, Jinwei Huang"EESM-based Fingerprint Algorithm for Wi-FiIndoor Positioning System"2013 2nd IEEE/CIC International Conference on Communications in China (ICCC): Wireless Networking andApplications (WNA),978-1-4673-2815-9/13/2013 IEEE.

[140] Marcos Faundez-Zanuy & Joan Fabregas“Testing Report of a Fingerprint-Based Door-Opening System”,IEEE A&E SYSTEMS MAGAZINE. JUNE 2005.

[141]Pallav Guptat, Srivaths Ravi, Anand Raghunathan, Niraj K. Jhat “Efficient Fingerprint-based User Authentication for Embedded Systems”,DAC2005, June l3-17,2005, Anaheim, Califomia, USA. Copyright 2005 ACM 1-59593-05 8-2/05/0004 .

[142]Maitane Barrenechea,Jon Altuna ,Miguel San Miguel “A Low-Cost FPGA-based Embedded Fingerprint Verification and Matching System”,250 - 261, DOI: 10.1109/WISES.2007.4408496,2007.

[143] Pablo David Gutiérrez, Miguel Lastra, Francisco Herrera, and José Manuel Benítez“A High Performance Fingerprint Matching System for Large Databases Based on GPU”,IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014.

[144] Haiyun Xu, Raymond N. J. Veldhuis, Tom A. M. Kevenaar, and Ton A. H. M. Akkermans“A Fast Minutiae-Based Fingerprint Recognition System”,IEEE SYSTEMS JOURNAL, VOL. 3, NO. 4, DECEMBER 2009,1932-8184/2009 IEEE.

[145] Radu F. Miron, Tiberiu S. Letia and Mihai Hulea “Two Server Topologies for a Distributed Fingerprint-BasedRecognition System” System Theory, Control, and Computing (ICSTCC), 2011 15th International Conference,2011.

[146] D. Bennet,Dr. S. Arumugaperumal“Fingerprint Based Multi-Server Authentication System”978-1-4244-8679-3/11/2011 IEEE.

[147] Lei Zhang, Mei Xie “Realization of a New-style Fingerprint Recognition System Based on DSP”,Proceedings of 2008 IEEE International Symposium on IT in Medicine and Education,978-1-4244-2511-2/08/2008 IEEE.

[148] Maddu Kamarajui , Penta Ani! Kumar “DSP based Embedded Fingerprint RecognitionSystem”,2013 13th International Cmiference on Hybrid Intelligent Systems (HIS) ,978-1-4799-2439-4/13/$31.00 ©2013 IEEE.

[149] Yanpeng Wang, Qing Li, Li Zhang “Design of Embedded Fingerprint Identification System Based on DSP”Anti-Counterfeiting, Security and Identification (ASID), 2011 IEEE International Conference ,978-1-61284-632-3/11/2011 IEEE.

[150] P. Lorrentza , W. G. J. Howellsb,K.D. McDonald-Maierc“A Fingerprint Identification System using adaptive FPGA based Enhanced Probabilistic Convergent Network”,2009 NASA/ESA Conference on Adaptive Hardware and Systems,978-0-7695-3714-6/09, 2009 IEEE DOI 10.1109/AHS.2009.8.

[151] Wencheng Yang, Jiankun Hu, and Song Wang“A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Using Topology Code for Local Registration and Security Enhancement” IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 7, JULY 2014.

[152] F. Jianjiang, “Combining minutiae descriptors for fingerprint matching”, Elsevier Pattern Recognition, vol.41, (2008), pp. 342 – 352.

[153] T. Li, C. Liang and K. Sei-ichiro, “Fingerprint Matching Using Dual Hilbert Scans”, SITIS, **(2009),** pp. 553-559.

[154]T. Tang, "Fingerprint recognition using wavelet domain features," Natural Computation (ICNC), 2012 Eighth International Conference on, Chongqing, 2012, pp. 531-534.

[155] M. Brunato and R. Battiti, “Statistical learning theory for location fingerprinting in wireless LANs,” Computer Networks, vol. 47, no. 6, pp. 825–845, 2005.

[156] A. Carlotto,M. Parodi, C. Bonamico, F. Lavagetto, and M. Valla, “Proximity classification for mobile devices using wi-fi environment similarity,” in Proceedings of the 1st ACM International Workshop on Mobile Entity Localization and Tracking in GPSLess Environments (MELT ’08), pp. 43–48, San Francisco, Calif, USA, September 2008.

[157] D. Maio et D. Maltoni. Neural Network based minutiae filtering in fingerprints. IEEE, 1998.

[158] Hao G. A hidden Markov model fingerprint matching approach. In: Proceedings of the 4th International conference on machine learning and cybernetics, Guangzhou. 2005. p. 505-509

[159] Kavita Tewari , Renu L. Kalakoti , Fingerprint Recognition and feature extraction using transform domain techniques, International Conference on Advances in Communication and Computing Technologies (ICACACT), IEEE,PP. 1 - 5 , 2014

[160] A. Caliskan and O. F. Ertugrul, "Wavelet transform based fingerprint recognition," Signal Processing and Communications Applications Conference (SIU), 2015 23th, Malatya, 2015, pp. 1481-1484.

[161] B. Garg, A. Chaudhary, K. Mendiratta and V. Kumar, "Fingerprint recognition using Gabor Filter," Computing for Sustainable Global Development (INDIACom), 2014 International Conference on, New Delhi, 2014, pp. 953-958.

[162] D. Liang, J. Yang, R. Xuan, Z. Zhang, Z. Yang and K. Shi, "Principal Component Analysis and Clustering Based Indoor Localizaion," 2015 IEEE International Conference on Data Mining Workshop *(ICDMW)*, Atlantic City, NJ, 2015, pp. 1103-1108.

[163] B. Stojanovic, A. Neskovic and O. Marques, "Fingerprint ROI segmentation using fourier coefficients and neural networks," Telecommunications Forum Telfor (TELFOR), 2015 23rd, Belgrade, 2015, pp. 484-487.

[164] Cai Li and Jiankun Hu, "A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 3, pp. 543-555, March 2016.

[165] R. D. Labati, A. Genovese, V. Piuri and F. Scotti, "Toward Unconstrained Fingerprint Recognition: A Fully Touchless 3-D System Based on Two Views on the Move," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 46, no. 2, pp. 202-219, Feb. 2016.

[166] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman and A. K. Jain, "FVC2004: Third Fingerprint Verification Competition," Pattern Recognition, 2004. Proceedings. First International Conference, ICBA 2004, Hong Kong, China, July 15-17, 2004., pp 1-7.

[167] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J.-J. Igarza, C. Vivaracho, D. Escudero, and Q.-I. Moro, “Biometric on the Internet MCYT Baseline Corpus: a Bimodal Biometric Database,” IEE Proc. Visual Image Signal Processing, vol. 150, no. 6, pp. 395–401, December 2003.

[168] Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

[169] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.

[170] D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997.

[171] Sae-Bae, N.,Memon,N.:"Online Signature Verification on Mobile Devices", IEEE transactions on information forensics and security, 2014, 9, (6),pp.933 – 947.

[172] Meenakshikalera, k., Sargur,s., Aihua, x.:"offline signature verification and identification using distance statistics", International Journal of Pattern Recognition and Artificial Intelligence, 2004,18, (7), pp.1339–1360.

[173] Fuentes, M., Garcia-Salicetti, S., Dorizzi,B. : "On-line Signature Verification: Fusion of a Hidden Markov Model and a Neural Network via a Support Vector Machine", Proc. of International Workshop on Frontiers of Handwritten Recognition, Niagara on the Lake, Canada, August 2002, pp. 253-258.

[174] Ly, V. , Garcia-Salicetti, S. , Dorizzi, B. : "Fusion of HMM's Likelihood and Viterbi Path for On-line Signature Verification", ECCV Workshop BioAW, Springer, 2004,3087 ,pp. 318-331.

[175] Muramatsu,D.,Matsumoto,T.: “An HMM On-line Signature Verifier Incorporating Signature Trajectories”, Proceeding of the Seventh International Conference on Document Analysis and Recognition (ICDAR), IEEE, 2003.

[176] Fahmy ,Maged M.M.: “Online handwritten signature verification system based on DWT features extraction and neural network classification”, Ain Shams Engineering Journal, 1, 2010, pp.59–70.

[177] Yang,L. Widjaja B.K, Prasad,R.: "Application of Hidden Markov Models for Signature Verification", Pattern Recognition, 1995, 28, (2), pp.161-170.

[178] Fierrez-Aguilar, J., Nanni,L.,Lopez-Peñalba,J.,Ortega-Garcia,J.,Maltoni, D.:"An on-line signature verification system based on fusion of local and global information", Proc. of 5th IAPR Intl. Conf. on Audio and Video based Biometric Person Authentication, Springer-Verlag, Berlin, Heidelberg, 2005,pp.523-532.

[179] Hook,C.,Kempf ,J. ,Scharfenberg,G.: "A Novel Digitizing Pen for the Analysis of Pen Pressure and Inclination in Handwriting Biometrics", ECCV Workshop BioAW, Springer 2004, 3087,pp. 283-294.

[180] Lejtman, D.Z.,Gorge,S.E.: "On-line handwritten signature verification using wavelets and back-propagation neural networks", IEEE, 2001.

[181] Signature Verification Competition: http://www.cs.ust.hk/svc2004/download.html, 2004.

[182] Plamondon, R., Lorette, G.: "Automatic Signature Verification and Writer Identification: The state of the art", Pattern Recognition, 1989, 22, (2), pp. 107-131.

[183] Mingming,M.,Wijesoma, W. S.: "Automatic On-line Signature Verification Based on Multiple Models", Conference on Computational Intelligence for Financial Engineering (CIFEr), New York, USA, March 2000, pp. 30-33.

[184] Fallah, A.,Jamaati, M., Soleamani, A.:"A new online signature verification system based on combining Mellintransform, MFCC and neural network", Digital Signal Processing, 2011, 21, pp. 404–416.

[185] Malallah,F. L., Sharifah, M. S. A. , Wan Azizun, W. A., Arigbabu,O. A., Vahab, I., Salman ,Y.: "Online Handwritten Signature Recognition by Length Normalization using Up-Sampling and Down-Sampling", International Journal of Cyber-Security and Digital Forensics (IJCSDF) ,2015, 4,(1),pp 302-313.

[186] Hung, N. E., Shen, Z., Long, S. R., Wu, M. C., Shih, H. H., Zheng, Q., Yen, N. C., Tung, C. C., Liu,H. H.: "The empirical mode decomposition and Hilbert spectrum for nonlinear and nonstationary time series analysis ", Proc. Roy. Soc. London A, 1998, 454, pp. 903–995.

[187] Fahmy ,Maged M.M.: "Online handwritten signature verification system based on DWT features extraction and neural network classification", Ain Shams Engineering Journal, 1, 2010, pp.59–70.

[188]Huang,N. E.,Shen,Z.,Long,S. R.: "A new view of nonlinear water waves: the Hilbert spectrum" , Annual Review of Fluid Mechanics, 1999, 31, pp. 417-457.

[189] Chang, C.P., Lee, J.C., Su,Y., Huang,P. S., Tu, T.M. :"Using empirical mode decomposition for iris recognition ", Computer Standards & Interfaces, 2009,31, pp.729 –739

[190] Bhagavatula, R.,Savvides, M.: "Analyzing Facial Images using Empirical Mode Decomposition for Illumination Artifact Removal and Improved Face Recognition,"IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 15-20 April 2007, 1, pp.I-505-I-508.

[191] Krinidis, S.,Krinidis, M.,Chatzis,V.: "Workspace for image clustering based on empirical mode decomposition", IET Image Processing, 2012, 6, (6), pp. 778 – 785

[192] Riffi,J., Mohamed Mahraz, A., Tairi, H., "Medical image registration based on fast and adaptive bidimensional empirical mode decomposition", IET Image Processing,August 2013, 7, (6), pp.567-574.

[193] Niang,O., Thioune,A. , Gueirea,M.C.E. , Delechelle, E. , Lemoine,J.: "Partial Differential Equation-Based Approach for Empirical Mode Decomposition: Application on Image Analysis", IEEE Transactions on Image Processing, Sept. 2012, 21, (9), pp.3991-4001.

[194] Yang,Z.,Qi, D., Yang,L.:"Signal period analysis based on Hilbert-Huang transform and its application to texture analysis ", in Proc. Intl. Conf. Image and Graphic, Hong Kong, 2004.

[195] Roy,A.,Doherty,J.F.: "Raised cosine filter-based empirical mode decomposition", IET Signal Processing, 2011, 5, (2), pp. 121–129.

[196] urRehman, N., Mandic, D.P., "Filter Bank Property of Multivariate Empirical Mode Decomposition", IEEE Transactions on Signal Processing, May 2011, 59, 5, pp.2421-2426.

[197] Rui, Ma, Chen,Yushu, Sun, Huagang: "Detection of weak signals based on empirical mode decomposition and singular spectrum analysis",IET Signal Processing ,2013, 7, (4), pp. 269–276.

[198] Sweeney, K.T., Kearney, D. , Ward, T.E. , Coyle, S. , Diamond, D. :"Employing ensemble empirical mode decomposition for artifact removal: Extracting accurate respiration rates from ECG data during ambulatory activity",35th Annual International Conference of the IEEE EMBS Osaka, Japan, 3 - 7 July, 2013,pp.977 - 980

[199] Elgamel,S.A.,Soraghan, J. : "Empirical mode decomposition-based monopulse processor for enhanced radar tracking in the presence of high-power interference",IET Radar Sonar Navig., 2011, 5, (7), pp. 769 – 779.

[200] Rilling , G.: "Decompositions Modales Empiriques Contributions à la théorie, l'algorithme et l'analyse de performances", PhD thesis, University of Lyon -Ecole Normale Superieure de Lyon, 2004.

[201] Luan ,L. ,Yang, W., Haomin, Z.: " Iterative filtering as an alternative algorithm for empirical mode decomposition ", Advances in Adaptive Data Analysis, 2009,01, (04),pp. 543-560.

[202] Rilling, G., Flandrin, P., Goncalves, P., Lilly, J.M.: "Bivariate Empirical Mode Decomposition," in Signal Processing Letters, IEEE , , Dec. 2007,14, (12), pp.936-939.

[203] Zadeh LA (1963) Optimality and non-scalar-valued performance criteria. IEEE Trans Automat Contr AC-8:59–60

[204] Y. Wang, T. Tan, and A. K. Jain. Combining face and iris biometrics for identity verification. In 4th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA'03), pages 805–813, Berlin, Heidelberg, 2003. Springer-Verlag.

[205] T. Scheidat, C. Vielhauer, J. Dittmann, "Distance-Level Fusion Strategies for Online Signature Verification", In: Proceedings of the IEEE International Conference on Multimedia and Expo 2005 (ICME), Amsterdam, The Netherlands, 2005.

[206] Marler RT, Arora JS (2004) Survey of multi-objective optimization methods for engineering. Struct Multidiscipl Optim 26:369–395

[207] Scheidat, T., C., Vielhauer and J.Dittman, 2007. Single semantic MultiInstance fusion of handwritten based biometric Authentication systems.IEEE 1-4244-1437-7/07 ICIP 2007.

[208] Toufik Hafs , Layachi Bennacer, Mohamed Boughazi , Amine Nait-Ali," Empirical mode decomposition for online handwritten signature verification", IET Biometrics , IEEExplore, 10.1049/iet-bmt.2014.0041.

[209] Kholmatov, A.,Yanikoglu,B. :"Identity authentication using improved online signature verification method", Pattern Recognition Letters, 2005,26, pp.2400–2408.

[210] Fierrez, J., Ramos-Castro, D., Ortega-Garcia, J. , Gonzales-Rodriguez,J.: "Hmm-based on-line signature verification: feature extraction and signature modeling". Pattern Recognition Letters , 2007, 28, pp.2325-2334.

[211] Gruber, C., Gruber, T.,Krinninger, S.:"Online signature verification with support vector machines based on lcss kernel functions". IEEE Transactions on Systems, Man, and Cybernetics - Part B: Cybernetics, 2010, 40, pp.1088–1100.

[212] Nanni, L., Lumini, A.: “A novel local on-line signature verification system”, Pattern Recognition Letters, April 2008, 29, (5), pp.559-568.

[213] Muramatsu ,D., Matsumoto, T.: “Online Signature Verification Algorithm with a User-Specific Global-Parameter Fusion Model”, in Proceedings of IEEE International Conference on Systems, Man, and Cybernetics, San Antonio, USA , 2009, pp.486-491.

[214] Rashidi, S., Fallah, A., Towhidkhah, F.: “ Authentication Based on Pole-zero Models of Signature Velocity”, Journal of Medical Signals and Sensors. 2013,3, (4), pp.195-208.

[215] Ly Van, B., Garcia-Salicetti, S., Dorizzi, B.: “On using the Viterbi path along with HMM likelihood information for on-line signature verification”, IEEE Transactions on Systems Man and Cybernetics Part B , 2007,37, (5), pp.1237-1247.