RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE El BACHIR EL IBRAHIMI DE BORDJ BOU ARRERIDJ

Thèse

Présentée à la Faculté Mathématique et Informatique

Département d'informatique

En vue de l'obtention du diplôme de doctorat 3ème cycle (**LMD**)
En **I**nformatique **D**écisionnelle et **I**nformatique **D**istribuée
IDID

Par: SAIDANI Kaouther

Thème

Mise en œuvre d'un système de prise de décision incrémentale en vue d'une identification biométrique multimodale temps réel

---

Soutenue le : Devant le jury composé de :

Pr. BOUBETRA Abdelhak	Université de BBA	(Président)
Pr. KHABABA Abdallah	Université de Sétif	(Examinateur)
Pr. BENHOCINE Abdelhamid	Université de Sétif	(Examinateur)
Dr. MEROUANI Abdelbaki	Université de BBA	(Examinateur)
Pr. MOSTEFAI Messaoud	Université de BBA	(Rapporteur)
Dr. BOUZIANE Abderraouf	Université de BBA	(Co-Rapporteur)

Remerciement

Je tiens en premier lieu a présenter mon grand respect et mes sincères remerciements a mon directeur de thèse ***Pr.M.MOSTEFAI*** pour son aide précieuse qu'il m'a apporté pour l'élaboration de ce travail, pour sa présence constante, pour sa veillance afin d'interpréter et d'analyser les résultats obtenus. Je n'oublie jamais qu'il a travaillé avec moi avec grande sincérité, qu'il m'a toujours encouragé afin d'affronter tous les obstacles pour faire aboutir ce travail de recherche à son terme.

Je remercie également ***Dr.A.BOUZIANE*** d'accepter le rôle de Co-encadreur et pour ses orientations.

Mes remerciements les plus chaleureux vont également à notre chef de formation (3ème cycle -Doctorat LMD ***'IDID'***) ***Pr.Abdelhak BOUBETRA*** pour ses encouragements et ses orientations.

Je suis très honorée que ***Pr.A. BOUBETRA***, ait accepté de présider le jury de ma thèse.

C'est également un très grand honneur d'avoir comme membre du jury les Messieurs :

Pr. KHABABA Abdallah	Université de Sétif
Pr. BENHOCINE Abdelhamid	Université de Sétif
Dr. MEROUANI Abdelbaki	Université de BBA

Que leurs remarques et leurs critiques soient les bienvenues.

Je voudrais aussi témoigner ma gratitude envers mes enseignants, mes encadreurs, ainsi que toutes les personnes qui ont contribué à ma formation.

J'adresse mes sincères remerciements à toutes les personnes avec qui j'ai eu la chance de travailler : ***Dr.S.Akrouf, Dr.A.Moussaoui, B.Abbadi, A.Oulefki, A.Bengadouj, S.Bekakchi .***

En un mot je remercie tous ceux qui m'ont aidé à concrétiser de prés ou de loin mes recherches.

Tables des matières

Liste des figures

Liste des tableaux

Résumé

Abstract

ملخص

Introduction générale

Chapitre 1

Systèmes d'authentification biométriques

1.1 Introduction 3

1.2 Procédé de vérification de l'identité d'une personne 3

1.2.1 Définition de la biométrie 4

1.2.2 Propriétés d'un système biométrique 5

1.2.3 Fonctionnement et architecture générale d'un système biométrique 7

1.2.4 Contraintes sur les systèmes biométriques 8

1.3 Evaluation des systèmes biométriques 9

1.4 Les modalités biométriques 11

1.4.1 Modalité visage 12

1.4.2 Modalité iris 14

1.4.3 Modalité géométrie de la main 15

1.4.4 Modalité empreinte digitale 15

1.4.5 Modalité voix 16

1.4.6 Modalité signature 17

1.4.7 Autre modalité 19

1.5 Applications et marché des systèmes biométriques 19

1.6 Discussion 20

Chapitre 2

Approche Adoptée

2.1 Introduction 22
2.2 Intérêt de la multimodalité 22
2.3 Description générale du système développé 23
2.3.1 Le personnage virtuel 24
2.3.2 L'agent visage 25
2.3.3 L'agent voix 29
2.3.4 L'agent décideur 30
2.3.5 La construction de la base de données biométriques 30
2.4 Stratégies de fusion 35
2.4.1 La somme simple 35
2.4.2 La somme pondérée 35
2.5 Faiblesses du système 37
2.5.1 Principales difficultés de la reconnaissance de visage 37
2.5.1 Principales difficultés de la reconnaissance vocale 38
2.6 Discussion 39

Chapitre 3

Authentification par la modalité signature

3.1 Introduction 40
3.2 Nature des signatures manuscrites 41
3.3 Le processus d'authentification de la signature manuscrite 43
3.3.1 Acquisition de la signature 44
3.3.2 Extraction des descripteurs 45
3.3.3 Mesure de similarité et classification 46
3.3.3.1 Déformation Temporelle Dynamique (DTW) 46
3.3.3.2 Distance de Hausdorff 52

3.4 Techniques d'acquisition des signatures online 53
3.5 Nouveau système d'acquisition online des signatures 54
3.6 Procédé d'acquisition online d'une signature 56

Chapitre 4

Approche Efficiente d'authentification de Signature en ligne

4.1 Introduction 59
4.2 Système d'acquisition 60
4.3 Authentification de la signature 62
4.3.1 Construction de la base de données 62
4.3.2 Tests préliminaires d'authentification 62
4.3.3 Constat général 64
4.4 Amélioration de la précision de l'authentification 64
4.4.1 Forme de la main au moment de la signature 64
4.4.2 Extraction du descripteur forme de la main 68
4.4.3 Fusion au niveau des scores 74
4.4.4 Avantages du descripteur de la forme de la main proposé 76
4.4.4.1 Détection des changements d'habitudes du signataire 76
4.4.4.2 Détection des efficiente des contrefaçons 77
4.4.5 Calcul de complexité 79
4.5 Comparaison de l'approche proposée avec d'autres techniques avancées 80
4.6 Discussion et conclusion 81

Chapitre 5

Méthodes de fusion

5.1 Introduction **83**
5.2 Les types de fusion **83**
5.2.1 Système multi- échantillons 83
5.2.2 Système multi- capteurs 83
5.2.3 Système multi- algorithmes 84
5.2.3 Système multi-instances 84
5.2.3 Système multi-biométries 84
5.3 Les différents niveaux de fusion **85**
5.4 La fusion au niveau des scores **88**
5.4.1 Normalisation des scores 88
5.4.1.1 Les différentes techniques de normalisation de scores 89
5.4.2 Approche par classification de scores 90
5.4.3 Combinaison des scores 90
5.5 Conclusion **92**

Chapitre 6

Vers une prise de décision incrémentale

6.1 Introduction **93**
6.2 Comportement autonome **93**
6.3 Architecture proposée **94**
6.3.1 Mécanisme de prise de décision incrémentale 95
6.3.2 Environnement de validation 96
6.4 Principales limites du système développé **97**

Conclusion générale ***99***
Références
Productions scientifiques

Liste des figures

Chapitre 1

Systèmes d'authentification biométriques

FIGURE 1.1 Les modalités biométriques **5**

FIGURE 1.2 Architecture générale d'un système biométrique **8**

FIGURE 1.3 Caractéristiques de performance d'un système biométrique **10**

FIGURE 1.4 Illustration du TFA et du TFR **11**

FIGURE 1.5 Courbe de performance ROC **12**

FIGURE 1.6 Exemple de méthodes de reconnaissance du visage **14**

FIGURE 1.7 Schéma de l'iris **15**

FIGURE 1.8 Reconnaissance du contour de la main l'iris **16**

FIGURE 1.9 Les points caractéristiques «les minuties » **17**

FIGURE 1.10 Vitesse en (X) et (Y) d'une signature **19**

FIGURE 1.11 Marché de la biométrie **21**

Chapitre 2

Approche Adoptée

FIGURE 2.1 Description du système développé **24**

FIGURE 2.2 Détection de visage **25**

FIGURE 2.3 Exemples des caractéristiques pseudo-haar **26**

FIGURE 2.4 Image intégrale **27**

FIGURE 2.5 La chaine de classifieurs en cascade **28**

FIGURE 2.6 Les fichiers associés de la personne inscrite **32**

FIGURE 2.7 Echantillon de personnes Inscrites **32**

FIGURE 2.8 Exemple de variation d'éclairage **36**

FIGURE 2.9 Exemple de variation de pose **37**

FIGURE 2.10 Exemple de présence des composants structurels (lunettes) **37**

Chapitre 3

Authentification par la modalité signature

FIGURE 3.1 Les profils (*x*) et (*y*) d'une signature en fonction du temps **41**

FIGURE 3.2 Les profils (*x*) et (*y*) d'une signature d'un faussaire **42**

FIGURE 3.3 Vitesse en (*x*) et (*y*) d'une signature **43**

FIGURE 3.4 Le processus de l'authentification de la signature manuscrite **43**

FIGURE 3.5 Dispositifs électroniques d'acquisition online **45**

FIGURE 3.6 La correspondance point à point entre deux signatures par l'algorithme ***DTW*** **47**

FIGURE 3.7 Exemple de chemin de déformation optimale par l'algorithme ***DTW*** **47**

FIGURE 3.8 Alignement temporel entre *R* et *T* **48**

FIGURE 3.9 Exemple de mise en correspondance de deux signatures très proches **50**

FIGURE 3.10 Schéma de déformation correspondant **50**

FIGURE 3.11 Exemple de mise en correspondance de deux signatures différentes **51**

FIGURE 3.12 Schéma de déformation correspondant **51**

FIGURE 3.13 Distance de Hausdorff entre les signatures **53**

FIGURE 3.14 Le Système développé **55**

FIGURE 3.15 Le Système amélioré **56**

FIGURE 3.16 Décomposition de la vidéo en frames et extraction des positions **57**

Chapitre 4

Approche Efficiente d'authentification de Signature en ligne

FIGURE 4.1 Système d'acquisition de signature en ligne utilisé **61**

FIGURE 4.2 Trames successives obtenus pendant un processus de signature..... **61**

FIGURE 4.3 Comparaison entre signatures hors ligne et en ligne **61**

FIGURE 4.4 Courbe *ROC* montrant la performance de la modalité signature en ligne..... **63**

FIGURE 4.5 TFR et TAR par rapport au seuil de la modalité signature en ligne..... **63**

FIGURE 4.6 Distances des mains signataires..... **69**

FIGURE 4.7 Mains de signataires volontaires **71**

FIGURE 4.8 Scores calculées de la similarité de la main **72**

FIGURE 4.9 Courbe ROC montrant la performance de la modalité forme de la main **71**

FIGURE 4.10 TFR et TAR par rapport au seuil de la modalité forme da la main..... **71**

FIGURE 4.11 Arbre de décision adoptée **75**

FIGURE 3.12 Courbe ROC montrant l'amélioration des performances de deux modalités..... **75**

FIGURE 4.13 TFR et TAR par rapport au seuil de deux modalités..... **76**

FIGURE 3.14 Exemple des scores de similarité de la main (H_S) **77**

FIGURE 4.15 Courbe ROC montrant l'amélioration des performances de deux modalités..... **78**

FIGURE 4.16 TFR et TAR par rapport au seuil de deux modalités..... **79**

Chapitre 5

Méthodes de fusion

FIGURE 5.1 Sources de différents types de fusion de trais biométriques..... **85**

FIGURE 5.2 Résumé des approches de fusion dans les systèmes biométriques multimodaux.... **86**

FIGURE 5.3 Organisation d'un processus multimodal basé sur la fusion de caractéristiques..... **87**

FIGURE 5.4 Schéma de la fusion de scores **87**

FIGURE 5.5 Organisation d'un processus multimodal basé sur la fusion de décisions..... **88**

Chapitre 6

Vers une prise de décision incrémentale

FIGURE 6.1 Architecture proposée..... **95**

FIGURE 6.2 Niveaux de prise de décision **96**

FIGURE 6.3 Exemple d'états du personnage virtuel..... **97**

FIGURE 6.4 Interface de validation des scénarios d'interactivité entre agents **97**

Liste des tableaux

Chapitre 1

Systèmes d'authentification biométriques

Tableau 1.1 Les modalités biométriques et leurs propriétés **6**

Tableau 1.2 Avantages et inconvénients de la modalité visage **14**

Tableau 1.3 Avantages et inconvénients de la modalité iris **15**

Tableau 1.4 Avantages et inconvénients de la modalité géométrie de la main **16**

Tableau 1.5 Avantages et inconvénients des empreintes digitales **17**

Tableau 1.6 Avantages et inconvénients de la modalité voix **18**

Tableau 1.7 Avantages et inconvénients de la modalité signature **19**

Chapitre 2

Approche Adoptée

Tableau 2.1 Construction de la base de données **6**

Tableau 2.2 Résultats d'authentification **38**

Chapitre 3

Authentification par la modalité signature

Tableau 3.1 Exemples des signatures offline et online avec leurs caractéristiques dynamiques **.57**

Chapitre 4

Approche Efficiente d'authentification de Signature en ligne

Tableau 4.1 Résultats des tests d'authentification pour la modalité signature **64**

Tableau 4.2 Comparaison de certains systèmes basés sur la forme de la main **65**

Tableau 4.3 Résultats des tests d'authentification pour la modalité forme de la main **74**

Tableau 4.4 Structure de la base de données liée à la personne inscrite **74**

Tableau 4.5 Résultats des tests d'authentification de la combinaison de deux modalités **76**

Tableau 4.6 Résultats des tests d'authentification de la combinaison de deux modalités **79**

Tableau 4.7 Temps de calcul pour le traitement **80**

Tableau 4.8 Comparaison avec d'autres techniques principales **81**

Chapitre 5

Méthodes de fusion

Tableau 5.1 Résumé des techniques de Normalisation de Scores **89**

RÉSUMÉ

Cette thèse rentre dans le cadre d'un projet de recherche, visant à développer un système d'authentification biométrique multimodale. Le travail présenté porte sur l'amélioration des mécanismes de prise de décision en vue d'une authentification souple et robuste aux attaques intentionnelles et non intentionnelles.

Partant d'une architecture d'authentification bimodale (visage et voix) développée au sein de notre laboratoire, nous avons cerné les limites de cette dernière face aux différents types d'attaques, puis nous avons proposé le rajout de la modalité signature afin d'améliorer les performances d'authentification.

Une nouvelle approche d'authentification par la modalité signature est proposée. Cette dernière est basée sur un descripteur original permettant d'effectuer des authentifications robustes face aux attaques intentionnelles et non intentionnelles. Comparée aux solutions décrites dans la littérature, la solution proposée présente le meilleur compromis complexité/performance.

Dans le but d'humaniser le processus d'authentification, l'architecture développée est dotée d'un personnage virtuel capable d'interagir efficacement avec le milieu extérieur et d'exécuter des scénarios de prise de décision incrémentales basés sur les trois modalités visage, voix et signature.

Mots clés : Authentification biométrique, traitement de l'image, temps réel, prise de décision incrémentale, acquisition online de signature manuscrite, vérification automatique, fusion.

ABSTRACT

This thesis returns within the framework of a research project aiming to develop a multimodal biometric authentication system. This work focuses on improving the mechanisms of decision making for a flexible and strong authentication to intentional and unintentional attacks.

Starting from bimodal authentication architecture (face and voice) developed in our laboratory, we identified the limits of this latter cope with different types of attacks, and we have proposed the addition of modality signing in order to improve authentication performance.

A new authentication approach modality signature is proposed. The latter is based on an original descriptor for performing robust authentication cope with intentional and unintentional attacks. Compared to the solutions described in the literature, the proposed solution provides the best compromise complexity / performance.

In order to humanize the authentication process, the developed architecture is equipped with a virtual character able to interact effectively with the outside environment and run scenarios incremental decision-making based on three modalities face, voice and signature.

Keywords: Biometric authentication, image processing, real-time, online acquisition of handwritten signature, automatic verification, fusion.

ملخـــــص

تأتي هذه الأطروحة في إطار مشروع بحث، يهدف إلى تطوير نظام للتعرف البيومتري متعدد الأنماط. يتعلق العمل المقدم، بتحسين آليات اتخاذ القرار، بغية التوصل إلى تعرف مرن و قوي في مواجهة الهجومات المقصودة و غير المقصودة.

انطلاقا من تصميم لنظام للتعرف ذو نمطين (الوجه و الصوت) مطور في مخبرنا، أحطنا بحدود هذا النظام في مواجهة مختلف أنواع الهجمات، ثم اقترحنا اضافة نمط التوقيع قصد تحسين أداء التعرف.

تم اقتراح مقاربة جديدة للتعرف عن طريق نمط التوقيع. تعتمد هذه الأخيرة على واصف يسمح بالقيام بتعرفات قوية في مواجهة الهجومات المقصودة و غير المقصودة. فبالمقارنة مع الحلول المنصوص عليها في النصوص، يمثل الحل المقترح، حلا وسطا بين التعقيد و الأداء.

و بهدف إعطاء الصبغة الانسانية لنظام التعرف هذا، فإن التصميم المطور مزود بشخصية افتراضية قادرة على الاندماج بشكل فعال مع الوسط الخارجي، و تنفيذ سيناريوهات لاتخاذ القرار المبني على الأنماط الثلاثة: الوجه، الصوت و التوقيع.

الكلمات المفتاحية: التعرف البيومتري – معالجة الصورة– اتخاذ القرار – التوقيع الالكتروني – التحقق الآلي – الربط.

Introduction Générale

Introduction Générale

Les besoins accrus en dispositifs de sécurité pour la protection des biens et des personnes ont favorisé le développement d'une panoplie de techniques et systèmes d'authentifications plus ou moins complexes et efficaces. Les performances de ces derniers sont souvent évaluées en offline et rarement sur site. Ceci rend la tâche de leur mise en service réel difficile, surtout dans le cas ou les exigences en niveaux de sécurité sont élevées (banques accès à des sites sensibles etc.…).

Plusieurs solutions basées sur des systèmes asses complexes ont été proposées. Bien qu'elles permettent d'obtenir des niveaux de sécurités élevées, ces dernières sont souvent chères et contraignantes, et ne se prêtent pas à une utilisation grand public.

Nous présenterons dans ce travail une expérience de mise en œuvre d'un système d'authentification biométrique multimodale développé au sein de notre laboratoire. Les faiblesses relevées face aux imitations frauduleuses des caractéristiques biométriques nous ont poussés à travailler sur le développement d'un module de prise de décision basé principalement sur les avancées dans le domaine de la prise de décision incrémentale.

Après une description globale des systèmes d'authentifications biométriques multimodaux existants nous nous focaliserons en deuxième partie sur le système développé au sein de notre laboratoire, et présenterons ses faiblesses face aux changements imprévus qui peuvent survenir durant son fonctionnement et aussi, les limites face aux attaques intentionnelles.

En troisième partie nous présenterons les améliorations apportées à notre système concrétisées par le rajout de la modalité signature ainsi qu'un module personnage virtuel pour l'amélioration de l'interactivité du système avec le milieu qu'il contrôle. Bien sûr, le tout sera géré par un module de prise de décision incrémental capable de fournir plusieurs niveaux de sécurité.

La quatrième partie sera consacrée à notre contribution originale, qui consiste à améliorer les performances d'authentification par la modalité signature et la proposition d'un descripteur efficace contre les attaques intentionnées. Une validation expérimentale de la solution proposée est effectuée.

Etant dans un contexte multimodal, nous présenterons en cinquième partie un état de l'art des méthodes de fusion existantes. Le choix d'une méthode se fera en fonction des contraintes de performance et de complexité.

La sixième partie traite de la mise en œuvre de l'ensemble des modalités en vue d'une prise de décision incrémentale allant d'une simple authentification vocale ou visuelle jusqu'à une authentification bimodale de la signature online**.**

Enfin nous terminerons par une conclusion et des perspectives.

Chapitre 1

Systèmes d'authentification biométriques

Chapitre 1

Systèmes d'authentification biométriques

Ce chapitre présente les systèmes d'authentification biométriques. Dans un premier temps nous définissons la biométrie et montrer des exemples de son application. Par la suite, nous abordons le fonctionnement et l'architecture générale d'un système biométrique. Enfin nous détaillons quelques modalités biométriques en citant leurs avantages et inconvénients.

Sommaire

1.1 Introduction 3

1.2 Procédé de vérification de l'identité d'une personne 3

1.2.1 Définition de la biométrie 4

1.2.2 Propriétés d'un système biométrique 5

1.2.3 Fonctionnement et architecture générale d'un système biométrique 7

1.2.4 Contraintes sur les systèmes biométriques 8

1.3 Evaluation des systèmes biométriques 9

1.4 Les modalités biométriques 11

1.4.1 Modalité visage 12

1.4.2 Modalité iris 14

1.4.3 Modalité géométrie de la main 15

1.4.4 Modalité empreinte digitale 15

1.4.5 Modalité voix 16

1.4.6 Modalité signature 17

1.4.7 Autre modalité 19

1.5 Applications et marché des systèmes biométriques 19

1.6 Discussion 20

1.1 Introduction

Les exigences de sécurité de la société d'aujourd'hui ont placé la biométrie au centre d'un large débat car elle est en train de devenir un élément clé dans une multitude d'applications.

Depuis plusieurs années, des efforts importants sont fournis dans le domaine de la recherche en biométrie. Ce constat s'explique par la présence d'un contexte mondial dans lequel les besoins en sécurité deviennent de plus en plus importants.

Les applications biométriques sont nombreuses et permettent d'apporter un niveau de sécurité supérieur en ce qui concerne les accès *logiques* (ordinateurs, comptes bancaires, données sensibles, etc.) ou des accès *physiques* (bâtiments sécurisés, aéroports, etc.).

Traditionnellement, il existe deux modes d'authentification d'un individu : Le premier mode est basé sur une *connaissance* (code PIN, mot de passe, etc.), tandis que le second est basé sur une *possession* (badge, carte à puce, etc.). Ces deux modes d'authentification peuvent être utilisés de manière complémentaire afin d'obtenir une sécurité accrue. Cependant, chacun d'eux souffre de faiblesses qui peuvent dégrader considérablement leur utilité. En effet, les mots de passes peuvent être oubliés et les badges peuvent être perdus.

L'authentification biométrique est une solution alternative aux deux modes d'identification précédents. Elle comporte un avantage primordial sur les solutions d'authentification traditionnelles compte tenu de la forte relation entre l'authentifiant et l'utilisateur.

1.2 Procédé de vérification de l'identité d'une personne

Il existe trois façons génériques pour vérifier ou déterminer l'identité d'un individu :

- *Ce que l'on possède* (badge, Une carte avec puce électronique….).
- *Ce que l'on sait* (mot de passe, code PIN[1], …).
- *Ce qui caractérise une personne* (empreinte digitale, visage, iris, signature…).

Les risques de vol et de perte des cartes électroniques posent actuellement un réel problème surtout pour les cartes bancaires. Ajouté à cela, la perte, l'oubli et la découverte des mots de passe associés rendent les deux premiers types d'informations peu sécurisés [Jain 2000].

[1] **PIN**: **P**ersonal **I**dentification **N**umber –Numéro d'Identification Personnel

Le fait d'inclure les propriétés physiologiques et comportementales des individus dans tout processus d'authentification des personnes augmenterait considérablement leur niveau de sécurité [Ross2006] [Gorm2003].

1.2.1 Définition de la biométrie

La biométrie consiste à vérifier ou déterminer l'identité d'un individu à partir de ses caractéristiques biologiques (comme l'ADN), comportementales (comme la dynamique de la signature) ou morphologiques (comme l'empreinte digitale).

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. La *Figure 1.1* illustre un exemple de quelques modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique.

- *La biométrie comportementale :* se base sur l'analyse de comportements d'un individu (la démarche, dynamique de frappe au clavier, dynamique de la signature, etc.).
- *La biométrie biologique :* se base sur l'analyse des données biologiques liées a l'individu (salive, ADN, etc.)
- *La biométrie morphologique :* se base sur les traits physiques particuliers qui, pour toutes personnes, sont permanents et uniques (empreinte digitale, visage, etc.).

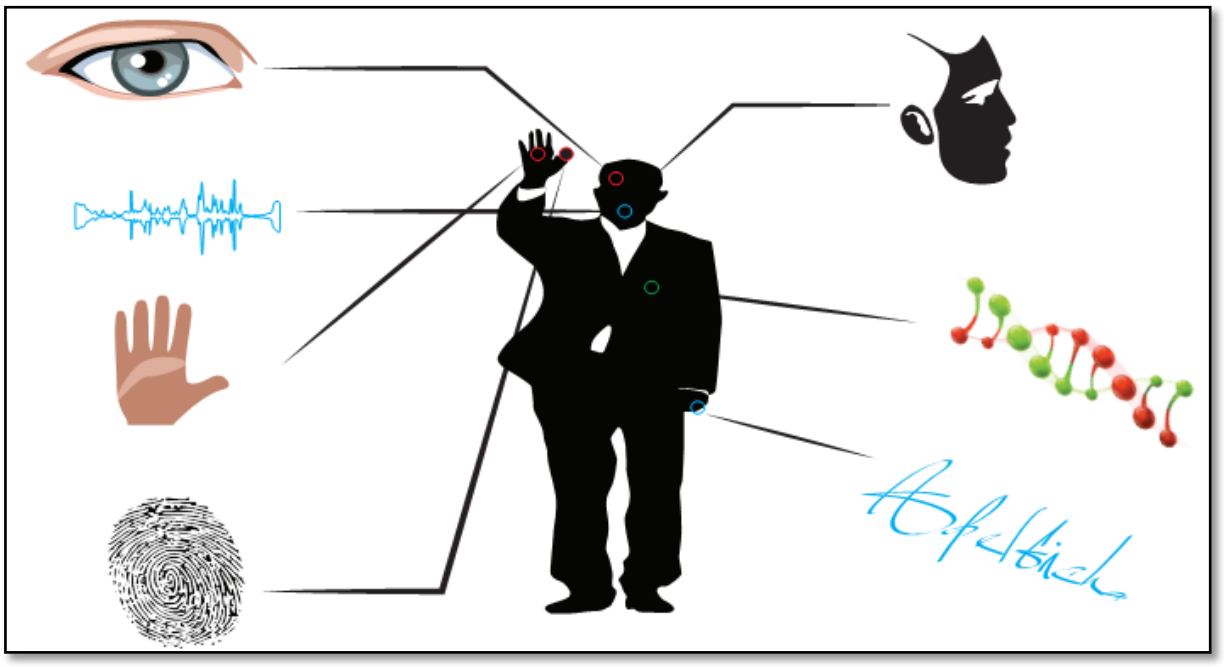


FIGURE 1.1- Les modalités biométriques (Physiques et comportementales)

1.2.2 Propriétés d'un système biométrique

Le cas parfait stipule qu'un trait caractéristique doit vérifier les critères suivants [Jain2004]:

- *universel* (exister chez tous les individus),
- *unique* (permettre de différencier un individu par rapport à un autre),
- *permanent* (autoriser l'évolution dans le temps),
- *enregistrable* (collecter les caractéristiques d'un individu avec son accord),
- *acceptable* (admise par les personnes à authentifier).

En réalité, peu de caractéristiques arrivent à satisfaire l'ensemble de ces conditions. Le *Tableau 1.1* présente les propriétés des principaux descripteurs biométriques susceptibles d'être utilisés dans les systèmes d'authentification biométriques.

Tableau 1.1- Les modalités biométriques et leurs propriétés (le nombre d'étoiles dans la colonne performance est relié à l'efficacité de l'authentification) [Mahi 2008]

Modalité	Universelle	Unique	permanente	enregistrable	acceptable	Performance
Modalités biologiques						
ADN[2]	Oui	Oui	Oui	Faible	Faible	*****
Groupe sanguin	Oui	Non	Oui	Faible	Non	*
Signal du cerveau (EEG)[3]	Oui	Oui	Oui	Faible	Non	****
Modalités comportementales						
Démarche	Oui	Non	Faible	Oui	Oui	***
Signature Dynamique	Oui	Oui	Faible	Oui	Oui	****
Dynamique de frappe	Oui	Oui	Faible	Oui	Oui	***
Voix	Oui	Oui	Faible	Oui	Oui	****
Modalités morphologiques						
Iris	Oui	Oui	Oui	Oui	Un peu	*****
Rétine	Oui	Oui	Oui	Oui	Un peu	*****
Visage	Oui	Non	Faible	Oui	Oui	****
Géométrie de la main	Oui	Non	Oui	Oui	Oui	****
Veine de la main	Oui	Oui	Oui	Oui	Oui	*****
Oreille	Oui	Oui	Oui	Oui	Oui	*****
Empreinte digitale	Oui	Oui	Oui	Oui	Oui	****

[2] **ADN** : **A**cide **D**ésoxyribo-**N**ucléique – Deoxyribo-Nucleic Acid.
[3] **EEG** : **E**lectro-**E**ncéphalo **G**raphie.

1.2.3 Fonctionnement et Architecture générale d'un système biométrique

Un système biométrique peut être représenté par quatre modules principaux [Jain2004]:

- *Module d'acquisition (capteur) :* Assure l'acquisition des traits caractéristiques de l'intrus sous forme de données biométriques brutes. Des prétraitements sur ces données peuvent avoir lieu, afin d'en préparer à l'opération d'extraction de descripteurs.

- *Module d'extraction de descripteurs :* Traite les données acquises pour en extraire l'ensemble des descripteurs. Ceci représente le trait caractéristique sous un format compact.

- *Module de comparaison :* Ce module est muni d'un classifieur qui s'occupe de comparer les descripteurs extraits avec un ensemble de descripteurs stocké dans une base de modèles. Quand il s'agit d'une identification, les descripteurs extraits sont comparés avec tous les modèles qui se trouvent dans la base (1:N). Pour la vérification, la comparaison se fait avec le modèle de la personne dont l'intrus prétend son identité (1:1). À l'issue de ce module, un ou n ensemble de taux de vraisemblance (des scores) sont générés.

- *Module de décision :* À travers un seuil spécifique de chaque personne enregistrée dans la base, ce module utilise les scores générés pour identifier l'intrus ou valider son identité.

Les systèmes biométriques fonctionnent selon trois modes que sont l'enrôlement, la vérification d'identité et l'identification (*Figure 1.2*) [Ross2003]:

- *Le mode d'enrôlement* : L'enrôlement est la première phase de tout système biométrique. Il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois. Pendant l'enrôlement, la caractéristique biométrique est mesurée en utilisant un capteur biométrique afin d'extraire une représentation numérique. Cette représentation est ensuite réduite, en utilisant un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker pour faciliter la vérification et l'identification.

- *Le mode de vérification ou authentification* : est une comparaison "1 :1", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisie avec le modèle biométrique de cette personne stockée dans la base de données du système. Dans ce cas, le système renvoie uniquement une décision binaire (oui ou non).

- *Le mode d'identification* : est une comparaison "1 : N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. La personne peut ne pas être dans la base de données. Ce mode consiste à associer une identité à une personne.

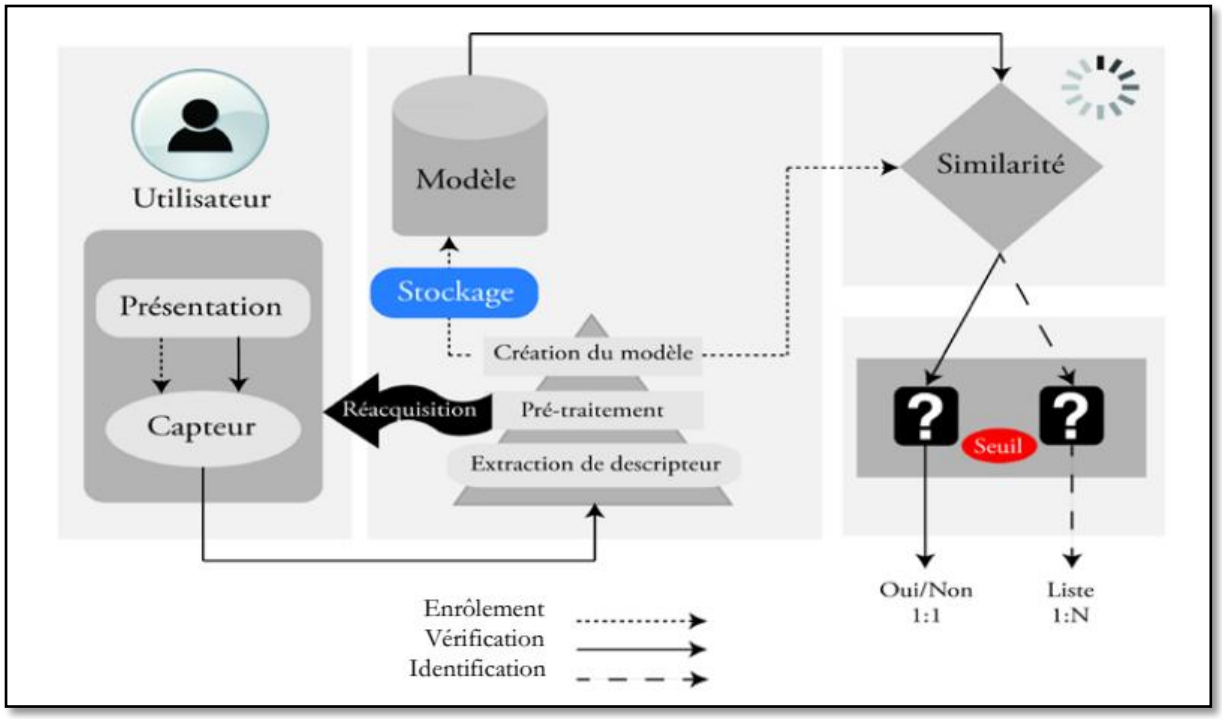


FIGURE 1.2- Architecture générale d'un système biométrique.

1.2.4 Contraintes sur les systèmes biométriques

Étant donné leur utilisation qui remonte à la fin des années 1960s, l'industrialisation des systèmes de reconnaissance automatiques biométriques a connu un décollage tardif. Cela est interprété par le manque de compétence nécessaire pour atteindre le niveau de sécurité demandé, qui dépend de plusieurs facteurs corrélés, à savoir :

- *L'acceptabilité.* Quand le système vise un usage grand public, le développeur doit tenir en compte les habitudes de la société et le niveau d'adaptabilité des personnes avec ce système, d'un point de vue ergonomie et facilité d'utilisation.

- *La performance.* Peu importe les conditions opératoires et environnementales, le processus de reconnaissance doit vérifier la vitesse et la précision demandées.

- *La finesse et la fiabilité.* Afin d'être fiable, le système peut réagir subtilement avec les tentatives de tromperie.

- *Le coût.* Pour une réussite dans le marché, le coût global du système doit être raisonnable.

1.3 Evaluation des systèmes biométriques

Un système biométrique est jugé performant s'il présente une efficacité et une robustesse en termes de précision et de vitesse de reconnaissance des individus. En évaluation de la précision de reconnaissance, trois métriques de performances sont souvent rencontrées [Abed2010] [Jain1999] :

- *Taux de Faux Rejets (TFR) :* Correspond au pourcentage de personnes légitimes, rejetées par erreur. [Bhat 2009].

- *Taux de Fausses Acceptations (TFA) :* Pourcentage d'imposteurs acceptés en tant que personnes légitimes. [ISO 2006].

- *Taux d'Egale Erreur (TEE) :* Ce taux est calculé à partir des deux premiers critères et correspond à l'endroit où TFR et TFA sont égaux, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations [Cher2009].

La précision d'un système biométriques est évaluée par le taux d'égalité d'erreurs (TEE) qui est obtenu graphiquement, en s'appuyant sur la courbe ROC (Receiver Operating Characteristic). Cette dernière regroupe les deux caractéristiques correspondant à l'évolution de TFR et de TFA en fonction du seuil de décision. Le croisement des deux caractéristiques donnera le rapport cherché (*Figure 1.3*). Plus le TEE est petit, plus le système biométrique est précis et vice versa.

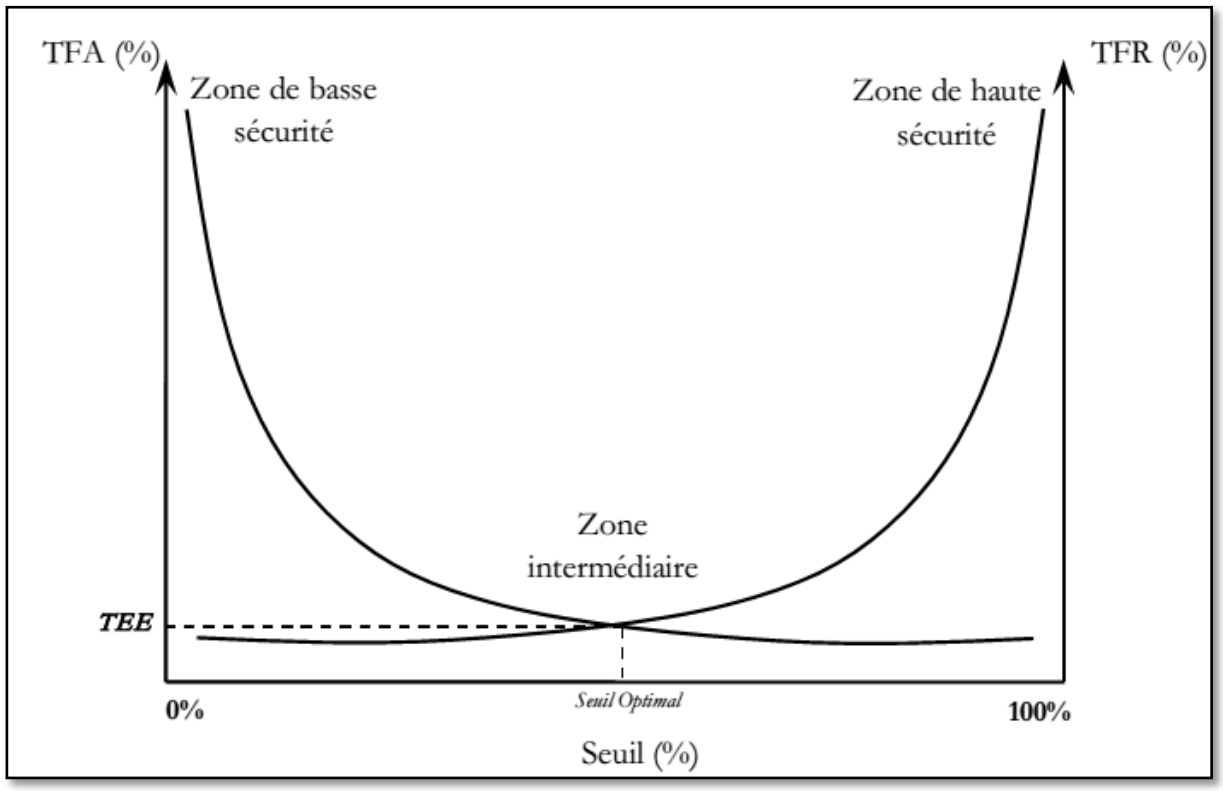


FIGURE 1.3- Caractéristiques de performance d'un système biométrique

La relation entre TFA et TFR est représentée dans la (*Figure 1.4*). Plus TFA est faible et plus TFR est élevé et vise vers ça. Il faut noter que les valeurs de ces erreurs sont directement liées au choix du seuil d'acceptation et de rejet qui dépend directement du type d'application.

En effet, dans le cas d'applications avec un niveau de sécurité très élevé (accès à une zone sensible), aucune fausse acceptation n'est tolérée et par conséquent la valeur de TFA est faible. Par-contre pour des applications moins sécurisées (accès à un parking public par exemple) un seuil d'acceptation beaucoup plus faible est toléré ce qui se traduit par un TFA élevé [Alla2009].

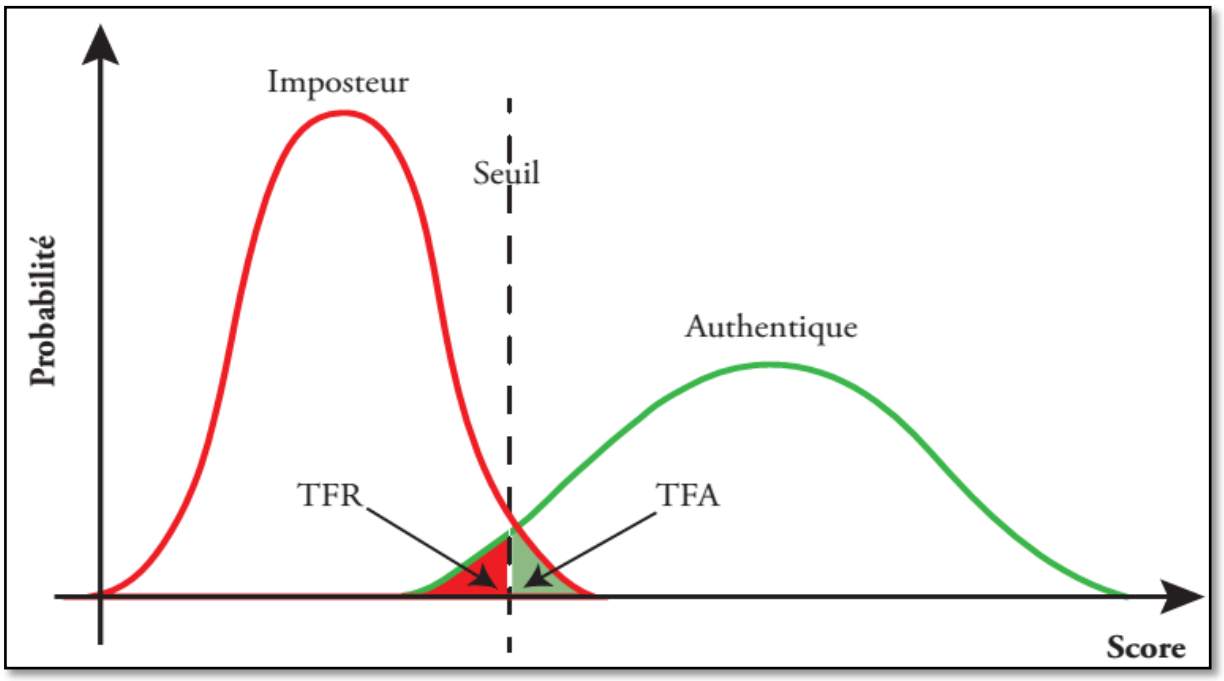


FIGURE 1.4- Illustration du TFA et du TFR.

La performance des systèmes d'authentification peut être aussi mesurée à partir de la courbe ROC ('Receiver Operating Characteristic')[4] qui permet de tracer le taux de faux rejets en fonction du taux de fausse acceptation (*Figure 1.5*). Plus cette courbe est proche de la forme du repère, plus le système est performant [Perr2002] [Egan1975] [Kuku2009].

La performance est un critère souvent demandé en systèmes de reconnaissance biométrique. De ce fait, les développeurs doivent cerner les facteurs qui permettent d'avoir une bonne performance. Ces facteurs sont liés à trois éléments : le trait caractéristique proprement dite (la biométrique), le dispositif d'acquisition, et la méthode de reconnaissance utilisée.

- *Le trait biométrique:* En fonction de la quantité d'information distinctive (descripteurs) contenue un tel trait biométrique, la reconnaissance sera plus ou moins performante.

- *Le dispositif d'acquisition:* Le rôle du dispositif d'acquisition se manifeste dans sa capacité de coder la modalité choisie de la façon qui permet d'extraite le maximum de descripteurs pertinents.

[4] **ROC**: **R**eceiver **O**perating **C**aracteristics curve–Courbe représentant les taux d'erreurs.

- *La méthode de reconnaissance:* Tout dépend de la biométrique acquise et la technique d'acquisition, la contribution de la méthode de reconnaissance adoptée à augmenter la performance, réside dans la manière d'extraction des descripteurs pertinents et l'adaptation de la métrique de mesure de vraisemblance avec la nature des informations acquises.

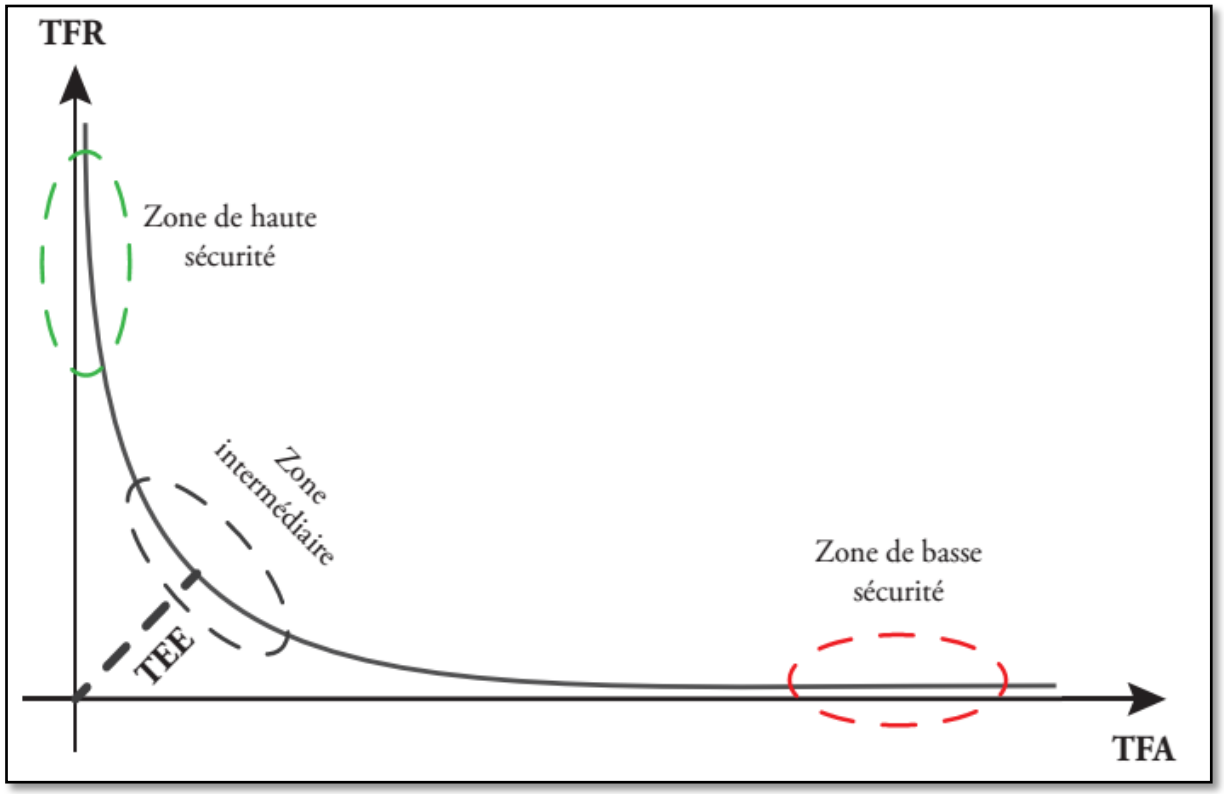


FIGURE 1.5- Courbe de performance ROC

1.4 Les modalités biométriques

Les différentes caractéristiques par lesquelles il est possible d'identifier un individu sont appelées modalités biométriques. Dans ce qui suit nous allons passer en revue les principales modalités couramment utilisées (ou étudiées) dans la construction des systèmes d'authentification monomodaux et multimodaux, les avantages et les inconvénients de chacune d'elles seront cités d'un point de vue coût et performance [Jain2000][IBG2010].

1.4.1 Modalité visage

Le visage est si complexe qu'on ne peut le considérer comme une simple modalité. En effet, une littérature abondante dans les diverses disciplines (cognitives, psychologiques, mathématiques, informatique, sociologique, etc….) démontrent bien la complexité de l'ensemble des facettes de cette modalité.

En voulant imiter le processus complexe d'authentification de personne chez l'être humain, des chercheurs ont proposé au fil des temps des modèles mathématiques visant à caractériser le visage en vue d'une authentification automatique des personnes. Ainsi, les premières applications de reconnaissance du visage se basaient principalement sur de simples représentations géométriques de ce dernier [Gold1971]. Par la suite, et avec les progrès de la technologie de l'information, de nouvelles méthodes plus complexes et plus performantes ont vu le jour [Siro1987]. Les plus connues parmi celles-ci sont :

- *Méthode d'Analyse en Composantes Principales (PCA) :* Cette méthode fut développée au MIT Media Lab©par Turk et Pentland 1991. Cette technique de l'algèbre linéaire est aussi connue sous le nom Eigenfaces (du fait qu'elle utilise des vecteurs propres pour caractériser la face avec ses erreurs résiduelles) (voir *Figure 1.6 (a)*). Cette méthode globale qui travaille directement sur les pixels de l'image est sensible aux changements d'éclairement de pose et d'expressions faciales [Turk1991].

- *L'Elastic Bunch Graph Matching (EBGM) :* Méthode globale qui permet de localiser les points caractéristiques du visage (coins du nez, des yeux, de la bouche.) puis à appliquer un treillis élastique à partir de ces points caractéristiques (*Figure 1.6 (b)).* Chaque point représente un nœud labélisé auquel lui est associé un jeu de coefficients d'ondelettes complexes, appelés « Jet ».

La reconnaissance d'un visage à partir d'images de tests se fait alors par mesure de similarité entre les différents jets et les longueurs des segments du treillis des images comparées [Wisk1997] [Bolm2003].

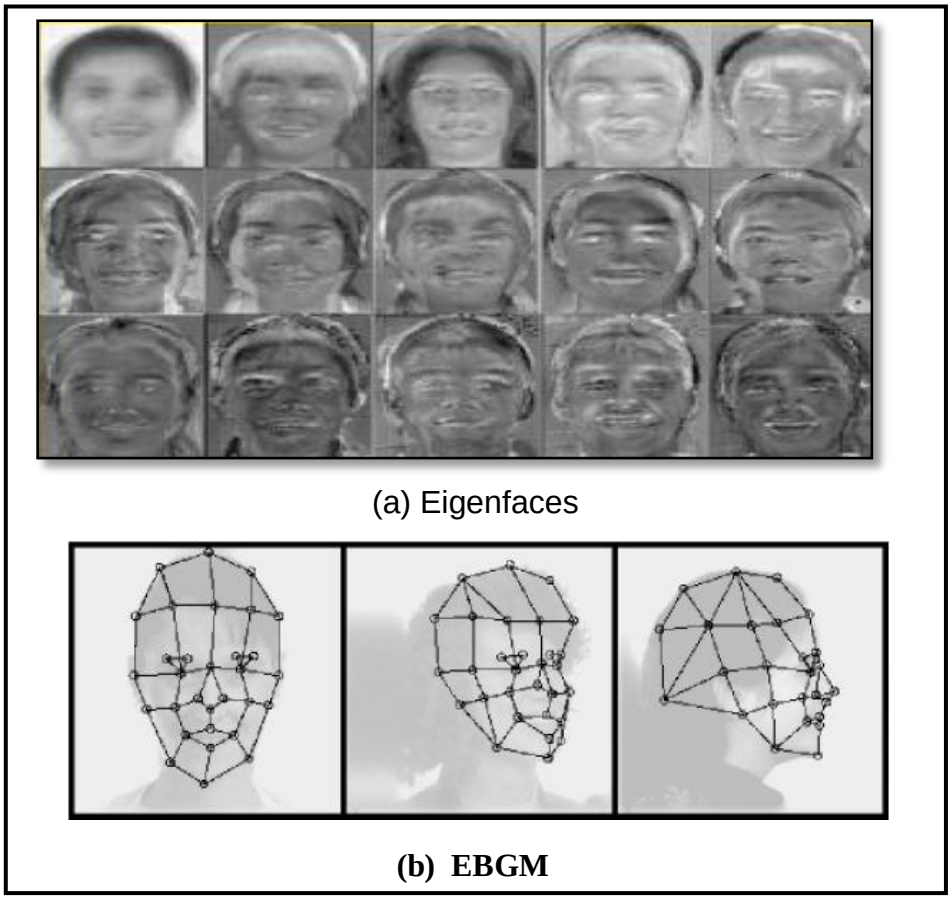


FIGURE 1.6- Exemple de méthodes de reconnaissance du visage

Le *Tableau 1.2* décrit quelques avantages et inconvénients liés à cette modalité.

Malgré sa sensibilité aux conditions d'acquisition et à l'état de la personne, cette modalité reste de loin la plus utilisée dans la majorité des systèmes d'authentification biométriques.

Tableau 1.2- Avantages et inconvénients de la modalité visage

Avantages	Inconvénients
Absence de contact avec le capteur.	Sensible à l'état de la personne : déguisement, maquillage, ajout d'accessoire de type lunettes, bonnet ou écharpe.
Méthode non intrusive pour la personne.	L'image est considérée comme trop personnelle pour être utilisée.
Pas de risques pour la santé.	Les traits du visage changent avec le temps
N'exige pas des personnes de faire un effort particulier.	Sensible aux changements de conditions d'éclairages.

1.4.2 Modalité iris

Le procédé de reconnaissance automatisé de l'iris est relativement récent [John2004]. Du fait de son unicité structurelle, l'iris peut être utilisé pour identifier avec certitude un individu (*Figure 1.7*) [Hill2003] [West1998]. L'extraction de l'image de l'iris exige l'utilisation d'une caméra haute définition doté d'une lumière infrarouge qui permet d'assurer un éclairage adapté.

Les principaux avantages et inconvénients de cette modalité sont résumés dans le *Tableau1.3*.

Bien qu'elle soit performante, cette technique reste relativement chère et contraignante.

FIGURE 1.7- Schéma de l'iris

Tableau 1.3- Avantages et inconvénients de la modalité iris

Avantages	**Inconvénients**
Très grande fiabilité	Phase d'acquisition lente.
Aucun contact avec le capteur	Positionnement de l'œil sur l'appareil contraignant.
Haut niveau de sécurité.	Réticence assez forte.
	Contraintes d'éclairage.

1.4.3 Modalité géométrie de la main

L'exploitation de la géométrie de la main pour l'authentification de personne est une pratique ancienne. Bien qu'elle soit facile à mettre en œuvre, cette modalité présente un handicap majeur qui est celui de sa non-unicité, ce qui limite considérablement ses performances [Ross1999].

FIGURE 1.8- Reconnaissance du contour de la main

Tableau 1.4- Avantages et inconvénients de la modalité géométrie de la main

Avantages	Inconvénients
Acceptabilité moyenne.	Unicité pas garantie.
très simple à utiliser.	système encombrant.
	rapport prix et fiabilité.

1.4.4 Modalité empreinte digitale

D'après les archives historiques, cette modalité semble être la plus ancienne car des traces qui datent de plus de 4000 ans ont été découvertes en Egypte. Cette modalité fut aussi utilisée très tôt par les Chinois pour signer des documents officiels. La puissance de cette modalité réside dans le fait que le dessin formé par les empreintes est unique pour chaque personne.

Les systèmes de vérification procèdent en général à l'extraction des caractéristiques principales de l'empreinte telles que les bifurcations de crêtes, les terminaisons, le centre etc…. et les utilise pour l'authentification (*Figure 1.9*) [Waym2005].

Les principaux avantages et inconvénients de cette modalité sont présentés au *Tableau 1.5*

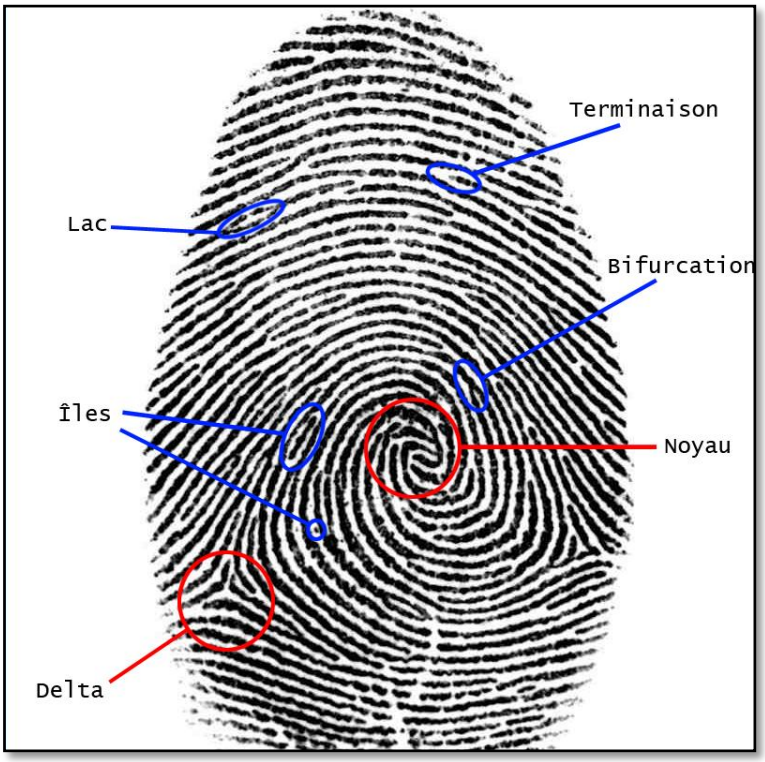


FIGURE 1.9- Les points caractéristiques «les minuties »

Tableau 1.5- Avantages et inconvénients des empreintes digitales

Avantages	Inconvénients
Technique la plus mûre, utilisée, maîtrisée et reconnue.	Lecture compromise si les doigts sont sales ou abimés.
Taille et prix du capteur abordable.	Possibilités de fraude par moulage du doigt.
Facile à utiliser avec un traitement rapide.	Risques de contamination par contact
Caractérisation unique de la personne.	
L'arrangement d'arêtes demeure permanent durant toute la vie.	

1.4.5 Modalité voix

S'il y'a une modalité qui est couramment utilisée pour véhiculer l'information entre individus c'est bel et bien la voix humaine [Wood2003] [Purz1963] [Broe1999]. Du fait de ses caractéristiques sonores, cette dernière se trouve noyée dans un monde plein de sons et de bruits

(avec ou sans sens). Ceci rend l'utilisation et l'exploitation de cette dernière à des fins d'authentification difficile. En effet, des erreurs d'interprétations peuvent facilement être commises si les bonnes conditions d'acquisitions ne sont pas vérifiées [Nist 2005].

Par ailleurs, du fait de sa simplicité, cette modalité reste très attractive, et beaucoup de travaux et projets de recherches sont continuellement lancés pour une exploitation efficace de la voix; dans la majorité des systèmes d'authentification interactifs [Rayn2000][Rayn2005].

Cette thématique assez large couvre principalement les axes suivants : Authentification du locuteur et reconnaissance de la parole. Seul l'axe authentification du locuteur nous concerne pour la construction de systèmes d'authentifications multimodaux incluant la modalité voix. Une étude détaillée de cette modalité est présentée dans [Erik2007].

Les principaux avantages et inconvénients de cette modalité sont présentés au *Tableau 1.6*.

Tableau 1.6- Avantages et inconvénients de la modalité voix

Avantages	**Inconvénients**
Aucun contact avec le capteur.	Sensibilité à l'état physique et émotionnel d'un individu.
Capteur généralement disponible (microphones).	Sensibilité aux conditions d'enregistrement du signal de parole : bruit ambiant et qualité du capteur (microphone) utilisé.
	Fraude possible par enregistrement de la voix de la personne.

1.4.6 Modalité signature

A la différence des autres modalités, la signature est une invention de l'homme qui vise à caractériser une personne par un ensemble de gestes instinctifs et réguliers produits par sa main. Le résultat de ce geste est reporté avec un stylo sur un support de type papier ou autre [Giat2005].

Comme c'est le cas pour les empreintes digitales, la signature est aussi une pratique ancienne bien ancrée dans les sociétés anciennes et modernes. Malgré ses limites, cette modalité non-contraignante connaît actuellement un regain d'intérêt lié aux avancées technologiques dans le domaine des supports d'acquisition numériques. Ces derniers ont favorisé le développement de

nouvelles techniques et systèmes d'authentification online de signatures dynamiques nettement plus performants que les procédés offline statiques qui travaillent seulement avec la signature sur papier [Mauc 1965][Lorr 1999] . En effet, en plus de la forme de la signature, les nouveaux dispositifs permettent l'extraction d'informations de type vitesse, accélération, pression, et inclinaison du stylo (*Figure 1.10*) rendant ainsi l'authentification plus précise.

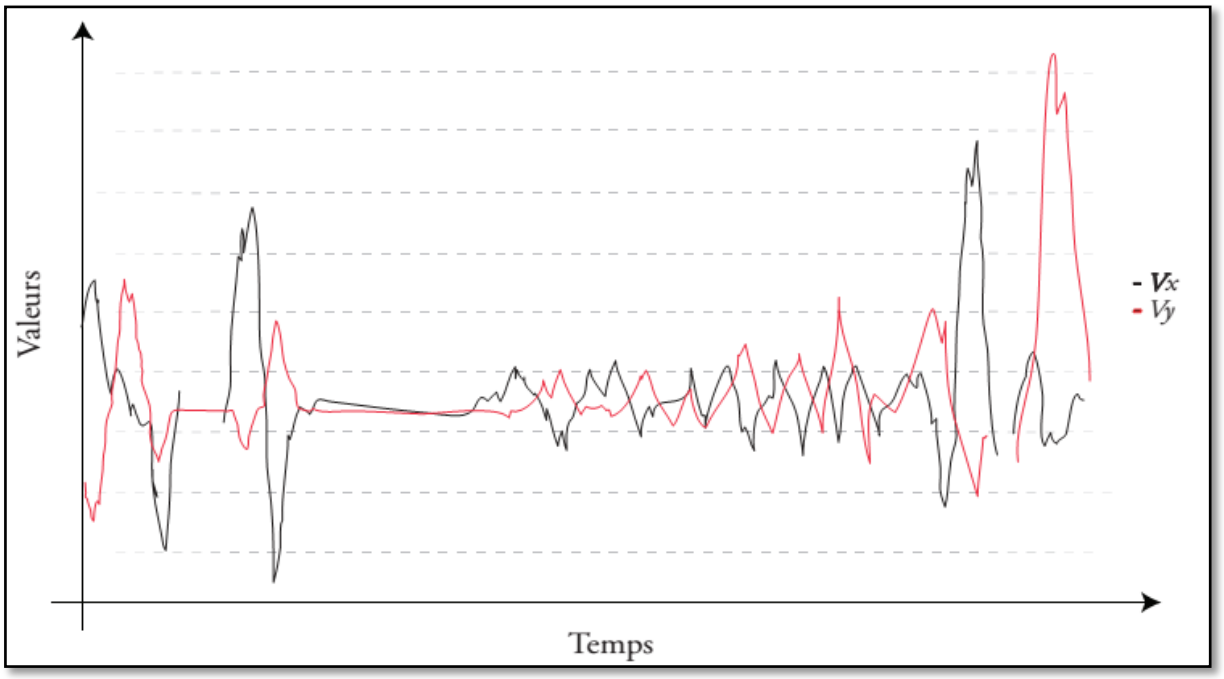


FIGURE 1.10- Vitesse en (X) et (Y) d'une signature

Les principaux avantages et inconvénients de cette modalité sont présentés au *Tableau 1.7*.

Tableau 1.7- Avantages et inconvénients de la modalité signature

Avantages	**Inconvénients**
Ergonomie	Sensible à l'état émotionnel et physique de la personne.
geste commun et socialement accepté	Fraude possible par copie d'une signature.
Difficilement imitable dans un temps très court (env. 2 sec)	
Technique aboutie basée sur le comportement	

1.4.7 Autres modalités

D'autres types de modalités sont en cours d'exploitation, et vont certainement bouleverser le monde des systèmes d'authentification biométriques. Il s'agit principalement des systèmes basés sur l'extraction de la forme de veines de la main. Bien qu'ils soient performants, ces derniers restent relativement chers. Mais il est encore tôt pour donner un avis relatif à l'exploitation de cette modalité [Jain1999].

1.5 Applications et marché des systèmes biométriques

Les applications de la biométrie peuvent être divisées en trois groupes principaux:

- *Applications commerciales:* telles que la sécurité de données électroniques, l'e-commerce[5], l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des archives, etc.

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

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

Le marché des systèmes biométriques représentait environ 5 milliards de dollars en 2008 [IBG 2010][6] (*Figure 1.11*). Les technologies les plus répandues sont les empreintes digitales (48% du marché), trait de visage (12% du marché), la géométrie de la main (11%), l'iris (9%), la reconnaissance vocale (6%), la signature (2%), les autres modalités telles que la rétine, la morphologie des oreilles ainsi que la radiographie dentaire (12%). Notons que les techniques comportementales (comme la démarche, le sourire, le mouvement des yeux, etc...) ont du mal à s'imposer.

[5] **E-C**ommerce : **C**ommerce **E**lectronique.
[6] **IBG**: **I**nternational **B**iometric **G**roup.

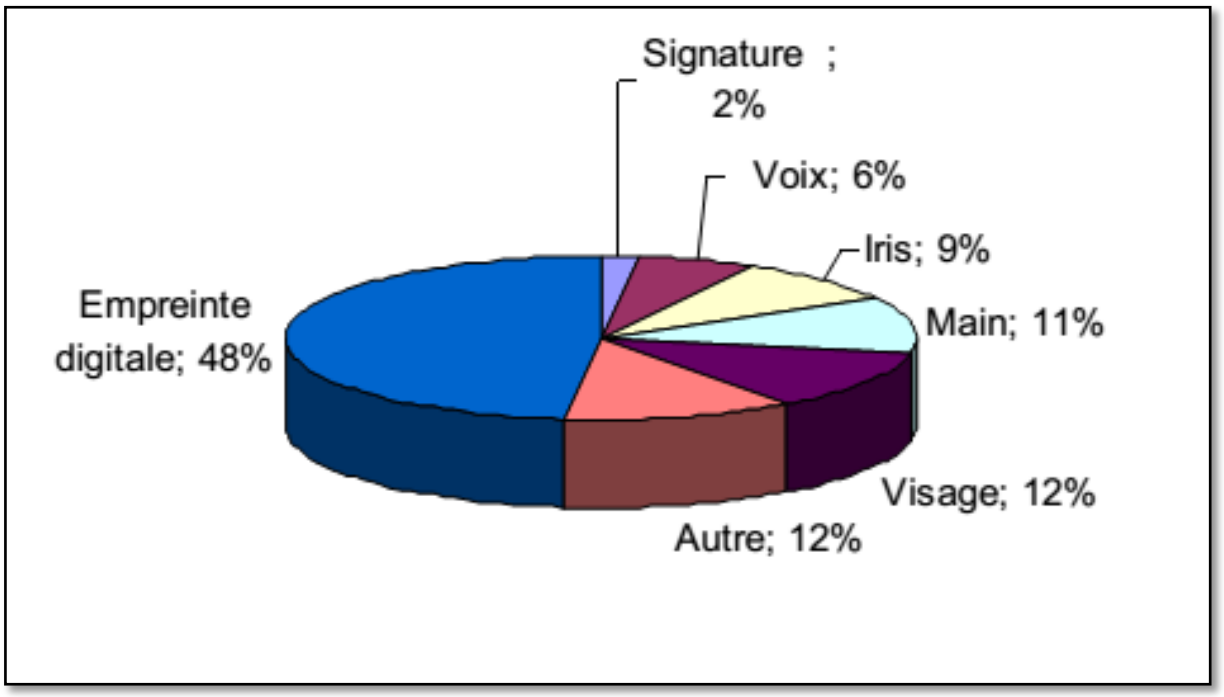


FIGURE 1.11- Marché de la biométrie

1.6 Discussion

D'après ce qu'on a vu précédemment, les systèmes monomodaux (utilisant une seule modalité) n'assurent, généralement, pas une authentification fiable. Cependant, la fusion d'informations présentées par les différentes modalités peut permettre une vérification robuste de l'identité [Ross 2006].

Un premier travail effectué au sein de notre laboratoire MSE visait à développer un système d'authentification bimodale basé sur les deux modalités visage et voix a été effectué [Akro2010]. Une amélioration du système développé est présentée dans [Chik2012].

Dans le chapitre suivant on va traiter en détail le système proposé (Système bimodale visage-voix), et présenterons les limites de ce dernier face aux changements de contextes et aux imitations intentionnelles.

Chapitre 2

Approche Adoptée

Chapitre 2

Approche Adoptée

Ce chapitre, présente notre système d'authentification bimodale qui utilise simultanément les deux modalités visage et voix pour l'authentification d'une personne, nous donnons tout d'abord une description générale du système développé, ensuite nous présentons les limites de ce dernier face aux changements de contextes et aux imitations intentionnelles. A cause de ces limites, nous montrons l'importance et la nécessité d'inclure ou de rajouter une troisième modalité pour surmonter ces limitations et renforcer le processus de prise de décision du système.

Sommaire

2.1 Introduction 22

2.2 Intérêt de la multimodalité 22

2.3 Description générale du système développé 23

2.3.1 Le personnage virtuel 24

2.3.2 L'agent visage 25

2.3.3 L'agent voix 29

2.3.4 L'agent décideur 30

2.3.5 La construction de la base de données biométriques 30

2.4 Stratégies de fusion 35

2.4.1 La somme simple 35

2.4.2 La somme pondérée 35

2.5 Faiblesses du système 37

2.5.1 Principales difficultés de la reconnaissance de visage 37

2.5.1 Principales difficultés de la reconnaissance vocale 38

2.6 Discussion 39

2.1 Introduction

Compte tenu de son importance, le domaine de l'identification biométrique est devenu un axe de recherche à part entière [Jain2004] [Jain2006]. Généralement les systèmes d'identification efficaces opèrent sur plusieures modalités pour améliorer les résultats de l'identification (approche multimodale) et de produire des résultats très satisfaisants dans le cas de conditions d'acquisition idéales [Akro2009] [Alla2009]. Malheureusement les conditions idéales sur le terrain (éclairage stable, la distance et la position de l'intrus par rapport à la caméra, absence de bruit sonore, etc ....) sont rarement réunies.

La montée des attentats et les risques d'insécurité ont poussé les sociétés de développement à doubler d'efforts pour proposer des systèmes de plus en plus efficaces mettant en jeux une ou plusieurs modalités dans leur processus d'authentification [Bouz2009]. A la différence des systèmes monomodaux qui sont en général simples, les systèmes multimodaux connaissent actuellement un succès croissant en raison de leur performance.

Les premiers systèmes basés sur la fusion du visage et de la voix ont été réalisés en 1995 [Brun1995], depuis cette date de nombreuses études ont été menées en associant différentes modalités, en faisant varier le niveau de fusion des données et en testant plusieurs règles de fusion [Ross2006].

Dans ce chapitre on va présenter le travail qui a été effectué au sein de notre laboratoire MSE et qui vise à développer un système d'authentification bimodale basé sur les deux modalités visage et voix [Akro2010]. Une amélioration du système développé est présentée dans [Chik2012].

2.2 Intérêt de la multimodalité

Les systèmes de reconnaissance biométriques, dits monomodaux, disposent d'une seule source d'informations biométrique *qu'on va traiter en détail dans le chapitre 5*. Ces systèmes sont souvent affectés par les limites suivantes [Jain2004] :

- *Bruit introduit par le capteur,*
- *Non-universalité,*
- *Manque d'individualité,*
- *Sensibilité aux attaques,*

- *Manque de représentation invariante*.

Quelques limites imposées sur ces systèmes peuvent être surpassées, en fusionnant plusieurs données biométriques de natures différentes, d'où la nécessité de passer vers les systèmes multimodaux [Ross2003][Kun2000].

D'un côté, cette approche s'adresse aux problèmes liés au manque d'universalité dans une population ou à l'instabilité d'une caractéristique chez la même personne. En général, ces problèmes conduisent à des taux TFR importants. En se basant sur plusieurs critères de reconnaissance, le système peut assurer le recouvrement d'un maximum de personnes légitimes.

D'un autre côté, les systèmes multimodaux sont susceptibles de répondre aux exigences strictes imposées par les applications critiques. Pour ces dernières, les fausses acceptations dues à une falsification ou une similarité à l'intérieur d'une population sont intolérables. Comme il est difficile d'imiter simultanément plusieurs traits caractéristiques, les systèmes multimodaux sont efficaces pour la réduction des tentatives frauduleuses et la minimisation des conséquences négatives des fausses acceptations.

Par ailleurs, la performance des systèmes monomodaux est sensible aux informations brouillées, à cause des mauvaises conditions d'acquisition, d'imperfection des capteurs ou d'une altération temporaire de la caractéristique biométrique. Pour les systèmes multimodaux, le défaut d'une modalité peut être compensé par d'autres modalités [VIE2006b].

2.3 Description générale du système développé

L'approche adoptée pour la conception de notre système s'inspire directement du processus complexe de prise de décision chez l'humain à savoir : une collaboration active entre les sens du cerveau sollicités [Wick2004].

Les principaux constituants de ce système (présentées en *Figure 2.1*) sont :

- *Un Agent personnage virtuel* : jouant le rôle d'interface dynamique avec l'extérieur.
- *Deux agents Actifs ;* ayant les rôles des parties du cerveau affectées aux sens mis en œuvre : vision, voix.

- *Un agent décideur « Decision Maker Agent »*[1] : ayant pour rôle la fusion des résultats obtenus par les modalités mises en œuvre et la transmission des consignes d'interactivité au personnage virtuel.

- *Une base de données multimodale*.

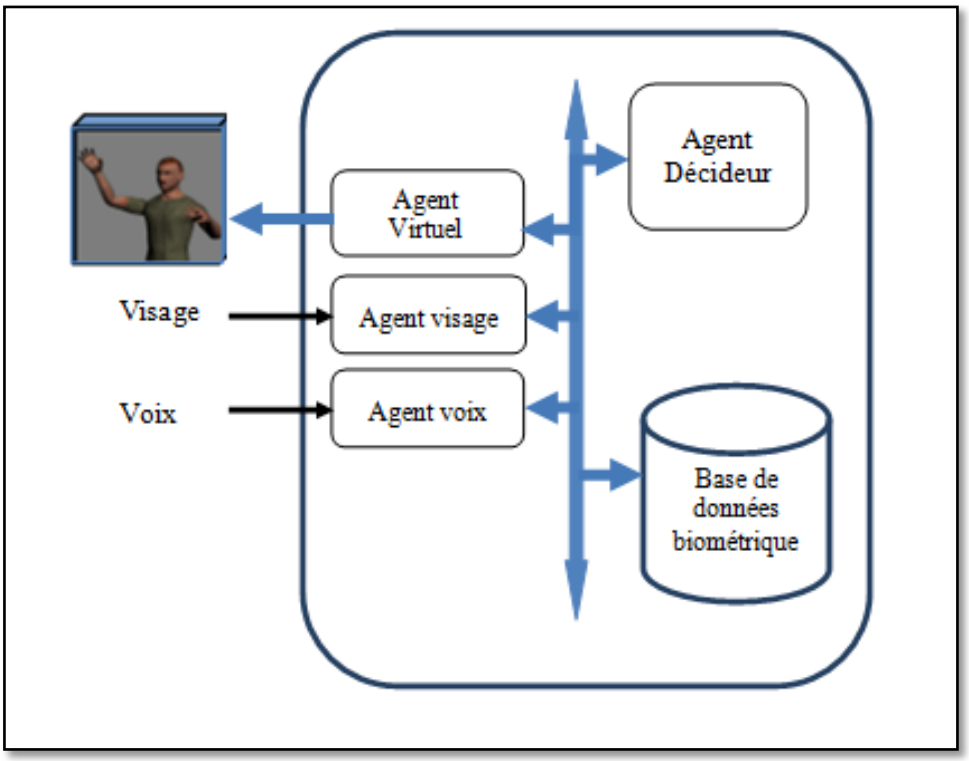


FIGURE 2.1- Description du système développé

2.3.1 Le personnage virtuel

Le rôle du personnage virtuel est d'assurer la bonne conduite des opérations d'inscription et d'authentification. Pour une première approche, le personnage évolue entre les deux états suivants:

- *Etat de repos*: au cours duquel aucune intrusion sonore ou visuel n'est rapportée.

- *État actif*: la déclaration d'une intrusion qui commute le personnage virtuel vers l'état actif consiste à envoyer une série de messages pour vérifier si l'intrus est un être humain ou non. Dans le cas d'un être humain, les processus d'inscription ou d'authentification sont lancés. Dans le cas de non-confirmation de la nature d'intrusion, une alarme retentit.

[1] **DMA**: **D**ecision **M**aker **A**gent – Agent Décideur.

2.3.2 L'agent visage

Le rôle de l'agent visage est la détection puis l'authentification du visage présent face à la caméra, *Figure 2.2*.

Pour la détection du visage, nous avons utilisé l'algorithme de *Viola et Jones* qui, en plus de sa disponibilité dans la bibliothèque *javacv* , se prête bien à un traitement en temps réel.

FIGURE 2.2- Détection de visage

- ***Explication de l'algorithme de Viola et Jones***

- ***Principe***

La méthode *Viola&Jones* a été proposée au départ pour la détection des visages dans une image numérique ou dans une séquence vidéo puis utilisée pour détecter d'autres objets comme les voitures.

Cette méthode combine quatre contributions clés qui sont les :

- ✓ *caractéristiques pseudo-haar,*
- ✓ *l'approche d'image intégrale,*
- ✓ *la méthode d'apprentissage adaptative AdaBoost,*
- ✓ *l'algorithme en cascades de classifieurs.*

1. Caractéristiques pseudo-haar

Une caractéristique *pseudo-haar* est représentée par un rectangle défini par son sommet, sa hauteur, sa longueur et son poids. Elle est calculée par la différence des sommes de pixels de deux ou plusieurs zones rectangulaires adjacentes.

La *Figure 2.3* ci-dessous présente des exemples de caractéristiques utilisées par *Viola et Jones*. Elles sont inspirées des descripteurs de haar qui ont été employés par Papageorgiou et *al* dans [Papa1998]. Les valeurs de ces caractéristiques sont calculées par la soustraction de la somme des pixels noirs de la somme des pixels blancs [Negr2008].

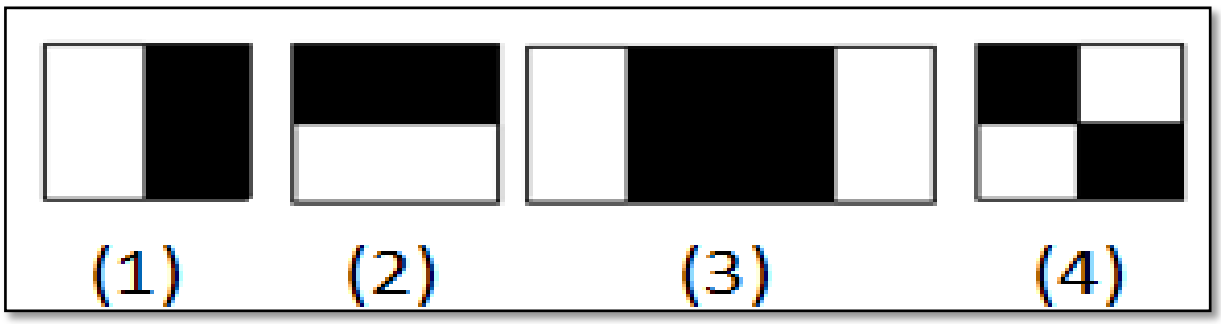


FIGURE 2.3- Exemples des caractéristiques pseudo-haar.

2. Approche d'image intégrale

La méthode d'image intégrale est utilisée pour déterminer la présence ou l'absence des caractéristiques dans chaque position de l'image et à n'importe quelle taille. Le but de cette méthode à part la détection de caractéristiques est la réduction du temps de calcul de ces dernières. La valeur intégrale de chaque pixel est la somme de tous les pixels au dessus de lui et de sa gauche.

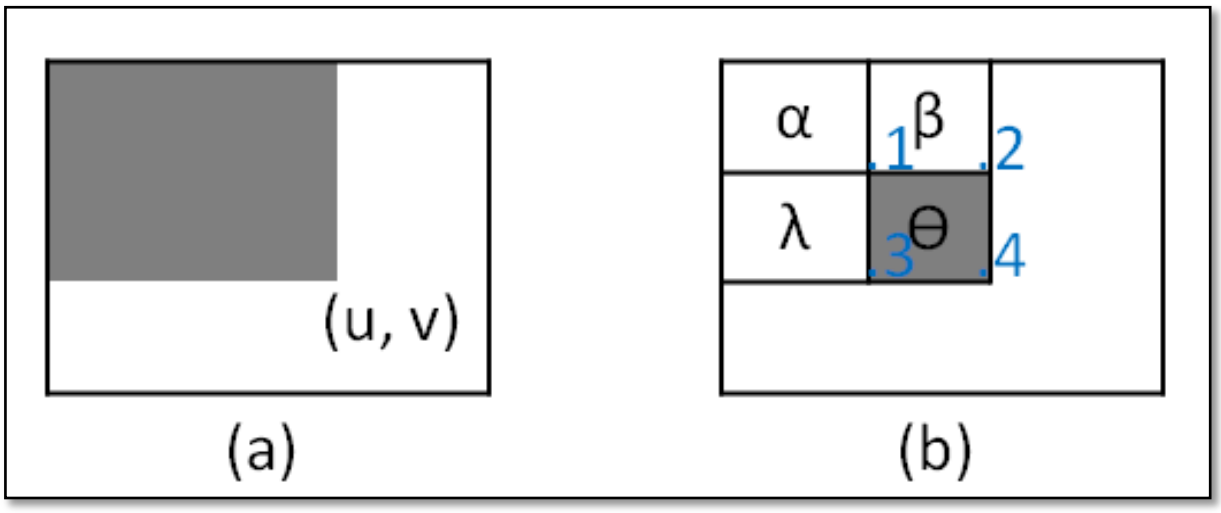


FIGURE 2.4- Image intégrale : (a) la valeur de l'image intégrale à la position (u, v), (b) calcul de la somme des valeurs de pixels dans le rectangleθ.

Dans le cas de la *Figure 2.4 (a)*, l'image intégrale est définie comme suit :

$$ii(u,v) = \sum_{u' \leq u,\, v' \leq v} i(u', v') \qquad (\mathbf{2.1})$$

Dans le cas de *Figure 2.4 (b)*, où on souhaite avoir la valeur d'image intégrale pour un rectangle (cas de rectangle θ dans la *Figure 2.4 (b)*). Nous pouvons obtenir la valeur de θ par le biais de l'expression ci-dessous :

$$\theta' = (\alpha + \beta + \lambda + \theta) - \big((\alpha + \beta) + (\alpha + \lambda)\big) + \alpha \qquad (\mathbf{2.2})$$

La somme des niveaux de gris des pixels dans la région rectangulaire θ est calculée rapidement à partir de quatre sommets de l'image intégrale selon l'équation ci-dessous :

$$\theta = ii(u_4\,, v_4) + ii(u_1\,, v_1) - \big(ii(u_3\,, v_3) + ii(u_2, v_2)\big) \qquad (\mathbf{2.3})$$

3. Algorithme AdaBoost

Paul viola et Michael Jones ont utilisé l'algorithme *AdaBoost* pour sélectionner les caractéristiques de *haar* à utiliser et pour fixer le niveau du seuil adéquat pour cette sélection. *Abadoost* combine plusieurs classifieurs *faibles* issus des caractéristiques *pseudo-haar* pour former un classifieur *fort*.

AdaBoost sélectionne un ensemble de classifieurs faibles. Il les combine et assigne un poids à chacun.

4. Algorithme en cascades de classifieurs

La quatrième contribution de la méthode *Viola&Jones* est la détection en cascades. Une cascade se compose de *n* filtres dont chacun est un classifieur *faible* composé d'une seule caractéristique *pseudo-haar* (*Figure 2.5*).

Au cours d'une détection, si un filtre échoue à passer une sous-région alors elle est immédiatement classée comme *Non visage* sinon la région passe vers le filtre suivant.

Les sous-régions de l'image qui traversent la totalité de la cascade sont classés comme *visage* et tous les autres sont classées *Non Visage*. Les poids qu'*AdaBoost* attribue aux filtres déterminent l'ordre des filtres dans la cascade commençant par le poids le plus lourd vers celui le plus faible pour éliminer les régions *Non visage* le plus tôt possible.

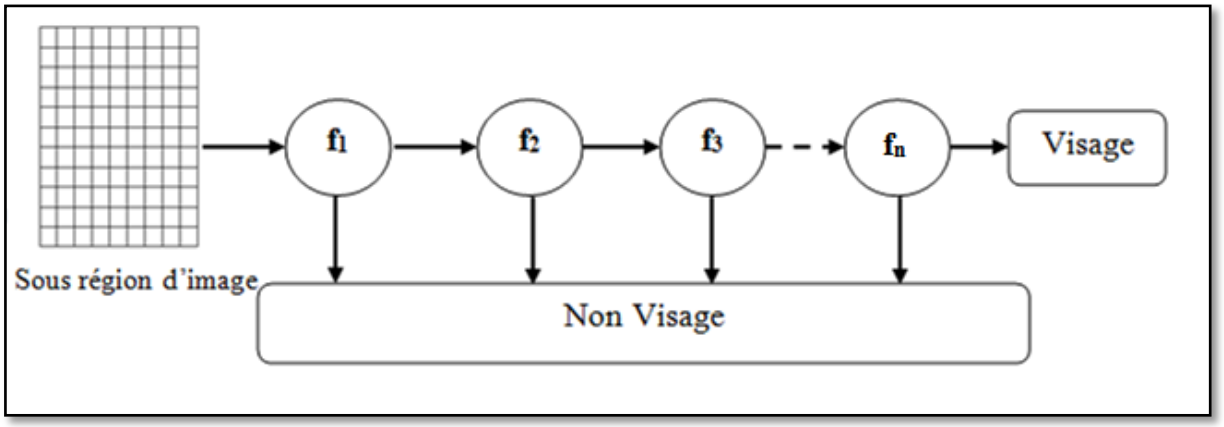


FIGURE 2.5- La chaine de classifieurs en cascade

Les avantages de l'algorithme de *Viola&Jones* sont :

- *Les caractéristiques pseudo-haar permettent la détection des objets en plusieurs échelles (détection multi-échelles).*
- *L'image intégrale permet le calcul des caractéristiques en temps réel.*
- *L'algorithme AdaBoost sélectionne les caractéristiques les plus discriminantes pour la classification et forme un classifieur de bonne performance.*
- *La cascade minimise le temps de calcul et affine les frontières de classification.*

- ***L'approche de vérification***

L'approche adoptée dans la vérification est basée sur la métrique de Hausdorff [Jeso2001], elle est considérée comme une mesure de similarité entre les formes naturelles.

Dans notre travail, cette métrique a été appliquée en tant que mesure de similitude entre les différents descripteurs de visage selon la définition suivante:

Considérez *S* et *T* comme deux ensembles de points. La distance de Hausdorff est défini par:

$$D_H\ (S,T) = \max\{f_d(S,T), f_d(T,S)\} \qquad (\mathbf{2.4})$$

Où f_d est appelée la distance relative de Hausdorff (ou semi-distance de Hausdorff). Elle est définie par :

$$f_d(S,T) = max_{p\in S} d(p,T) \qquad (\mathbf{2.5})$$

La distance *d* utilisé est habituellement la distance euclidienne.

2.3.3 L'agent voix

L'agent joue le rôle du système auditif chez l'homme. Il a pour fonction d'engager dans le cas d'un bruit, le processus de vérification et d'authentification de la voix.

La vérification du locuteur est basée sur des modèles de mélange gaussien (GMM).

$$W(n) = 0.54 - 0.46 * \cos\left(\frac{2\pi n}{N-1}\right) \qquad (\mathbf{2.6})$$

Après avoir calculé les coefficients MFCC (Mel Frequency Cepstral Coefficients) un modèle de locuteur est estimé en appliquant un algorithme d'estimation appelé EM (Expectation Maximization).

Le rapport de vraisemblance entre l'ensemble des paramètres biométrique et le modèle de l'individu permettra de calculer le score de la modalité voix.

2.3.4 L'agent décideur

Cet élément représente l'agent central (cerveau) qui rassemble les différentes références de nombreux autres agents et décide de prendre des mesures appropriées (accorder l'accès, refuser l'accès) exprimées par un agent conversationnel animé.

Dans le cas où un changement se produit dans la scène surveillée, un module de détection de mouvement envoie un message à l'agent décideur. Ce dernier déclenche le système de vérification comme une première action à la recherche d'un visage humain. Dans le cas d'une réponse positive l'agent visage et l'agent voix continuent à vérifier et un score de correspondance est généré.

Une tâche de raisonnement est effectuée sur ces résultats en utilisant l'une des méthodes de fusion qui seront détaillés dans le *chapitre 5*. L'agent décideur décide de l'action à entreprendre (accorder l'accès, refuser l'accès). Si le système identifie la personne avec succès, l'accès est alors accordé.

2.3.5 La construction de la base de données biométriques

Généralement, le processus adopté pour la construction de bases de données biométriques est basé sur le principe hors-ligne ' Premier arrivé, premier servi (PAPS)'. Une fois la base de données remplie, elle devient opérationnelle pour une utilisation dans un système d'authentification.

Souvent, et afin d'améliorer les performances de la recherche sur de telles bases, on procède à une réorganisation hors ligne des données acquises [Ross2006]. Cette approche contraignante va à l'encontre des exigences des systèmes temps réel qui doivent être capable de collecter et de réorganiser de manière fluide et transparente les données comme elles arrivent.

Si l'on veut rendre les systèmes d'authentification moins contraignants, plus autonome, et capable d'interagir de manière naturelle avec les humains, il est nécessaire de leur fournir des mécanismes de collecte et de réorganisation de données inspirés de ceux des humains.

Le mécanisme adopté par un des membres de notre laboratoire MSE (Responsable de la partie base de données) pour la construction de la base de données multimodale est basé sur les constatations suivantes :

- La mémoire humaine audiovisuelle se remplit progressivement avec le temps suite aux événements avec lesquels la personne est confrontée au cours de sa vie.

- Qui se ressemblent s'assemblent

Sur la base de ces deux constatations il est possible d'envisager la construction de systèmes d'authentification biométrique qui, au début de leur mise en service ne disposent d'aucune donnée dans leur base. Il n'y a donc plus de phases distinctes d'inscription puis d'authentification comme c'est le cas pour l'ensemble des systèmes d'authentification classiques, mais plutôt des opérations d'inscription enligne ou d'authentification. Ainsi, la procédure d'activation de l'une des deux phases suit la logique suivante :

SI *(personne détectée) & (autorisé à être enregistré)* ***ALORS***

Enrôlement

SINON *Authentification*

Afin d'assurer une organisation multimodale de la base de données, la structure multidimensionnelle (où chaque modalité est affectée à une dimension) est adoptée. Pour une première approche, une base de données biométriques 2D dédiée au stockage des deux modalités visage et voix fut construite.

Toute personne inscrite lui est associé quatre fichiers (*Figure 2.6*) indexés en fonction de la position de la personne dans une matrice de position de mémoire 2D. Cette dernière peut changer progressivement avec l'arrivée de nouveaux candidats. L'exemple suivant montre la procédure d'indexation de neuf personnes inscrites $\{P_0$ à $P_8\}$ en fonction de leur degré de similitude avec le groupe inscrit (*Figure 2.7*).

Le critère de similitude adopté entre les candidats est basé sur la métrique Hausdorff [Hutt 1993] pour la modalité visage et GMM avec MFCC pour la modalité voix [Iqba2011]. Les résultats de similarités obtenus (présentés dans le *Tableau 2.1.a* et *2.1.b*) nous permettent d'ordonner les personnes (*Tableau 2.1.c* et *2.1.d*) du plus similaire (avec un score élevé) au moins similaire (avec un faible score).

Enfin un indice codé est généré pour chaque personne inscrite selon sa position 2D. Comme indiqué dans le *Tableau 2.1.e* l'indice initial de la personne P_2 est 50. Cette valeur sera codée avec une clé secrète et utilisée pour produire les indices des fichiers de la personne requise.

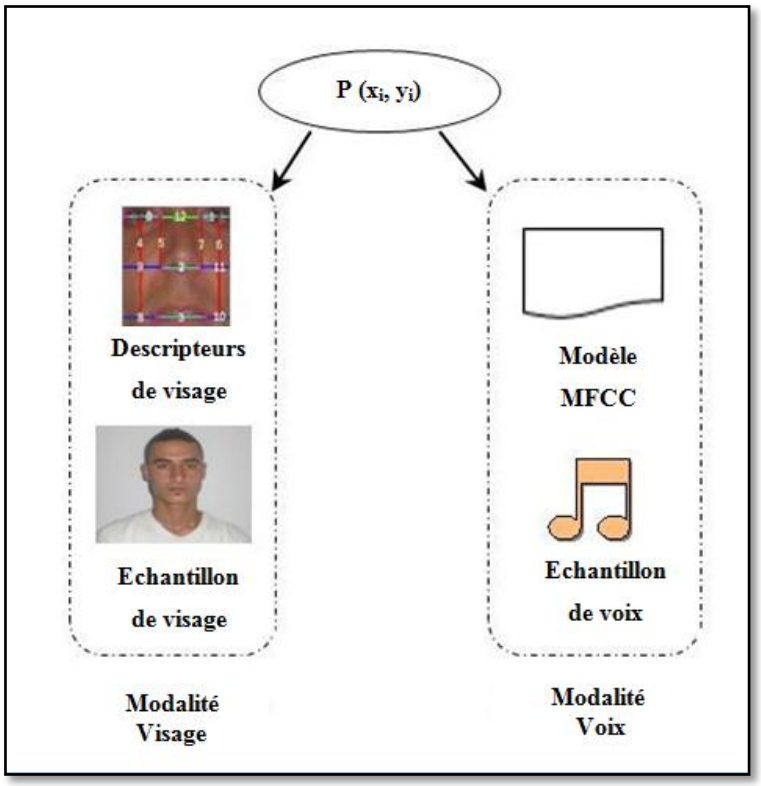


FIGURE 2.6- Les fichiers associés de la personne inscrite

FIGURE 2.7- Echantillon de personnes Inscrites

Tableau 2.1- Construction de la base de données

(a) Les résultats de similarité de visage des personnes inscrites

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_0	100	74	68	52	71	68	59	63	57
P_1	74	100	77	76	66	85	78	68	72
P_2	65	77	100	78	74	72	80	77	68
P_3	57	76	78	100	69	84	87	65	72
P_4	71	66	74	69	100	60	71	76	54
P_5	68	85	72	84	60	100	84	66	66
P_6	59	78	80	87	71	84	100	71	78
P_7	63	68	77	65	76	66	71	100	59
P_8	55	72	68	72	64	66	78	62	100

(b) Les résultats de similarité de voix des personnes inscrites

	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8
P_0	78	42	34	23	36	28	25	8	20
P_1	43	88	24	13	11	27	15	23	22
P_2	17	11	74	12	24	10	19	36	29
P_3	29	12	18	80	34	32	27	26	21
P_4	28	6	12	11	86	23	16	5	21
P_5	13	36	18	17	11	76	22	11	18
P_6	16	33	23	20	33	17	83	18	21
P_7	39	39	12	22	14	33	13	88	33
P_8	26	27	27	18	23	10	33	16	72

(c) Ordre des visages des personnes inscrites

Indice visage	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Score	52	62	65	57	54	56	59	59	55
Nouvel ordre	P_2	P_1	P_6	P_7	P_3	P_5	P_8	P_4	P_0

(d) Ordre des voix des personnes inscrites

Indice Voix	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Score	8	11	10	12	4	11	16	12	10
Nouvel ordre	P_6	P_3	P_7	P_1	P_5	P_2	P_8	P_0	P_4

(e) Nouvelles positions des personnes inscrites

Voix/Visage	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
0			P_6						
1				P_1	P_3				
2									
3			P_7						
4						P_5			
5	P_2								
6							P_8		
7									P_4
8								P_0	

L'intérêt de ce travail est de produire une base de données dynamique sécurisée par les techniques de marquage [Asma2012].

2.4 Stratégies de fusion

En général, les fusions dans les systèmes multimodaux sont divisées en deux classes. Dans la première classe, la fusion se produit avant le traitement de la correspondance (l'étape de capture qui opère sur les caractéristiques extraites). Cependant, dans la seconde classe, la fusion se fait après la manipulation (calcul d'un score final de la correspondance et la prise de décision appropriée).

Dans ce système, deux types de fusions ont été testées: la *somme simple* et la *somme pondérée*. Le score de correspondance est utilisé par le module de décision pour déterminer le résultat d'authentification finale de l'ensemble du système par une comparaison basée sur un seuil global.

2.4.1 La somme simple

Cette approche est tout simplement la moyenne des scores pour prendre la décision d'acceptation ou de rejet. Selon la règle suivante:

$$S = \frac{1}{N}\sum_{1}^{N} s_i \qquad (\mathbf{2.7})$$

2.4.2 La somme pondérée

Dans cette méthode, les scores sont pondérés par les relations de leur taux d'erreur (EER). La règle est décrite ci-dessus:

$$S = \sum_{i}^{N} w_i s_i \qquad (\mathbf{2.8})$$

N : nombre de termes utilisés.

w: poids $w = \frac{eer_i}{\sum_i^N eer_i}$

S : score

2.5 Faiblesses du système

Ce système possède des faiblesses face au changement de contexte (changement de la voix et/ou visage).

2.5.1 Principales difficultés de la reconnaissance de visage

Les principales difficultés rencontrées par un système de reconnaissance faciale sont [Souh2008][Said2006]:

- *Changement d'éclairage :* Les changements dans le temps de l'éclairage rendent le processus de reconnaissance du visage très difficile. En effet, les changements causés par les variations d'éclairage augmentent de façon significative la différence entre les données enregistrées dans la base (phase d'enregistrement) et les données acquise en ligne pour la vérification, entrainant ainsi une mauvaise authentification des sujets censés être autorisés à y accéder (*Figure 2.8*).

FIGURE 2.8- Exemple de variation d'éclairage

- *Variation de pose :* (*Figure 2.9*).

FIGURE 2.9- Exemple de variation de pose

- *Présence ou absence des composants structurels :* telles que la barbe, les lunettes , ou le moustache (*Figure 2.10*).

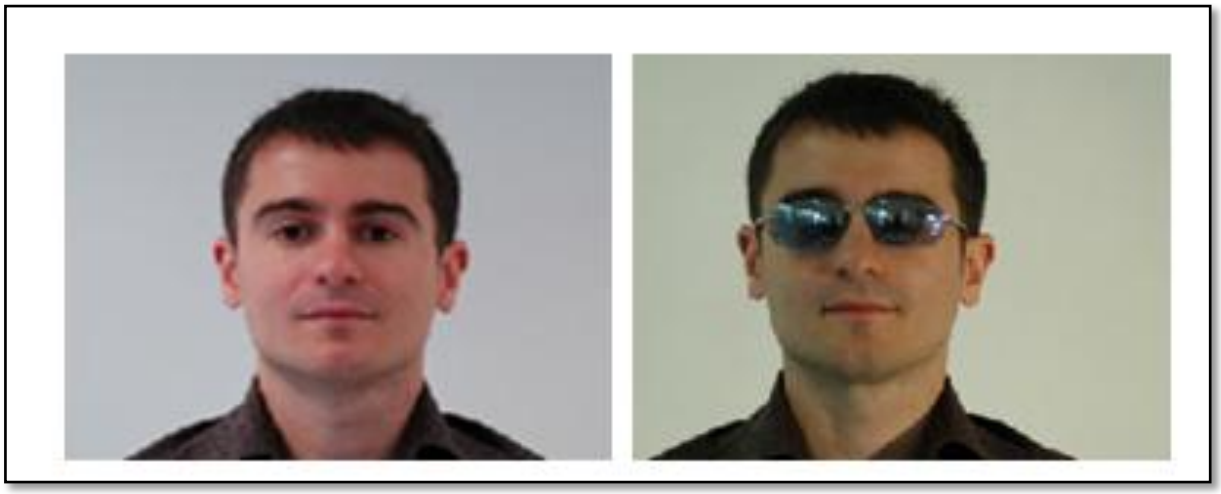


FIGURE 2.10- Exemple de changements en présence des composants structurels (lunettes)

- *Autres difficultés :*
  - ✓ *Expressions faciales,*
  - ✓ Les *vrais jumeaux qui ont le même indicatif d'ADN,*
  - ✓ *Occultations partielles,*
  - ✓ *Température du corps.*

2.5.2 Principales difficultés de la reconnaissance vocale

La performance du système d'authentification par la modalité voix dépend de :

- *la qualité du signal*, qui dépend de la variabilité de la voix du locuteur dans le temps comme dans le cas de maladie (*rhume*), des états émotionnels (*angoisse, joie*) et de l'âge,
- *Des conditions d'acquisition de la voix :* telles que le bruit et la réverbération,
- *la qualité des équipements* : tels que le microphone, sans oublier le fait que différentes personnes peuvent avoir des voix similaires.

Les résultats du *Tableau 2.2* suivant montrent les faiblesses de ce système face au changement de contexte (changement de la vois et/ou visage)

Tableau 2.2- Résultats d'authentification

Personne inscrite	**Pourcentage de similarité**	**Décision d'authentification**	
Authentification bimodale (visage et voix)	Cas 1	Visage de test 70% Voix similaire 73%	Authentifié
	Cas 2	Visage avec des lunettes 22% Voix similaires 78%	Rejeté
	Cas 3	Visage de test 76% Voix modifiée 13%	Rejeté

- ***Explication du tableau***

Une personne préinscrite est invitée à effectuer plusieurs tests d'authentification (*Tableau 2.3*). Les tests effectués incluent la voix et le visage. Si aucun changement pertinent ne se produit sur l'une des deux modalités, la reconnaissance dépasse 70 % (cas 1). Cependant, si des changements importants affectent l'une des deux modalités telles que: la même personne porte des lunettes (cas 2) ou modifie sa voix (cas 3), l'authentification échoue.

2.6 Discussion

Vu les faiblesses de ce système face au changement de contexte (changement de la vois et/ou visage) et aux imitations intentionnelles, l'utilisation des deux modalités visage et voix peut s'avérer insuffisante pour une authentification robuste d'une personne [Akro 2010].

Le rajout d'une troisième modalité est devenu nécessaire pour renforcer le processus de prise de décision du système.

Une étude approfondie sur modalités susceptibles d'être ajoutés à notre système est effectué. Cette dernière prend en considération les paramètres suivants :

- *Besoins pour la mise en œuvre de la modalité*
- *Degré d'acceptabilité par le grand public*
- *Performance d'authentification*

De toutes les modalités existantes, nous avons opté pour la signature qui reste de loin la plus adoptée par le grand public et cela malgré qu'elle soit faillible aux attaques intentionnelles.

Une vision nouvelle du processus de signature a permis à notre équipe de proposer un nouveau dispositif d'acquisition online de la signature qui permet non seulement de récupérer la signature, mais aussi de fournir des données discriminantes, capables de mettre en échec toute tentative d'imitation intentionnelle ou non [Oule2013].

Un état de l'art sur l'authentification par la modalité de la signature sera présenté au chapitre trois, suivi par la présentation de notre dispositif d'acquisition online de signature.

Chapitre 3

Authentification par la modalité signature

Chapitre 3

Authentification par la modalité signature

Ce chapitre présente l'authentification par la modalité signature. Dans un premier temps nous présentons un état de l'art sur les techniques développées pour l'acquisition, le traitement et l'authentification de la signature. Par la suite, nous abordons le système d'acquisition online développé.

Sommaire

3.1 Introduction 40

3.2 Nature des signatures manuscrites 41

3.3 Le processus d'authentification de la signature manuscrite 43

3.3.1 Acquisition de la signature 44

3.3.2 Extraction des descripteurs 45

3.3.3 Mesure de similarité et classification 46

3.3.3.1 Déformation Temporelle Dynamique (DTW) 46

3.3.3.2 Distance de Hausdorff 52

3.4 Techniques d'acquisition des signatures online 53

3.5 Nouveau système d'acquisition online des signatures 54

3.6 Procédé d'acquisition online d'une signature 56

3.1 Introduction

Les technologies d'authentification des personnes sont devenues le centre d'intérêts des différents secteurs socioéconomiques, visant à assurer une meilleure protection des biens et des personnes [Prab2007], [Boye2007]. Ces technologies sont, auparavant, basées sur des outils à détenir (les badges, les cartes d'identité, les mots de passe, etc.). Malheureusement ces derniers sont assujettis à la perte, le vol ou l'utilisation contrefaite.

L'avènement de la biométrie comme nouvel outil d'authentification a permis la construction de systèmes de sécurité plus performants que les systèmes traditionnels [Jain1999][Jain2000], [Viel2006]. Ces derniers exploitent les traits biométriques des individus (empreinte, voix, visage, iris etc.) pour effectuer une authentification précise et moins contraignants.

Les différents traits biométriques utilisés aujourd'hui peuvent être regroupés en deux familles: les traits physiologiques et les traits comportementaux. Pour les traits comportementaux, la signature manuscrite occupe une place privilégiée, du fait qu'elle est bien enracinée dans la société et largement reconnue comme un moyen légal et acceptable pour la preuve d'identité [Mill1994]. De plus, l'authentification par signature est, par opposition à de nombreuses modalités, un processus non envahissant et assez familiarisé par le grand public. Comme toutes les caractéristiques comportementales, la signature manifeste la volonté et la conscience de celui qui l'appose qui exprime, à cet effet, son approbation pour toute action qui suit [Viel2006a] [Yamp2008].

À cause de l'utilisation étendue de la signature manuscrite, surtout pour les transactions bancaires, ainsi que l'évolution marquante en TIC, l'automatisation de vérification s'avère une nécessité primordiale pour autant d'applications utilisant la signature, telles que les banques, le e-commerce et l'assurance [Urec1999][Fair1997][Wije2001]. Du fait que la signature reflète une relation complexe entre le comportement de la main pendant l'apposition et l'état psychophysique du signataire, la vérification automatique des signatures fait appel à des études pluridisciplinaires [Mill1994][Newh2000][Plam1995]. Plusieurs rapports récapitulatifs, qui résument les travaux de recherche actuels, ont été publiés dans la littérature. Le rapport de *Impedovo et Pirlo* [Impe2008] est un exemple de travail de synthèse de grande renommée dans ce contexte.

3.2 Nature des signatures manuscrites

Les signatures manuscrites existent en plusieurs formes et variétés. Nous avons les signatures acquises à partir d'un support papier par un scanner ou autre (signature offline), et celles acquise directement (online) lors de la signature par des dispositifs spécialisés.

L'acquisition des signatures offline est généralement non contraignante du fait qu'elle ne nécessite pas de matériel coûteux. Cependant, l'authentification de ce type de signatures pose de réels problèmes du fait de l'absence des propriétés dynamiques de la signature. Pour y remédier, plusieurs procédés d'acquisition online de signatures furent proposés [Impe2008].

La signature dynamique est généralement capturée par un dispositif spécialisé de type (tablette graphique, caméra, etc…) qui peut fournir les données suivantes :

$$S(t) = [x(t), y(t), p(t)] \text{ (coordonnées et pression du stylet)}$$

Un exemple de données dynamiques d'une signature est présenté en (*Figure 3.1*). Comme on peut le constater cette signature présente deux ***Pen-up*** correspondants à des levés de stylo.

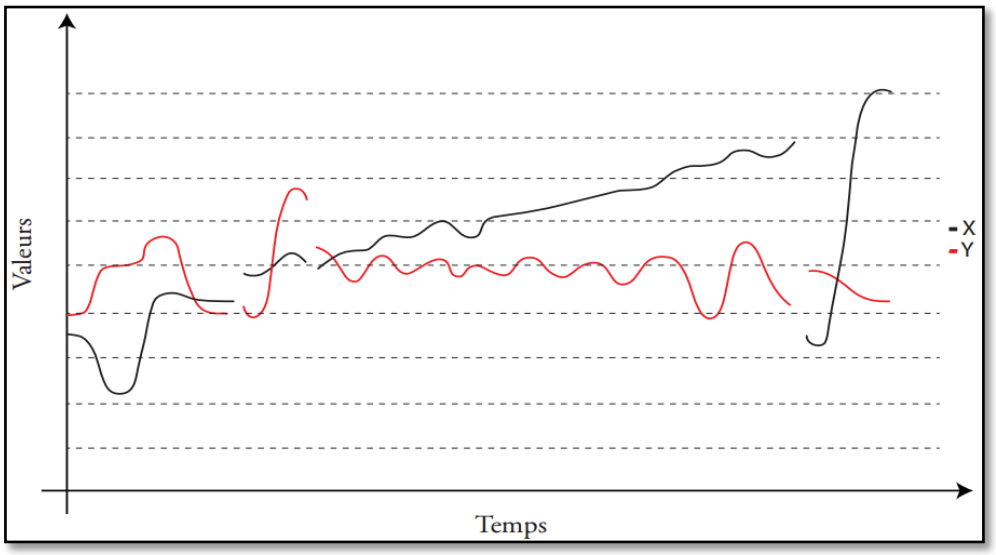


FIGURE 3.1- Les profils (x) et (y) d'une signature en fonction du temps

Les données de signature, peuvent être utilisées après traitement pour calculer les dérivées de (x), (y). Les dérivées premières de x et y sont les vitesses $V(x)$, $V(y)$ dans les deux directions (qui peuvent être combinées pour calculer la vitesse totale) et les dérivées secondes sont les deux accélérations $A(x)$, $A(y)$.

Il est à noter qu'à chaque fois qu'une personne effectue une signature elle produit un nombre d'échantillons différents. Cette variation pose des problèmes pour la comparaison entre signatures d'un même individu.

Une signature peut être considérée comme une suite de battements. [Dima1994] définit la signature comme une suite de composantes principales délimitées par des interruptions brutales [Palm1995] [Palm1997].

Généralement, le faussaire ne peut pas signer la signature d'une autre personne d'un seul coup et avec la même dynamique (vitesse et accélération) que celle du propriétaire de la signature sans effectuer au préalable beaucoup d'exercices. En effet, la différence est souvent constatée au niveau des ***Pen-up*** qui sont généralement plus longs chez le faussaire qui s'applique pour assurer une bonne imitation [Brau1993].

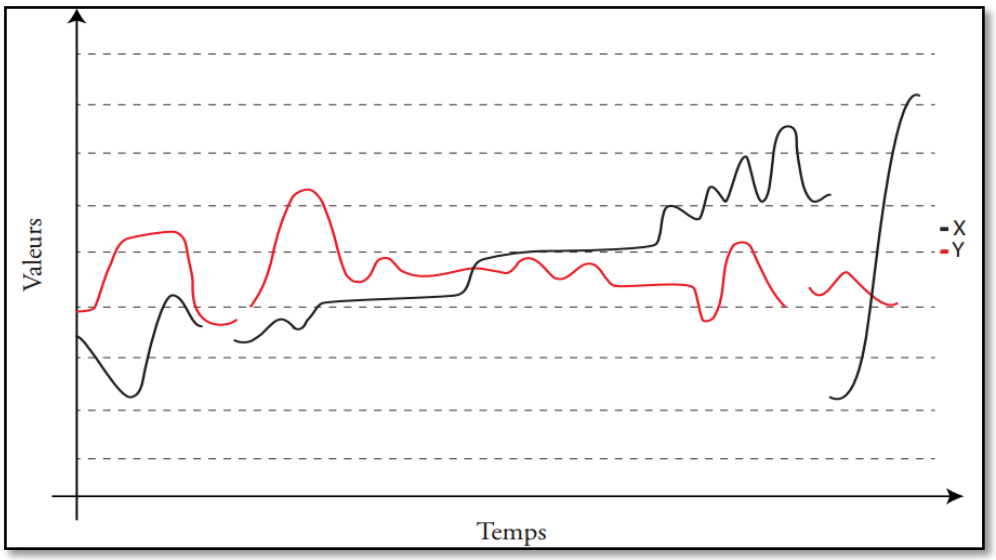


FIGURE 3.2- Les profils (x) et (y) d'une signature d'un faussaire

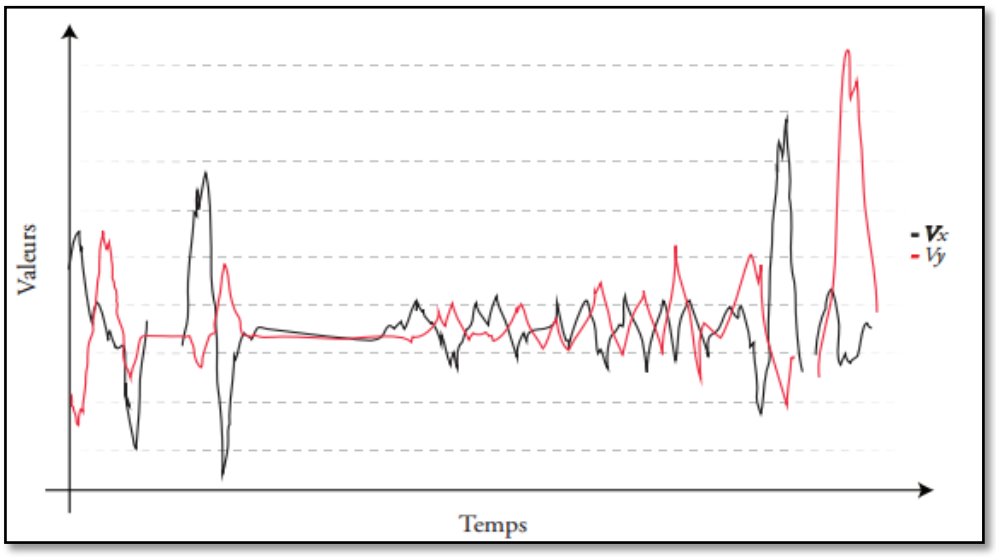


FIGURE 3.3- Vitesse en (*x*) et (*y*) d'une signature

3.3 Le processus d'authentification de la signature manuscrite

L'authentification est le processus d'analyse de la signature apposée par une personne candidate, en vue de juger son authenticité par un système de traitement. Une signature authentique est celle qui présente un taux de similarité acceptable avec son homologue enrôlée dans une base de données.

L'authentification automatique de la signature s'effectue en quatre phases (*Figure 3.4*) :

- *L'acquisition de la signature.*
- *L'extraction des descripteurs.*
- *La mesure de similarité et la classification.*

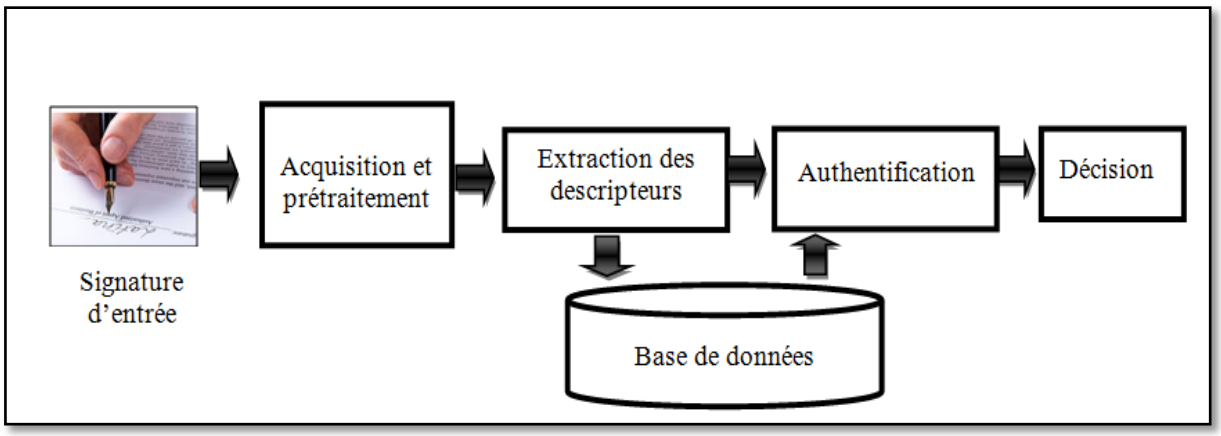


FIGURE 3.4- Le processus de l'authentification de la signature manuscrite

3.3.1 Acquisition de la signature

Cette opération est effectuée selon deux approches. L'approche statique qui permet une acquisition offline des signatures. Souvent, l'opération est faite en scannant une signature après l'avoir apposé sur un support papier, en utilisant un stylo ordinaire. Par conséquent, une image contenant l'information relative à la signature est obtenue. Pour l'approche dynamique, l'évènement de la production d'une signature est transmis comme une fonction de temps, au moyen d'un dispositif dédié. Les deux approches présentent des avantages et des inconvénients qui ont fait l'objet des études comparatives [Rigo1998].

L'approche dynamique fournit un supplément d'informations à propos de la chronologie d'évolution de la signature, alors que celle statique définit, uniquement, la forme de la signature. Bien que les signatures acquises offline soient plus stables que celles acquises online, l'éventualité de détection des imitations est très faible, à cause du faible nombre de descripteurs fournis avec l'approche statique. Les signatures onlines sont traitées comme des séquences de chiffres, quel que soit le dispositif d'acquisition, alors que les signatures offlines sont traitées comme des images. Par conséquent, l'approche dynamique se prête bien à des applications embarquées et temps réel, alors que l'approche statique fait appel à des traitements lourds et relativement coûteux. De plus, le changement du stylo ou du papier peut entraîner des erreurs de vérification des signatures offlines. Enfin, les usagers sont moins à l'aise avec les dispositifs d'acquisition online. Un temps important sera nécessaire pour adapter les habitudes des nouveaux utilisateurs avec ces dispositifs, afin d'effectuer des signatures stables.

Un exemple de dispositifs électroniques d'acquisition online est présenté dans la *Figure3.5* [Kiku2001] [Mart1997] [Mart1998].

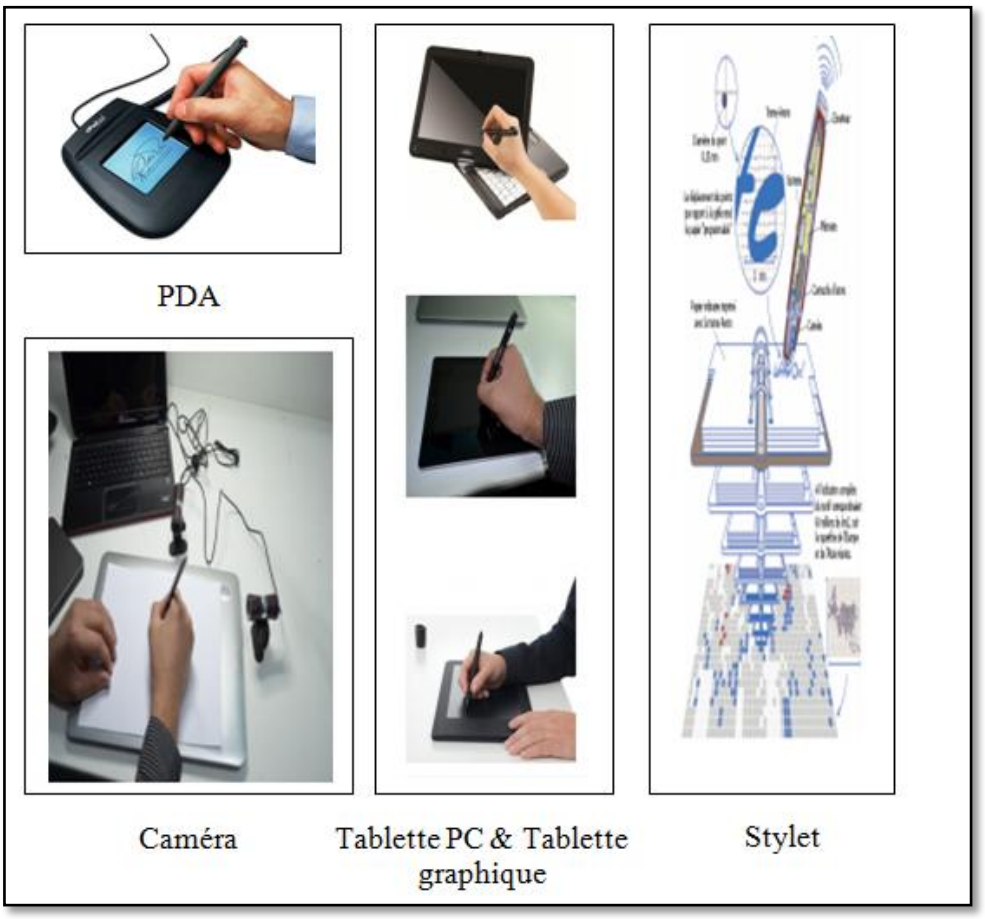


FIGURE 3.5- Dispositifs électroniques d'acquisition online

3.3.2 Extraction des descripteurs

L'extraction des descripteurs consiste à attribuer à la signature acquise une liste de paramètres discriminants qui interviennent dans la mesure de similarité. La fiabilité de vérification dépend du nombre de descripteurs et leur pertinence, et ceci, dépend fortement du dispositif d'acquisition [Gupt2009]. L'ensemble des descripteurs qui caractérisent la signature manuscrite sont divisés en deux groupes.

Le premier comprend les descripteurs globaux qui décrivent les propriétés de la signature dans sa globalité (la durée totale de la signature, le nombre de composantes, l'orientation globale, etc.).

Le deuxième groupe comprend les descripteurs locaux qui sont les propriétés liées à une position précise dans la signature (la vélocité et l'accélération instantanées, courbure locale, etc.).

L'extraction des descripteurs peut être précédée par une phase préliminaire de traitement qui vise à améliorer la lisibilité des données reçues et corriger quelques erreurs liées à l'acquisition. Les algorithmes standards de prétraitement sont utilisés, à cet effet.

3.3.3 Mesure de similarité et classification

Le test de l'authenticité d'une signature sujet est évalué par la mise en correspondance de ses descripteurs avec ceux de la signature apparentée stockée dans une base de données. Cette dernière est développée durant le processus d'enrôlement. Une ou plusieurs techniques sont utilisées pour mesurer la vraisemblance entre chaque couple de descripteurs. Une variété de techniques a été décrite dans la littérature. Selon la nature de chacune de ces techniques, trois types peuvent être distingués [Plam2000].

Les techniques statistiques qui consistent à mesurer la distance entre les couples de descripteurs. Les réseaux de neurones et les ***HMM*** (***H****idden* ***M****arkov* ***M****odel*) sont les exemples les plus courants de ce type de techniques [Fuen2002].

Les techniques de mise en correspondance (***Template Matching***) qui visent à comparer le motif d'évolution d'une signature dans le temps, avec celui d'une signature de référence dans la base. Parmi les techniques de mise en correspondance, nous avons la technique ***DTW*** (***D****ynamic* ***T****ime* ***W****arping*) qui s'adapte bien à la non-linéarité des différentes versions d'une même signature [Lesz2006].

Les techniques structurelles comparent les structures de deux signatures décrites par leurs primitives et représentées par des graphes ou des arbres de données [Chen2002].

À l'issue de la phase de mesure de la similarité, une décision binaire concernant l'authenticité de la signature à vérifier est effectuée. Toutefois, la définition d'un seuil de décision optimal reste le défi d'actualité pour l'ensemble des méthodes existantes [Aliz2010].

3.3.3.1 Déformation Temporelle Dynamique (Dynamic Time Warping (DTW))

Initialement, la ***DTW*** fut développée dans les années 50 par *Bellman* pour des applications de reconnaissance de la parole [Bell1957]. Cette méthode de programmation dynamique permet de trouver l'appariement optimal entre les points de deux courbes à comparer. La mise en correspondance se base principalement sur la minimisation d'une distance entre couples

de points correspondants. Pour cela des opérations de type allongement et rétrécissement selon l'axe du temps sont effectuées.

Le principe de la méthode est illustré dans les *Figures 3.6 et 3.7*.

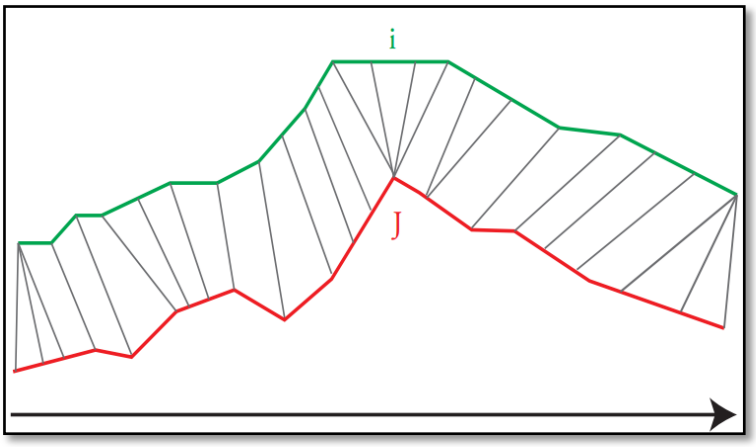


FIGURE 3.6- La correspondance point à point entre deux signatures par l'algorithme ***DTW***

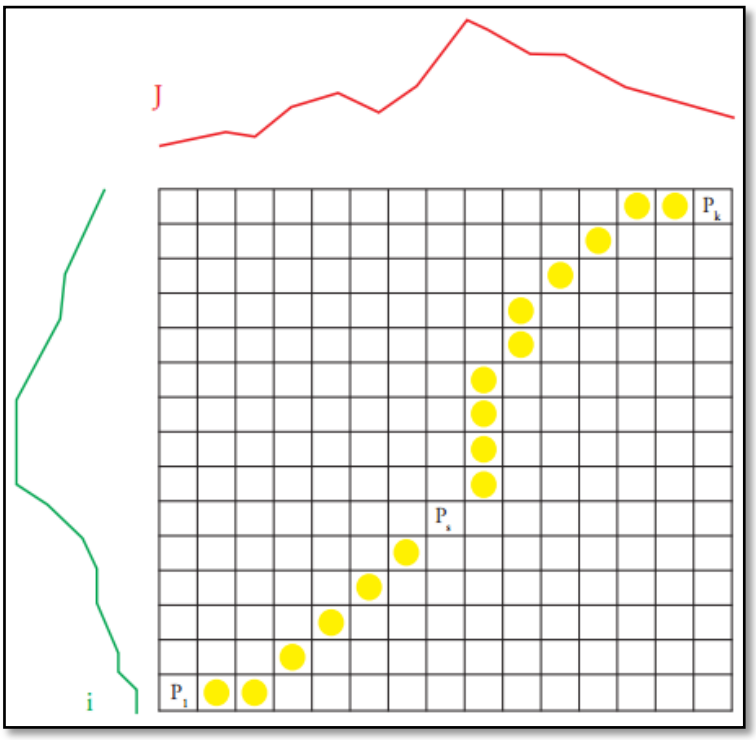


FIGURE 3.7- Exemple de chemin de déformation optimale par l'algorithme ***DTW***

Le fait de travailler en online permet d'extraire les informations $x(t)$ et $y(t)$ des signatures représentées en (x, y). Ceci rend l'utilisation de ***DTW*** possible pour l'authentification de la signature.

En effet, un grands nombre de travaux à base de la ***DTW*** a été menés [Hast1992] [Bae1995].

Cette technique est exploitée afin de calculer la similarité entre les signatures qui sont des suites qui varient en fonction du temps. Cette approche cherche à trouver la meilleure mise en correspondance (appariement) entre une signature de référence (*R*) enregistrée et une signature à tester (*T*).

Ces signatures sont représentées par les vecteurs suivants :

T: [*T*(*I*); *i* =1, 2, …..*I*]

R: [*R*(*J*); *j* =1, 2, …..*J*]

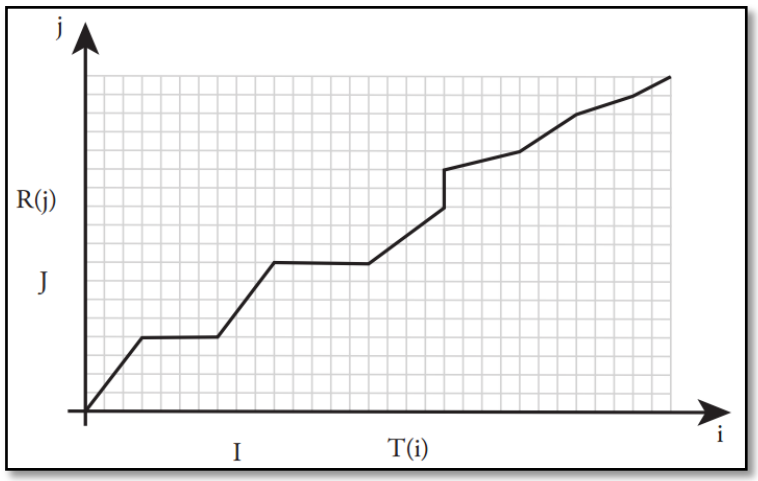


FIGURE 3.8- Alignement temporel entre *R* et *T*

Pour ces deux vecteurs on va définir une distance locale (*d*), qui représente la distance entre *T*(*i*) un vecteur de *T*, et *R*(*j*) un vecteur de *R*, ensuite on déclare la distance globale (*D*) qui représente la somme des distances locales sur lesquelles on peut ajouter une pondération. Cette distance doit être peu sensible aux distorsions temporelles.

Pour cela, on va l'évaluer le long d'un chemin optimal *w*: [$i_{(k)}$,$j_{(k)}$], *k* =1, 2, …..*K*, en respectant les contraintes suivantes :

- ✓ Coïncider les extrémités, le chemin de déformation (*w*) doit alors commencer en [*T*(0), *R*(0)] et terminer en [*T*(*I*),*R*(*J*)].
- ✓ Progresser d'une manière monotone le long du chemin, $w_{k-1} < w_{k..}$
- ✓ Respecter la continuité du chemin.

À cela il faut ajouter les contraintes dites locales [Sako1978] tel que:

Contraintes du type A :

$$\partial(i,j) = d(i,j) + \min[\partial(i-1,j), \partial(i-1,j-1), (i-1,j-1)]$$

Contraintes du type B :

$$\partial(i,j) = d(i,j) + \min\begin{Bmatrix} \partial(i-2,j-1) + 2 * d(i-1,j) \\ \partial(i-1,j-1) + d(i,j) \\ \partial(i-1,j-2) + 2 * (i,j-1) \end{Bmatrix}$$

Contraintes du type C :

$$\partial(i,j) = \mathrm{d}(i,j) + \min\begin{Bmatrix} \partial(i-1,j) \\ \partial(i-1,j-1) + \mathrm{d}(i,j) \\ \partial(i,j-1) \end{Bmatrix}$$

Où *d*(*i*,*j*) la distance locale, et (*D*) la distance globale, ou l'accumulation des distances locales.

Le calcul de la distance minimale entre la signature de référence (*R*) et la signature inconnu (*T*) est comme suit :

$$\partial(T,R) = \frac{d(i,j)}{N(g)}$$

Où $N(g)$ est un facteur de normalisation, qui pour les contraintes de type (**B**) ou (**C**), vaut *I*+*J*.

Dans cette thèse, nous avons utilisé la contrainte du type (**A**) pour réaliser nos expériences.

En premier lieu on applique la ***DTW*** entre signatures en vue de l'extraction du degré de leur similitude. Il faut bien noter que le descripteur pris est le profile *x* de chaque signature. [Jaya2009].

Pour distinguer entre ces dernières, le profil de la signature de référence est présenté en bleu et celui de la signature de test en rouge (*Figure 3.9*).

L'exemple suivant montre la mise en correspondance entre ces deux signatures identiques ainsi que leur schéma de déformation (*w*) en vert qui est presque droit (*Figure 3.9 (b)*), (*Figure 3.10*).

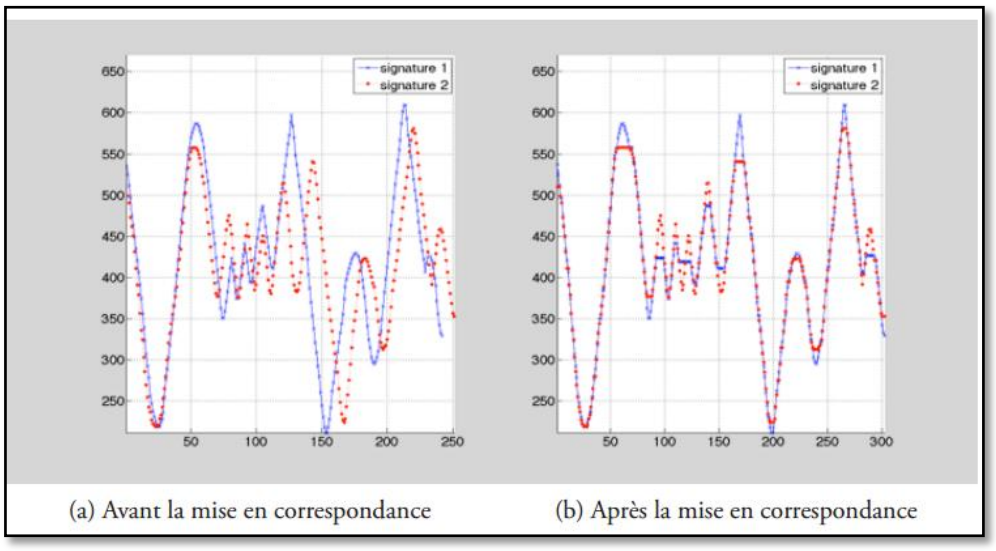


FIGURE 3.9- Exemple de mise en correspondance de deux signatures très proches

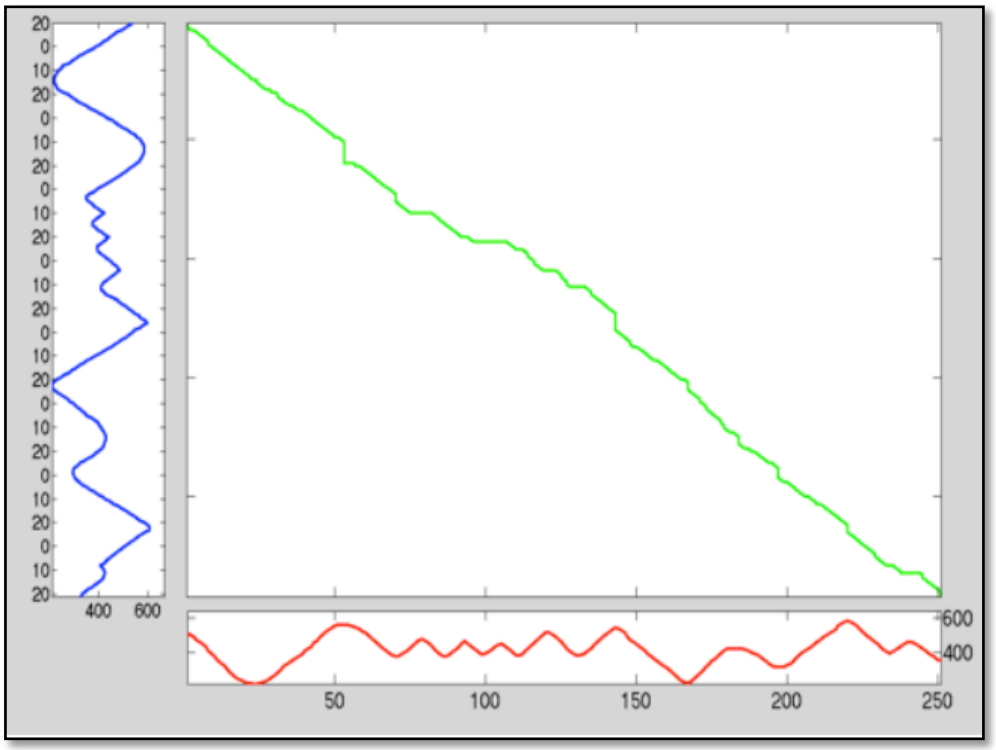


FIGURE 3.10- Schéma de déformation correspondant

Un deuxième exemple de mise en correspondance entre deux signatures différentes (signature de référence avec un faux aléatoire) est présenté en (*Figure 3.11)*.Comme on peut le constater en (*Figure 3.12)*, le schéma de déformation correspondant est une ligne qui n'est pas droite ce qui décrit bien le degré de non-similarité entre ces deux signatures.

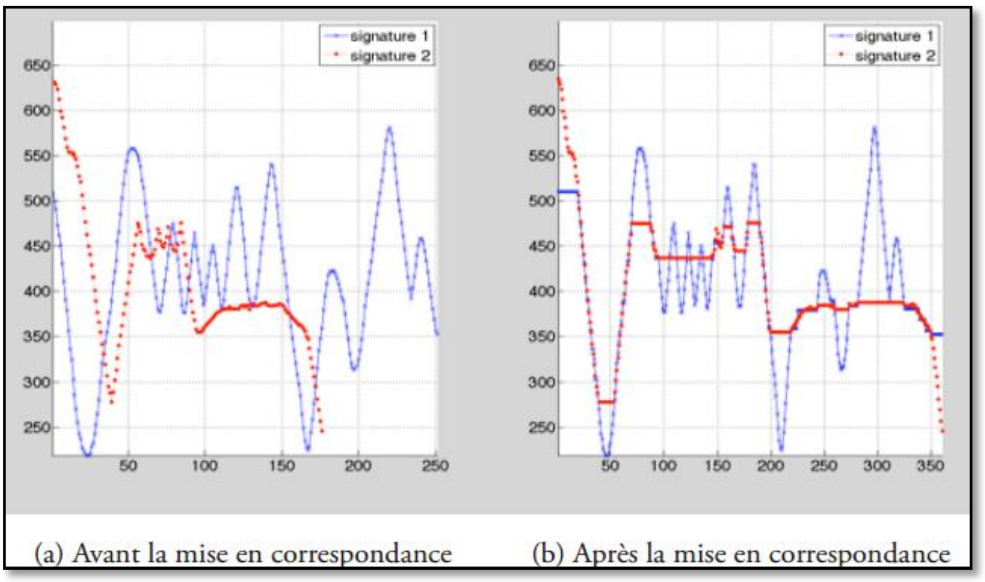


FIGURE 3.11- Exemple de mise en correspondance de deux signatures différentes

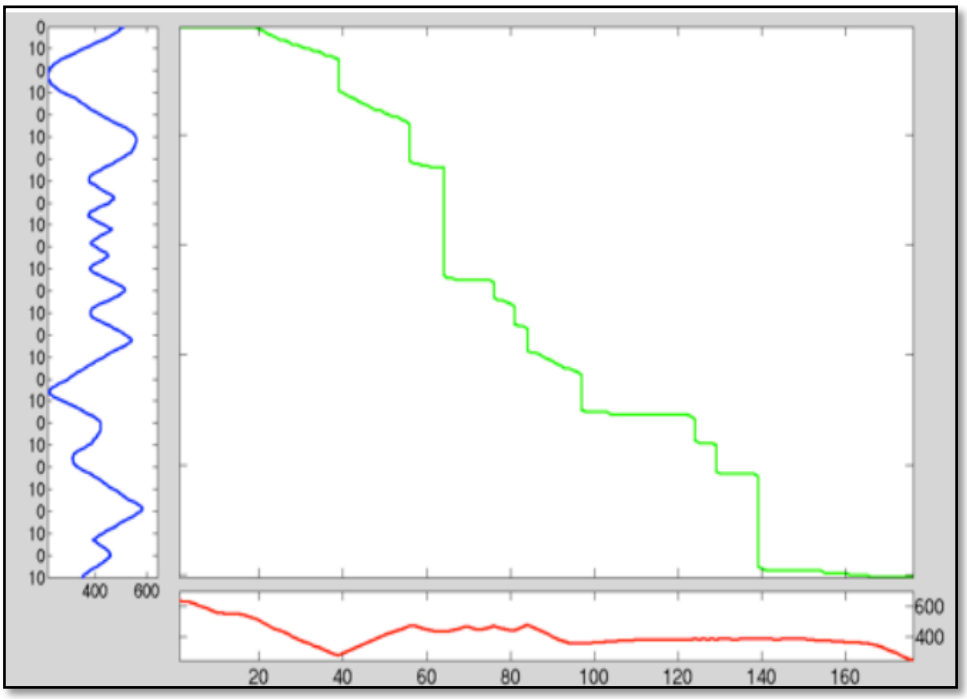


FIGURE 3.12- Schéma de déformation correspondant

Bien qu'elle soit performante, la ***DTW*** présente un inconvénient majeur, est celui de sa gourmandise, en calculs récursifs, ce qui la rend inadaptée pour des applications où les contraintes de temps de réponse sont strictes [Fren2003].

3.3.3.2 Distance de Hausdorff

La distance de Hausdorff est fortement utilisée dans des applications de localisation et d'identification faciale [Jeso2001] [Kirc2002]. Le principe de cette dernière est comme suit :

Soit les deux ensembles de points $A = \{a_1, a_2, \ldots., a_m\}$, $B = \{b_1, b_2, \ldots., b_n\}$. La distance de Hausdorff entre Aet B est égale à :

$$HD(A,B) = HD(B,A) = \max\big(hd(A,B), hd(B,A)\big)$$

Avec

$$hd(A,B) = max_{a\in A} min_{b\in B} ||a-b||$$

En pratique on utilise la métrique de Hausdorff modifiée qui est plus robuste au bruit que l'originale. La formulation de cette dernière est :

$$MHD(A,B) = MHD(B,A) = \max(mhd(A,B), mhd(B,A))$$

Avec

$$mhd(A,B) = \frac{1}{N}\sum_{a\in A} min_{b\in A}\, ||a-b||$$

L'authentification d'une signature est effectuée en calculant en premier sa distance par rapport à la signature de référence. La valeur obtenue est ensuite comparée à un seuil fixé (*S*). Si la distance est inférieure à (*S*), la signature est considérée comme une imitation, sinon elle est déclarée comme étant signature authentique.

Un exemple de résultats de calcul de la distance de Hausdorff entre une signature de test et dix signatures de référence (Réf) est présenté dans la (*Figure 3.13)*.

Seule la signature du propriétaire de la signature est proche de la signature de référence. Sa distance est la plus petite valeur.

FIGURE 3.13- Distance de Hausdorff entre les signatures

3.4 Techniques d'acquisition des signatures online

Les techniques d'acquisition online sont apparues à la suite du besoin d'automatiser la vérification des signatures manuscrites, Un exemple de ces dispositifs est présenté dans la (*Figure3.5*). Comme la technique d'acquisition influence énormément la qualité de vérification, les progrès dans ce contexte ne cessent de se poursuivre. Une technique efficace est celle qui permet de mieux caractériser la signature. Autrement dit, celle qui permet de sonder les informations les plus discriminantes dissimulées dans la signature, et qui donne lieu à l'extraction d'un maximum des descripteurs pertinents [Gupt2006].

Les techniques basées sur les périphériques de pointage (les tablettes, PDA, les pavés tactiles, etc.) sont traditionnellement utilisées pour traduire la trajectoire d'une signature en une séquence de points [Hamm1995]. Des améliorations ont été apportées sur ces techniques afin de les rendre plus ergonomiques, ce qui permet aux utilisateurs de signer d'une façon plus naturelle [Shim2004]. Une variante de ces techniques consiste à effectuer la signature sur un papier superposé sur une tablette, au moyen d'un stylo à encre. Ce dernier produit, entre temps, une réplique sur la tablette, en vue de bénéficier des avantages de l'acquisition online et offline, simultanément. Des fonctionnalités ont été ajoutées, dont on peut citer la détection de la variation de pression et inclinaison du stylet utilisé. L'exploitation d'une souris connectée à un PC pour la signature a aussi fait l'objet de plusieurs études, du fait qu'elle représente un périphérique standard et répandue [Lei2005].

La plupart des outils évoqués jusqu'à présent visent un usage grand public. Pour une application donnée, telle que le gestionnaire de formulaires électroniques sur le réseau, plusieurs outils peuvent être utilisés, en même temps, pour l'apposition des signatures. Le problème

d'interopérabilité sera posé dans ce cas, tant qu'il y a un système unique de vérification automatique des signatures au niveau de l'ordinateur central. Ce dernier n'est pas en mesure d'adapter les données reçues à partir de différentes sources [Alon2005]. À ce point, l'avantage avec les approches offline est que les signatures acquises sont les même pour une telle personne, quelles que soient les outils ou les conditions d'acquisition.

L'acquisition dynamique des signatures effectuées sur le papier était une solution attractive pour autant d'auteurs. *Nabeshima et al.* développent un stylet muni d'une caméra qui suit son parcours pendant la signature et enregistre par des snapshots le trait d'encre sur le papier. Un capteur de pression permet de contrôler la caméra, en cas de pose et de levé du stylet [Nabe1995]. *Munich et Perona* proposent l'utilisation d'une caméra standard et fixe pour filmer tout l'environnement de signature. Dans ce cas, le trait produit par un stylo ordinaire sur le papier est récupéré à partir de la représentation spatiotemporelle de la signature fournie de la séquence vidéo [Muni2003]. En partant de l'approche de *Munich et Perona*, des chercheurs exploitent la vision pour récupérer d'autres informations liées à l'acte de signature. Dans [Chen2012], Cheng et al. ajoutent une caméra latérale pour enregistrer la posture d'empoignement du stylo. Cette information très discriminante a amené à de bons résultats de reconnaissance. Dans [Tolb1999], les gants numériques (*Data-Gloves*) utilisés en réalité virtuelle ont été exploités pour l'acquisition dynamique et à plusieurs degrés de liberté des informations relatives au comportement de la main ainsi qu'au mouvement du stylo, pendant l'opération de signature.

3.5 Nouveau système d'acquisition online de signatures

Dans le cadre du projet conduit par l'équipe de traitement de l'information du laboratoire MSE, et qui vise à développer un système d'identification biométrique multimodale, un travail publié antérieurement a porté sur le développement d'un système d'acquisition online des signatures manuscrites, en vue de renforcer l'efficacité du système global par le rajout d'une nouvelle modalité [Oule2013].

Comme le représente la *Figure 3.14*, ce système est composé d'une caméra de haute résolution placée horizontalement devant une fenêtre vitrée transparente, sur laquelle la signature est effectuée.

Le signataire procède, à l'aide d'un cône blanc ayant un point coloré, à l'opération de signature en déplaçant le doigt, sur lequel le capuchon est mis, sur la surface de la vitre placée

verticalement. Les mouvements filmés par la caméra sont utilisés pour la génération des caractéristiques de la signature correspondante ($x(t)$, $y(t)$, (x,y)). Cette méthode capte la trajectoire du doigt, y compris les intervalles où le doigt est hors contact avec la vitre. Cette information supplémentaire, enfouie dans la signature acquise, représente un comportement dynamique et invisible, spécifique au signataire.

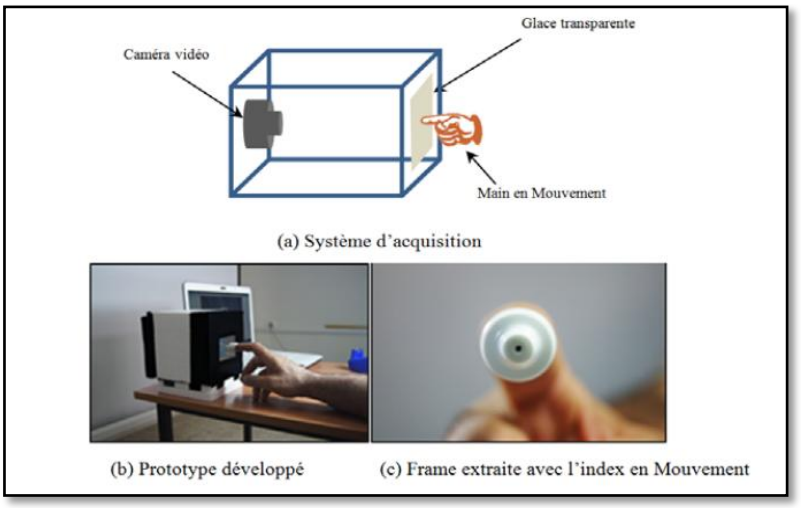


FIGURE 3.14- Le Système développé

Des améliorations apportées sur le dispositif discuté ci dessus, et qui visent essentiellement à le rendre plus facile à exploiter. Par conséquent l'apposition de la signature sera faite d'une façon plus naturelle et quasiment identique à l'approche classique (la signature sur un papier).

Les signatures reconstruites reproduisent fidèlement le mouvement de la main. Toutefois, elles se présentent un peu différemment de leurs homologues offlines, ceci s'explique par le fait que le public n'est pas assez familiarisé avec les méthodes d'acquisition onlines, notamment avec nôtre nouvelle approche. De plus, la position du verre n'est pas bien adaptée pour permettre aux signataires d'effectuer naturellement cette opération. Des modifications stratégiques ont été apportées sur le prototype précèdent, dans le but de rendre l'opération de signature plus précise et plus proche de la démarche classique (*Figure 3.15*). À savoir :

- ✓ La plaque de verre est disposée horizontalement, ce qui fait que l'objectif de la caméra devient dirigé vers le haut perpendiculairement à la plaque de signature.
- ✓ Le stylet à utiliser est muni d'un bout, ayant une forme et une couleur bien définie.

✓ Afin d'ajuster les conditions d'éclairage, la vitre est protégée par un couvercle opaque.

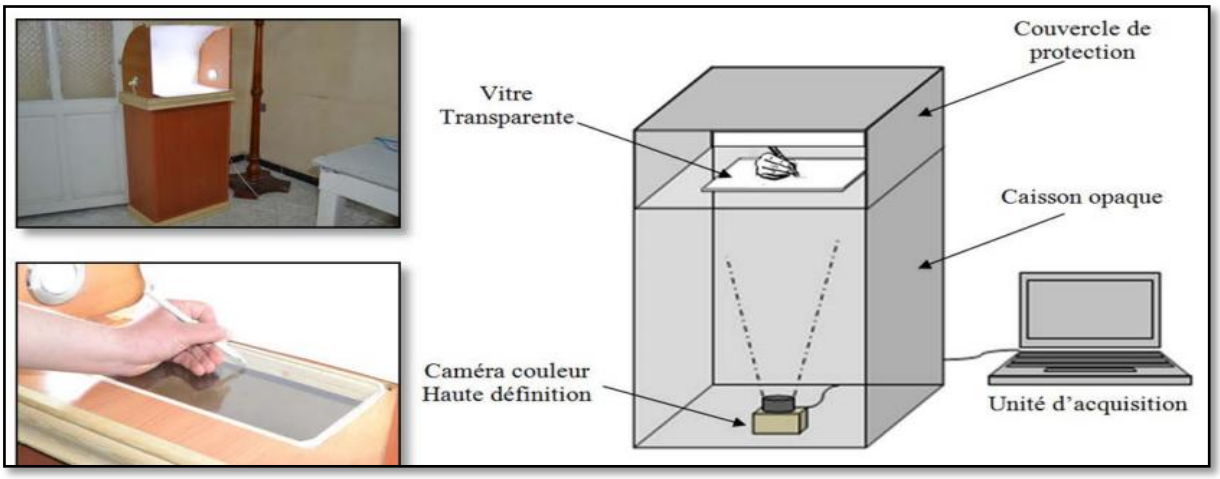


FIGURE 3.15- Le Système amélioré

3.6 Procédé d'acquisition online d'une signature

Toute personne qui désire se faire identifier doit placer son index (stylo dans le système amélioré) sur la glace et effectuer sa signature comme si elle le faisait sur papier.

Le mouvement effectué par la main est alors enregistré par la caméra. La séquence vidéo acquise (*Figure 3.16(a), (b)*) est ensuite décomposée en frames afin d'extraire les caractéristiques requises par les systèmes d'authentification à savoir : les variations $x(t)$, $y(t)$ avec leurs vélocités correspondantes ainsi que les coordonnées (x,y) des positions successives de l'index (stylo dans le système amélioré)

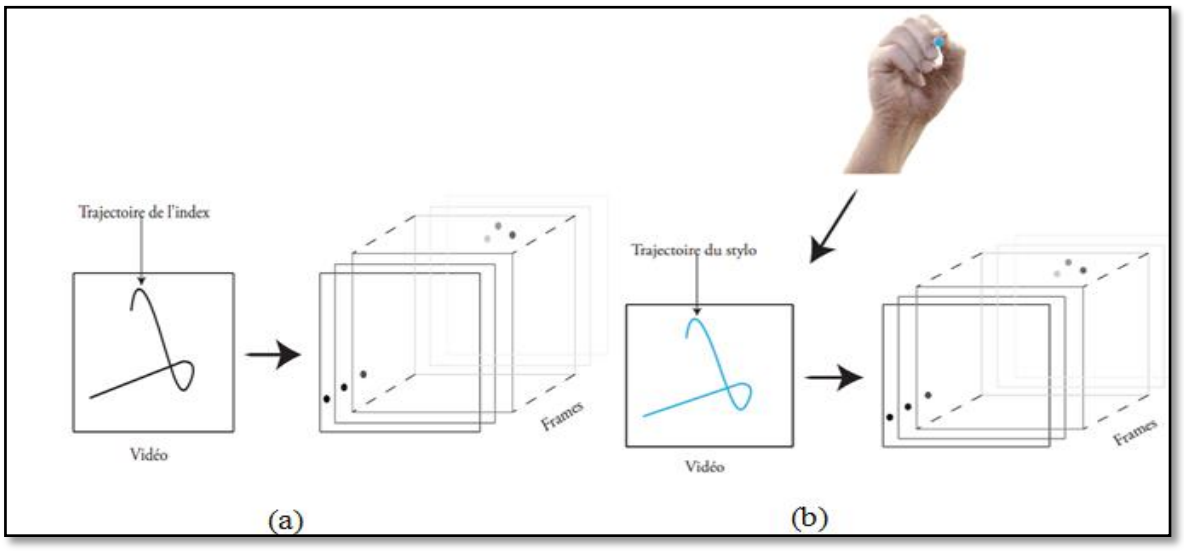
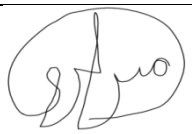
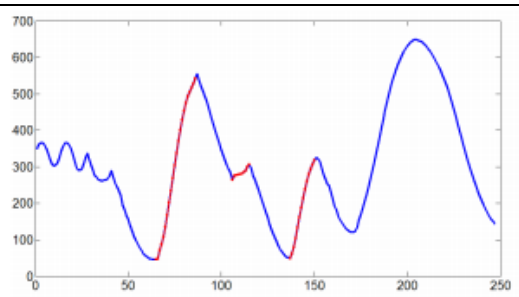
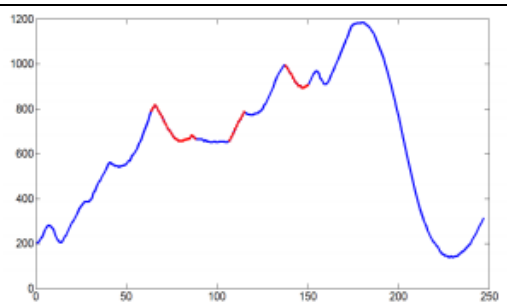
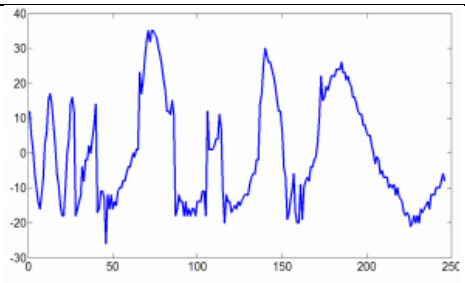
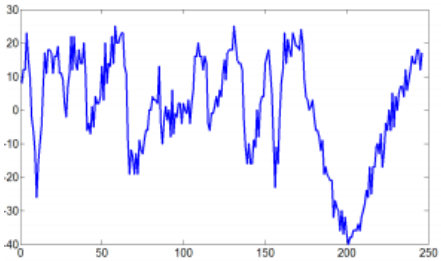
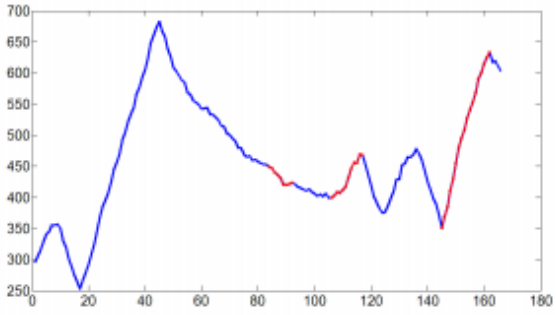
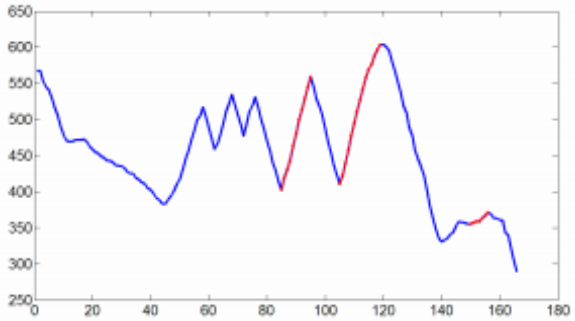
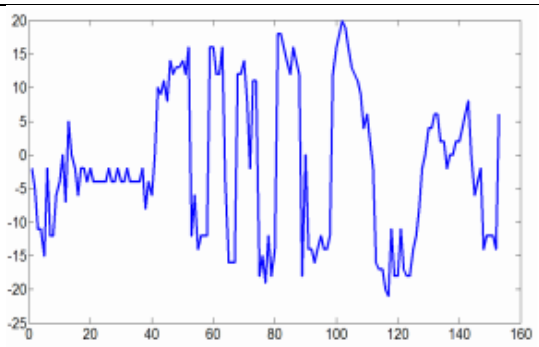
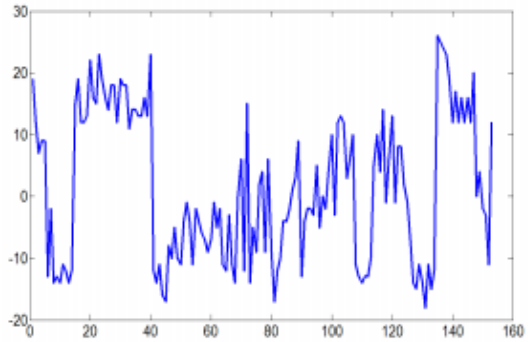


FIGURE 3.16- Décomposition de la vidéo en frames et : (a) extraction des positions de l'index, (b) extraction des positions du stylo

Le *Tableau 3.1* présente quelques résultats de signatures obtenues en online, pour chaque signature sont associées les courbes de variations dans le temps $x(t)$, $y(t)$ ainsi que leurs vélocités $V_x(t)$ et $V_y(t)$ respectives. Comme on peut le constater, les signatures reconstruites (par le système amélioré) sont maintenant très proches des signatures obtenues en offline.

Tableau 3. 1- Exemples des signatures offline et online avec leurs caractéristiques dynamiques

Signature offline	Signature online
(x,y)	(x,y)
	
Les caractéristiques dynamiques de la signature online	
$x(t)$	$y(t)$
	

$V_x(t)$	$V_y(t)$
	
Signature offline	Signature online
(x,y)	(x,y)
	
Les caractéristiques dynamiques de la signature online	
$x(t)$	$y(t)$
	
$V_x(t)$	$V_y(t)$
	

3.7 Discussion

Dans ce chapitre nous avons présenté l'authentification par la modalité signature. Dans un premier temps nous avons présenté un état de l'art sur les techniques développées pour l'acquisition, le traitement et l'authentification de la signature. Par la suite, nous avons abordé le système d'acquisition online développé.

Dans le chapitre suivant, nous allons présenter le système d'acquisition développé et les limites de la méthode d'authentification (DTW) contre les contrefaçons qualifiées, également nous illustrerons l'importance d'inclure le descripteur forme de la main pour surmonter ces limitations et pour améliorer la précision de l'authentification.

Chapitre 4

Approche Efficiente d'authentification de Signature en ligne

Chapitre 4

Approche Efficiente d'authentification de Signature en ligne

Dans ce chapitre, nous présentons le système d'acquisition développé et les limites de la méthode d'authentification (DTW) contre les contrefaçons qualifiées, également nous illustrons l'importance d'inclure le descripteur forme de la main pour surmonter ces limitations et pour améliorer la précision de l'authentification. A la fin de ce chapitre nous montrons l'évaluation des performances de l'approche proposée avec des expérimentations approfondies. L'approche proposée a permis d'obtenir le meilleur compromis entre l'efficacité (EER=2) et la simplicité (utilisation d'un seul capteur pour l'acquisition).

Sommaire

4.1 Introduction **59**

4.2 Système d'acquisition **60**

4.3 Authentification de la signature **62**

4.3.1 Construction de la base de données 62

4.3.2 Tests préliminaires d'authentification 62

4.3.3 Constat général 64

4.4 Amélioration de la précision de l'authentification **64**

4.4.1 Forme de la main au moment de la signature 64

4.4.2 Extraction du descripteur forme de la main 68

4.4.3 Fusion au niveau des scores 74

4.4.4 Avantages du descripteur de la forme de la main proposé 76

4.4.4.1 Détection des changements d'habitudes du signataire 76

4.4.4.2 Détection des efficiente des contrefaçons 77

4.4.5 Calcul de complexité 79

4.5 Comparaison de l'approche proposée avec d'autres techniques avancées **80**

4.6 Discussion et conclusion **81**

4.1 Introduction

Les contrefaçons qualifiées posent un réel problème à la majorité des systèmes d'authentification de signature existants. Ceci limite l'utilisation de cette modalité dans le cas d'applications avec des exigences de haut niveau de sécurité (militaires, banques et les domaines sensibles, et ainsi de suite). En dépit de cela, cette modalité non-contraignante reste très utilisée par un grand nombre de systèmes d'authentification biométriques multimodaux [Impe2008] [Jain2002].

Plusieurs travaux basés conjointement sur la signature et sur une autre modalité ont été proposés pour la construction de systèmes efficaces d'authentification bimodale (la signature la parole, la signature et le visage, la signature et l'iris, etc.).

[Humm et al 2006] ont développé un système d'authentification bimodale utilisant les deux modalités de signature et de la parole. L'approche proposée est basée sur deux scénarios : dans le premier, une signature bimodale et des informations vocales sont acquises. Il a été demandé à l'utilisateur de parler du contenu de sa signature. Toutefois, dans le second scénario, Il a été demandé à l'utilisateur d'écrire et de lire de manière synchrone le contenu d'un texte donné.

Dans une autre étude, [Elmi et al 2012] ont combiné la signature et les modalités du visage. Le système proposé est basé sur la fusion au niveau des traits du visage et la signature d'un utilisateur. Les marques utilisées ont été obtenues à partir de deux systèmes de vérification ; le premier système était basé sur la vérification du visage en utilisant une combinaison de filtre de Gabor pour l'extraction de caractéristiques et la machine à vecteur pour la classification. Le second système était basé sur la vérification de signature en ligne, en utilisant la méthode Nalwa [Nalw1997]. Plusieurs stratégies ont été utilisées pour fusionner les marques de visage et de signature en ligne tels que simple somme, minimum et marques maximales.

[Alma et al 2011] ont présenté un système d'authentification biométrique multimodale fondé sur un nouveau système caractéristique du niveau de fusion de la signature et les fonctionnalités de l'iris. Les dernières ont été extraites séparément et concaténées pour former un vecteur caractéristique fusionné. Une approche d'optimisation par des nuages de particules binaire a été utilisée pour réduire la dimension du vecteur de caractéristiques tout en gardant le même niveau de performance.

Bien que ces combinaisons renforcent la sécurité et la précision, la complexité des méthodes proposées augmente avec l'augmentation du nombre de caractéristiques extraites et le nombre de capteurs utilisés.

4.2 Système d'acquisition

Un prototype de laboratoire MSE [Oule2013] a été mis au point à cet effet (*Figure 4.1*). Il est composé d'une caméra à haute résolution placée en face d'un verre de signature transparent. Les signataires effectuent leurs signatures en déplaçant leurs stylos sur la vitre. Les mouvements acquis sont utilisés pour générer les caractéristiques de signature correspondant [x(t), y(t), (x,y)].

Pour réduire les effets des variations d'éclairage, le plan de signature est protégé par un couvercle opaque. Des exemples de trames successives acquises au cours d'un processus de signature sont présentés en *Figure 4.2*.

La *Figure 4.3* représente certaines signatures reconstruites obtenues avec notre système d'acquisition. Dans le cas de signatures continues, hors ligne [*Figures 4.3 (a)* et *4.3 (e)*] et en ligne [*Figures 4.3 (b) et 4.3 (f)*] les signatures sont identiques.

Cependant, tout *pen-up* en mode hors ligne [*Figures 4.3 (c)* et *4.3 (g)*] sera considéré comme une courbe continue en mode en ligne [*Figures 4.3 (d)* et *4.3 (h)*].

Cette information dynamique complémentaire permettra une analyse précise de la signature et rendra difficile toute tentative d'imitation intentionnelle.

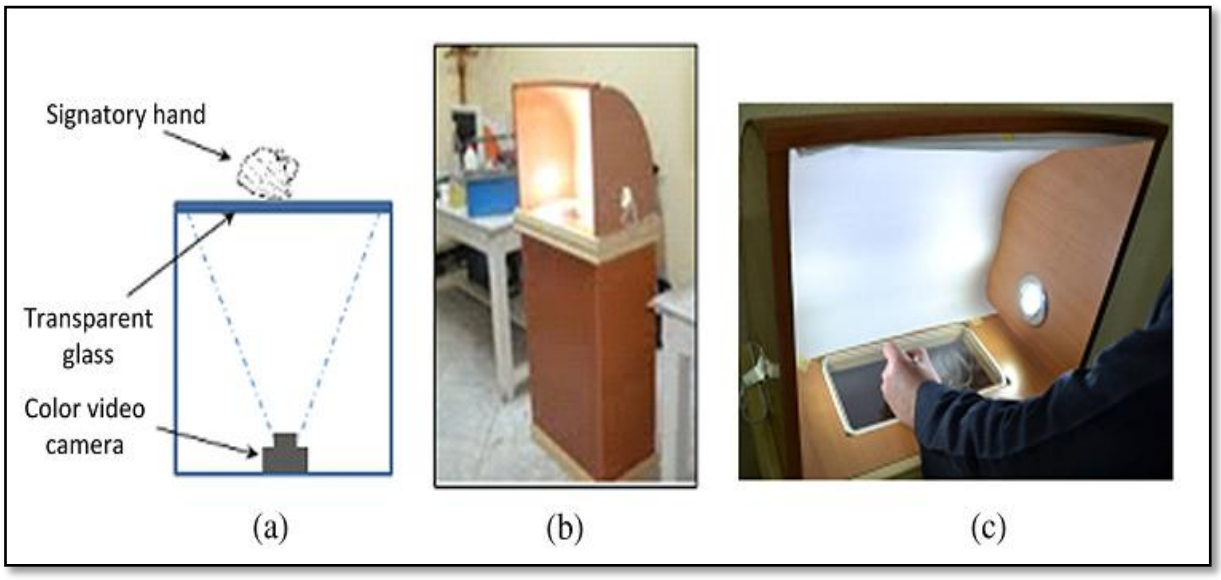


FIGURE 4.1- Système d'acquisition de signature en ligne utilisé : (a) vue globale, (b) prototype de laboratoire MSE, et (c) vue de l'opération de signature

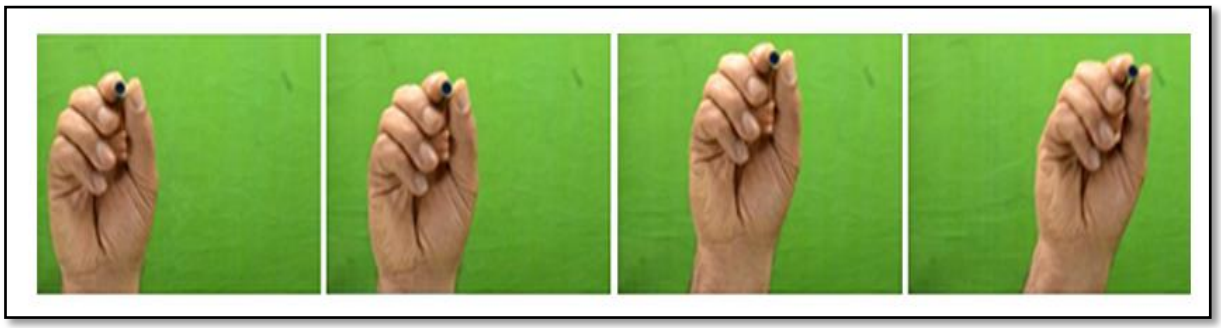


FIGURE 4.2 - Trames successives obtenus pendant un processus de signature

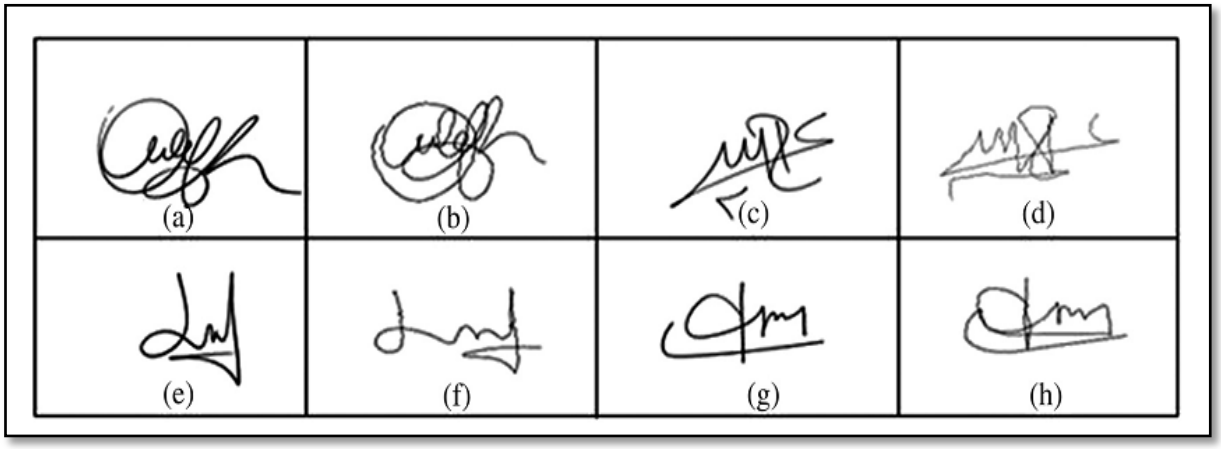


FIGURE 4.3 - Comparaison entre signatures hors ligne [(a), (c), (e), (g)] et en ligne [(b), (d), (f), (h)].

4.3 Authentification de la Signature

Une large série de techniques ont été développées pour effectuer les taches d'authentification de signature en ligne ou hors ligne [Gupt2006]. Toutes cherchent à trouver les meilleures caractéristiques représentatives, en vue d'effectuer une mesure de similarité efficace entre signatures d'inscription et celles des essais. Pour une première approche, la méthode *DTW* [Zogh2009] bien connu a été utilisée pour effectuer une tâche d'authentification de signature. L'objectif n'est pas d'évaluer ses performances dans les cas ordinaires, mais plutôt de montrer ses limites dans le cas de contrefaçons qualifiées.

4.3.1 Construction de la base de données Test

La base de données de test comporte les signatures de 100 participants : 60 hommes et 40 femmes. Il a été demandé à chaque participant d'effectuer 10 signatures authentiques, 3 pour la génération de la signature de référence et 7 pour les tests. Après un temps d'entrainement, chaque contributeur a produit ou effectué cinq contrefaçons de signatures aléatoires et 5 vraies signatures.

Un total de 700 signatures authentiques avec 500 contrefaçons aléatoires et 500 contrefaçons qualifiées ont été collectées à des fins de test d'authentification. Les formes de la main des utilisateurs ont également été enregistrées au début du processus de signature. Il existe trois acquisitions pour la génération de la main de référence 7 pour les essais et qui ont été appariés avec des données de signature pour les essais.

4.3.2 Tests préliminaires d'authentification

La performance d'authentification est généralement évaluée en dessinant la courbe (*ROC*) ainsi que les évolutions du taux de fausses acceptations (*FAR*) et le taux de faux rejets (*FRR*) à différentes valeurs de seuil.

Les résultats d'authentifications obtenus nous ont permis d'établir la courbe *ROC* et les courbes du *FRR-FAR* comme on peut le voir sur les *Figures 4* et *5* et le *Tableau 1*. On peut voir que la *DTW* donne des résultats acceptables dans le cas des signatures authentiques. Toutefois, l'inclusion de contrefaçons diminue considérablement la précision d'authentification.

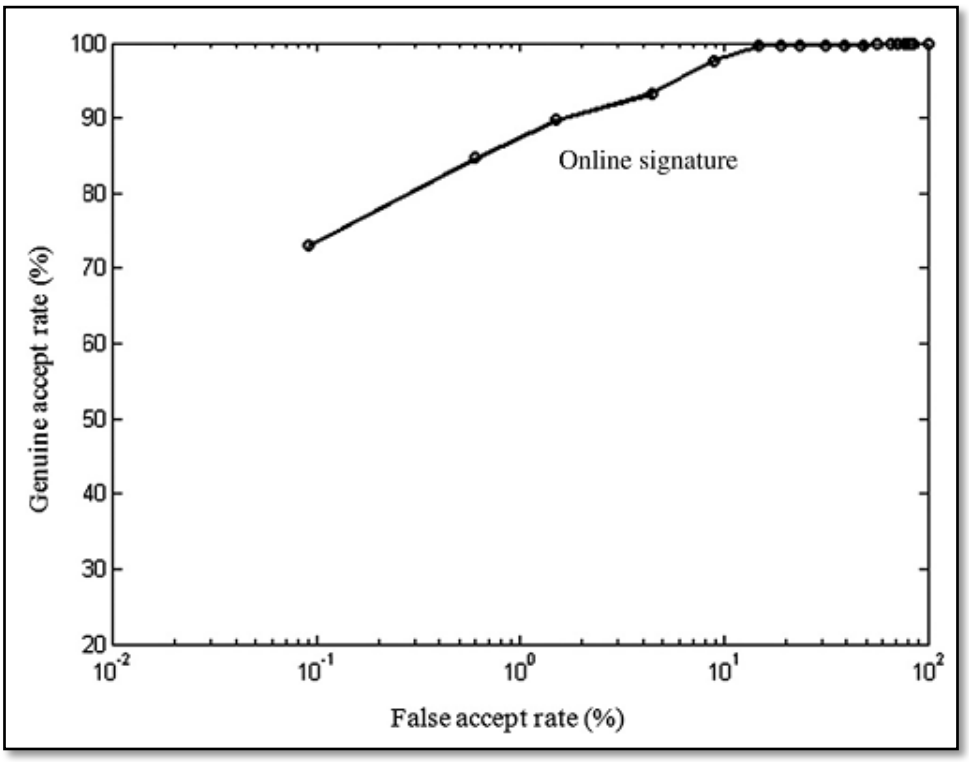


FIGURE 4.4 – Courbe *ROC* montrant la performance de la modalité signature en ligne

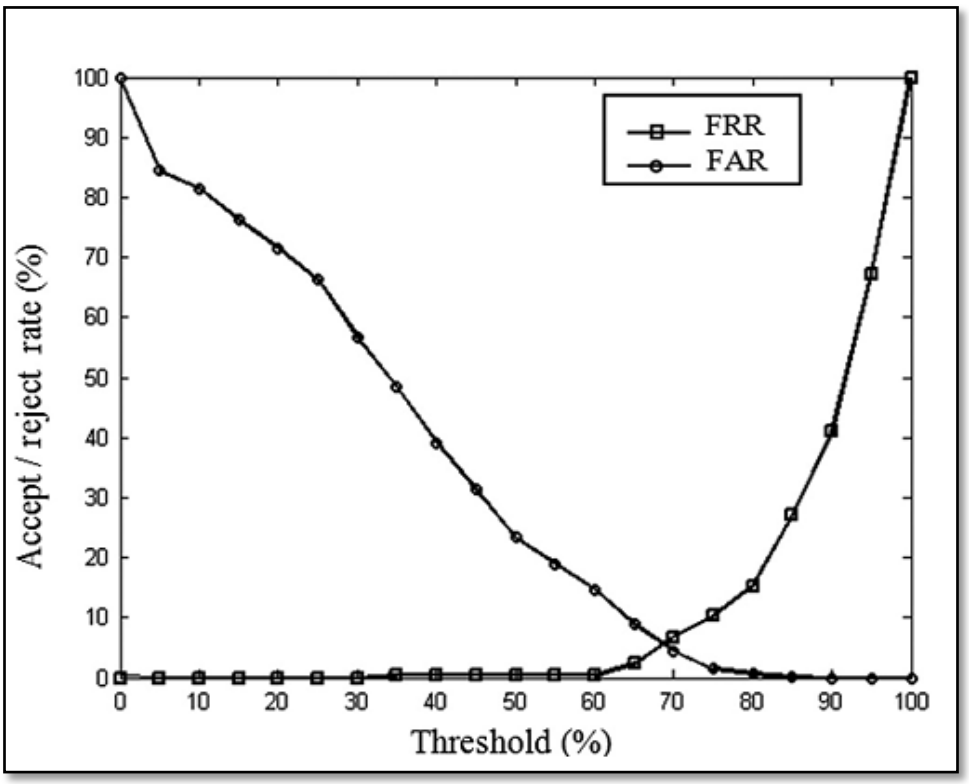


FIGURE 4.5 - Taux de faux Rejet et acceptation par rapport au seuil de la modalité signature en ligne

Tableau 4.1- Résultats des tests d'authentification pour la modalité signature

Seuil	Véritable taux d'acceptation GAR (%)	Taux de fausses acceptations FAR(%)
33	100	56.8
40	99.6	39.1
55	99.6	18.9
65	97.7	8.9
80	84.7	0.6
85	73	0.09
88	58.9	0.00

4.3.3 Constat général

Habituellement, les systèmes d'authentification concentrent leur traitement sur les caractéristiques dynamiques et/ou statiques des signatures acquises. Cette approche donne des résultats satisfaisants dans les cas ordinaires, mais reste vulnérable contre les contrefaçons qualifiées. Cela est dû au fait qu'il n'y a pas de relation entre le signataire et sa signature. Dans ce qui suit, nous allons montrer que l'inclusion de la forme de la main dans le processus d'authentification permet de réduire considérablement les contrefaçons qualifiés *FARs* et d'améliorer les performances d'authentification de signature.

4.4 Amélioration de la Précision de l'Authentification

4.4.1 Forme de la main au moment de la signature

Plusieurs travaux intéressants [Mill1971], [Erns1971], [Jaco1972] ,[Jain1999], [Reil2000], [Wong2002], [Oden2003], [Goh2003], [Kuma2003], [Han2004], [Pave2004], [Cova2005], [Yoru2006], [Varc2007], [Migu2007], [Migu2008], [Baha2010], [Rong2012] , [Jing2012], [Rafa2013] , [Park2013], [Marc2014] , [Carl2014], [Shef2015] ont utilisé la forme de la main dans leurs systèmes d'authentification. Ces derniers exploitent les images capturées de la vue de dessus et la vue de côté de la main pour calculer la largeur des doigts à divers endroits, la largeur et l'épaisseur de la paume, la longueur des doigts, et ainsi de suite (*Tableau 4.2*).

[Jain1999]	Extraction de différentes caractéristiques de la main : • longueur et hauteur des doigts, • hauteur de la main.
[Reil2000]	Des mesures sont effectuées sur les deux vues (face et profil : analyse en 3D). Suite à une détection des contours par l'opérateur de Sobel, 25 caractéristiques sont extraites : • largeurs des 4 plus grands doigts (annulaire, auriculaire, majeur, index). • largeur de la paume. • longueurs du majeur et de l'auriculaire Angles et distances entre les « fourchettes interdigitales ».
[Wong2002]	Les caractéristiques extraites sont séparées en deux groupes : • Le groupe 1 contient 13 caractéristiques (longueurs et largeurs des doigts), • le groupe 2 contient les 3 régions extrêmes (de l'index, du majeur et de l'annulaire). Les régions extrêmes sont des séries de points ordonnés issus du contour des doigts.
[Kuma2003]	Les deux caractéristiques biométriques étudiées sont : la géométrie de la main et les empreintes palmaires (lignes de la main). ✓ Géométrie de la main : 16 primitives issues de la géométrie de la main en sont extraites : • Longueurs des 4 plus grands doigts • Largeurs des 2 articulations des 4 plus

	grands doigts • Largeur de la paume • Hauteur de la paume • Aire de la main • Hauteur de la main (paume + majeur). Les empreintes sont extraites grâce à différents masques permettant de faire apparaître les lignes d'orientation 0°, 45°, 90°, 135°.
[Pave2004]	• Caractéristiques géométriques. • longueur du doigt, • largeurs du doigt, • largeur de la paume, • contour de la main.
[Cova2005]	Les caractéristiques extraites sont : • Longueurs des doigts, • Chaînes de mesure de la largeur des doigts (vecteur de largeurs), • Largeurs de la base des doigts, • Largeur du « poignet », • Aire de la partie supérieure de la main, • Largeur de la paume, • Aires des doigts, • Aire de la paume.
[Yoru2006]	• Les coordonnées du contour de la main
[Varc2007]	Les caractéristiques extraites sont : • largeur du doigt à 3 hauteurs différentes, • hauteur du doigt, • la taille de la palme.
[Migu2007]	Les caractéristiques extraites sont : • Caractéristiques géométriques de la main, • Texture des empreintes digitales.

[Migu2008]	Les caractéristiques extraites sont : • Contour de la main.
[Baha2010]	Les caractéristiques extraites sont : • Mesures géométriques (longueur et largeur) de quatre doigts.
[Rong2012]	Les caractéristiques extraites sont : • Contour de la main.
[Jing2012]	Les caractéristiques extraites sont : • largeur du doigt, • longueur du doigt.
[Rafa2013]	Les caractéristiques extraites sont : Caractéristiques géométriques de la main : • région, • périmètre, • longueur, • largeur, • aspect proportion.
[Park2013]	Les caractéristiques extraites sont : • largeur des doigts, • la longueur des doigts, • largeur de la paume, • le rapport entre la longueur du doigt du milieu, l'index et l'annulaire.
[Marc2014]	Les caractéristiques extraites sont : • 8 mesures de chaque doigt, • 2 mesures de l'angle de chaque doigt, sauf le pouce • 6 descripteurs de la main.

[Carl2014]	Les caractéristiques extraites sont : • contour de la main, • la forme la main.
[Shef2015]	Les caractéristiques extraites sont : • forme de la main, • des caractéristiques géométriques.

Au meilleur de notre connaissance, il n'y a aucun travail qui exploite la vue de dessous de la forme de la main au moment de la signature pour améliorer les performances de tout système d'authentification de signature. Le défi ici est de montrer que cette information pourrait être exploitée efficacement pour réduire les contrefaçons qualifiées *FAR*.

En réexaminant les images vidéo acquises, nous avons constaté qu'il est possible d'extraire au début du processus de signature un descripteur discriminant forme de main qui peut caractériser la main du signataire. En effet, sur la base du principe selon lequel une personne a les mêmes habitudes concernant sa pose initiale de la main au moment de signature, on peut extraire et exploiter un descripteur forme de la main afin de vérifier si la main au moment de la signature est similaire à celle de la personne inscrite ou non.

4.4.2 Extraction du descripteur forme de la main

En raison de l'état fermé de la main au moment de la signature, les métriques de distance bien utilisées et décrites dans [Jain1996] ne conviennent pas à notre cas. Ainsi, plusieurs tests basés sur la surface de la main, le périmètre, la largeur et la hauteur ont été effectuées pour trouver le meilleur descripteur discriminatoire de la forme de la main. Les largeurs des mains seulement nous ont donné de bons résultats.

Un exemple de deux mains acquises avec leurs correspondantes largeurs de forme de la main est présenté dans la *Figure 4.6*.

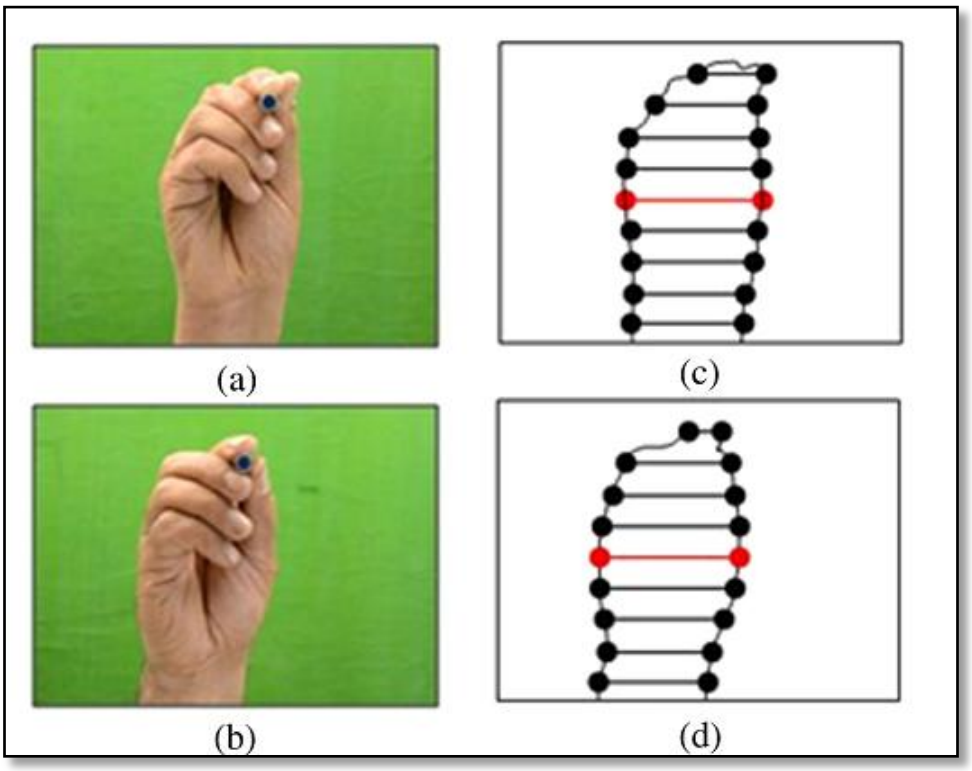


FIGURE 4.6 - Distances des mains signataires: (a) et (b) deux mains au moment de signature, (c) et (d) largeurs de mains correspondantes

Pour chaque main, un ensemble de neuf distances sont extraits et utilisés pour calculer la similitude des mains. Pour une meilleure précision, on peut prendre plus de neuf largeurs de forme de la main (par exemple 17 ou 21 valeurs).

Considérons deux mains au moment de la signature, $Main_x$ et $Main_y$, avec leurs neuf largeurs de main correspondantes :

$$Main_x\ (d_{x0}, d_{x1}, d_{x2}, d_{x3}, d_{x4}, d_{x5}, d_{x6}, d_{x7}, d_{x8})$$

$$Main_y\ (d_{y0}, d_{y1}, d_{y2}, d_{y3}, d_{y4}, d_{y5}, d_{y6}, d_{y7}, d_{y8})$$

Le pourcentage de similitude $S(X,Y)$; entre les deux mains au moment de signature est obtenu comme suit:

Tout d'abord, un vecteur de différence composé des neuf paires de différences est calculé avec :

$$V_{Diff\,(x,y)}=\{|d_{x0}-d_{y0}|,|d_{x1}-d_{x2}|,\ldots,|d_{x8}-d_{y8}|\} \quad (\mathbf{4.1})$$

Les valeurs obtenues sont comparées à un seuil prédéfini *T* et fixés à "zéro" si la différence est inférieure à *T* ou "un" si non. La mesure de similarité est alors calculée comme suit:

$$S(X,Y) = \left(\frac{\text{Nbr de valaur zero}}{9}\right) * 100 \quad (\mathbf{4.2})$$

Un exemple d'un vecteur de différence quantifié obtenu est: $V_{QDiff\,(x,y)} = \{1,1,0,0,0,0,1,0,0\}$.

La similarité calculée est égale à (6/9) x 100 = 67%.

Notez que la valeur de *T* est fixée de manière empirique en fonction du niveau de sécurité requis.

Dans les expériences, la valeur de *T* est fixée à 10. Les *Figures 4.7 et 4.8* présentent, respectivement, des exemples de mains au moment de la signature de certains contributeurs ainsi que leurs scores de similarités de la main calculés. On voit que la probabilité d'avoir les mains analogues est faible. Par conséquent, il est possible d'exploiter cette information pour réduire le nombre de contrefaçons acceptées.

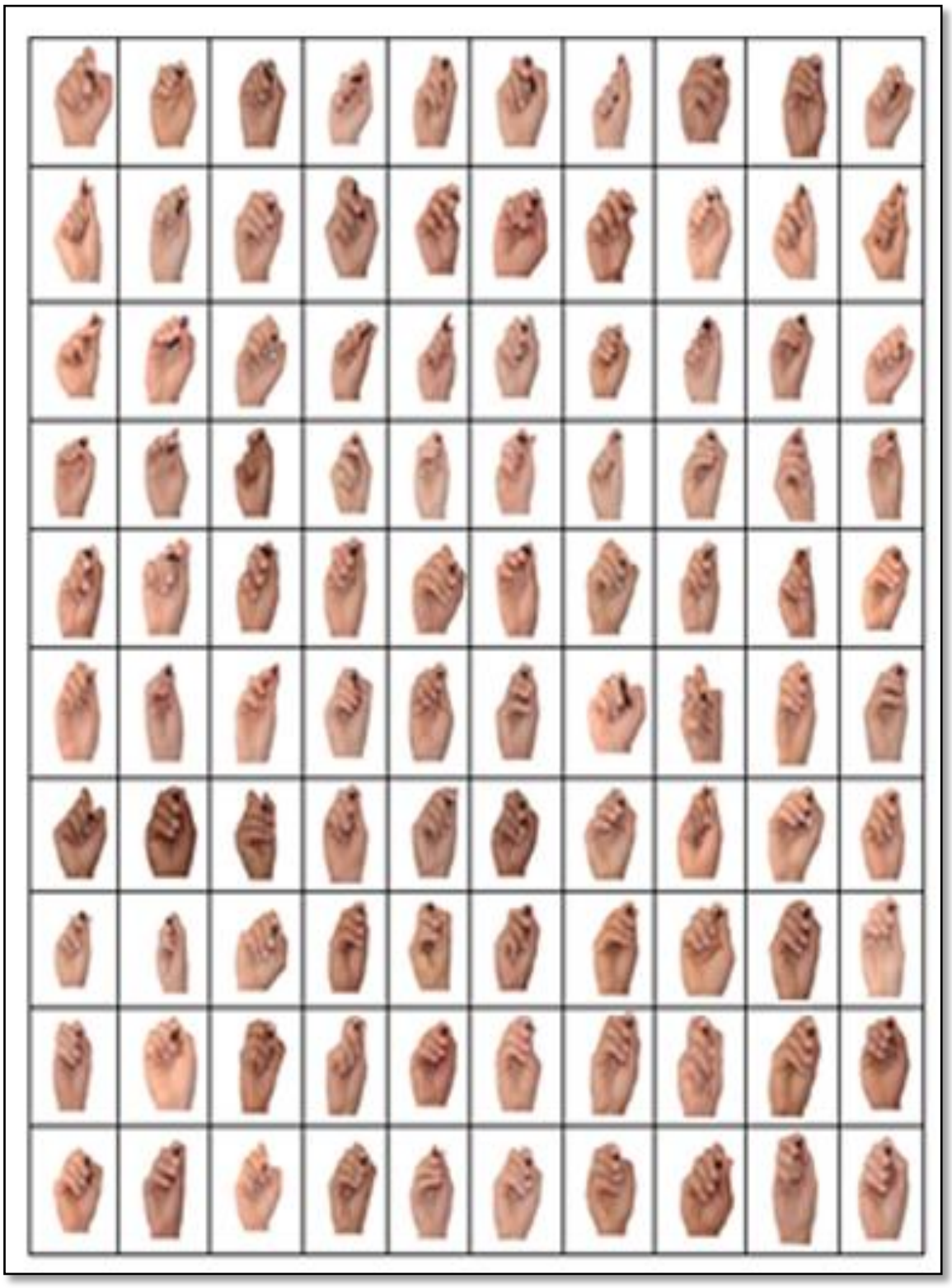


FIGURE 4.7 -Mains de signataires volontaires

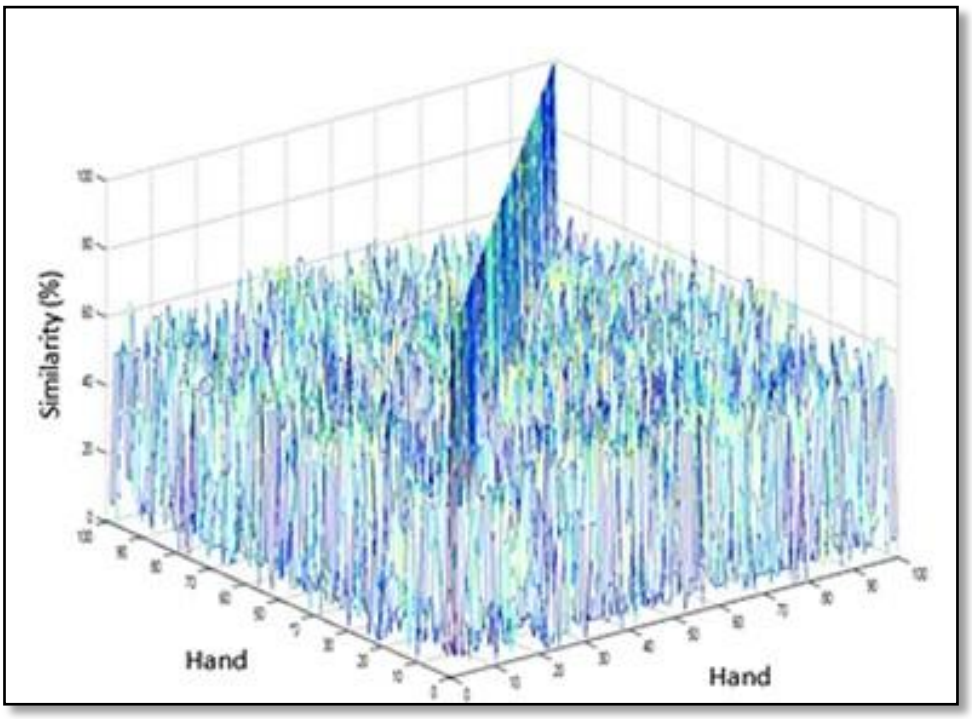


FIGURE 4.8 - Scores calculées de la similarité de la main

Les *Figures 4.9 et 4.10* et le *Tableau 4.3* montrent la performance de l'authentification sur la base de la modalité forme de la main. Les résultats obtenus confirment l'efficacité de cette modalité pour l'authentification.

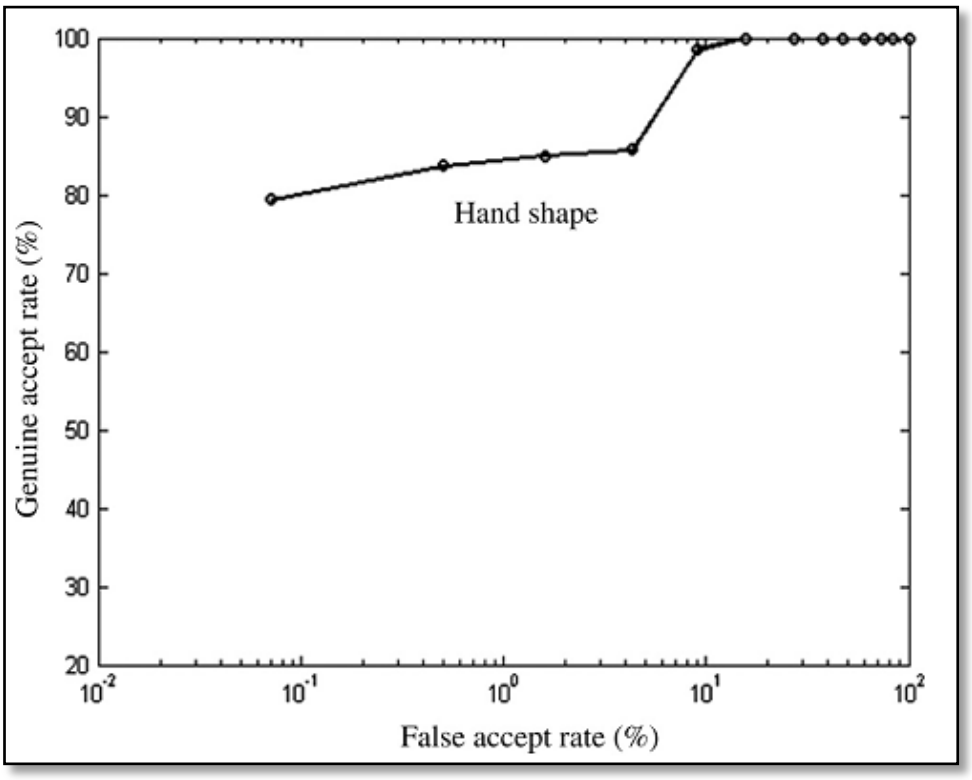


FIGURE 4.9 - Courbe ROC montrant la performance de la modalité forme de la main

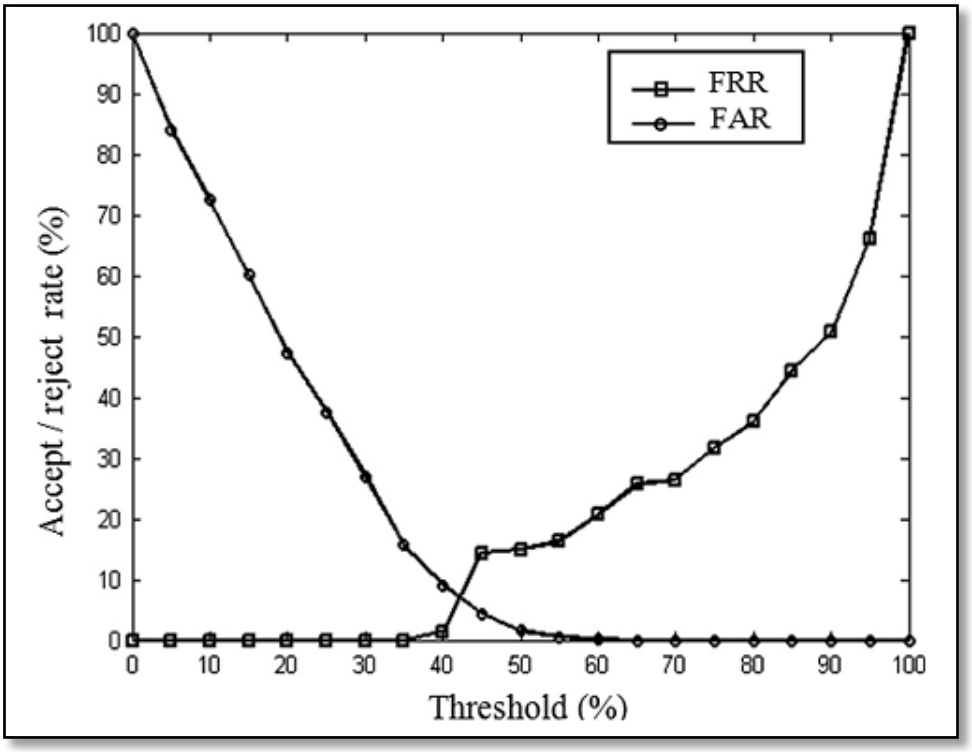


FIGURE 4.10 - Taux de faux rejet et acceptation par rapport au seuil de la modalité forme da la main

Tableau 4.3 Résultats des tests d'authentification pour la modalité forme de la main

Seuil	Véritable taux d'acceptation GAR (%)	Taux de fausses acceptations FAR(%)
35	100	15.6
40	98.6	9.00
45	85.7	4.30
50	85	1.60
56	83.7	0.50
60	79.4	0.07
63	74.3	0.00

4.4.3 Fusion au niveau des scores

Dans notre cas, toute personne inscrite est automatiquement identifié par sa signature de référence et son vecteur de la forme de la main (*Tableau 4.4*).

Tableau 4.4 - Structure de la base de données liée à la personne inscrite

Personne enrôlée	Signature référence	Vecteur de la forme de la main
P_0	Ref_0	$\{d_{00},d_{01},\ldots,d_{08}\}$
P_1	Ref_1	$\{d_{10},d_{11},\ldots,d_{18}\}$
…	…	…
…	…	…
…	…	…
P_n	Ref_n	$\{d_{n0},d_{n1},\ldots,d_{n8}\}$

Le processus d'authentification consiste à fusionner les scores d'authentification de la signature et de la forme de la main. Ainsi, aucune bonne imitation ne pourra automatiquement tromper le système de vérification de signature, à moins que la main de l'imitateur soit similaire à celle de la personne enrôlée. Un arbre de décision [Lip2012] est appliqué aux scores obtenus avec les deux modalités signature et forme de la main.

Le traitement est effectué en deux étapes (*Figure 4.11*). Dans la première étape, les scores d'authentification de signature sont comparés à un seuil fixé (T_1). Ceux avec des scores plus élevées que T_1 sont retenus pour la deuxième étape de traitement, tandis que le reste est considéré comme contrefaçons et sont rejetées. La deuxième étape consiste à comparer les résultats correspondants des scores de la main à un seuil fixe (T_2). Si le score obtenu est supérieur à T_2, alors la signature correspondante est déclarée comme une véritable signature, sinon elle est déclarée comme étant une contrefaçon.

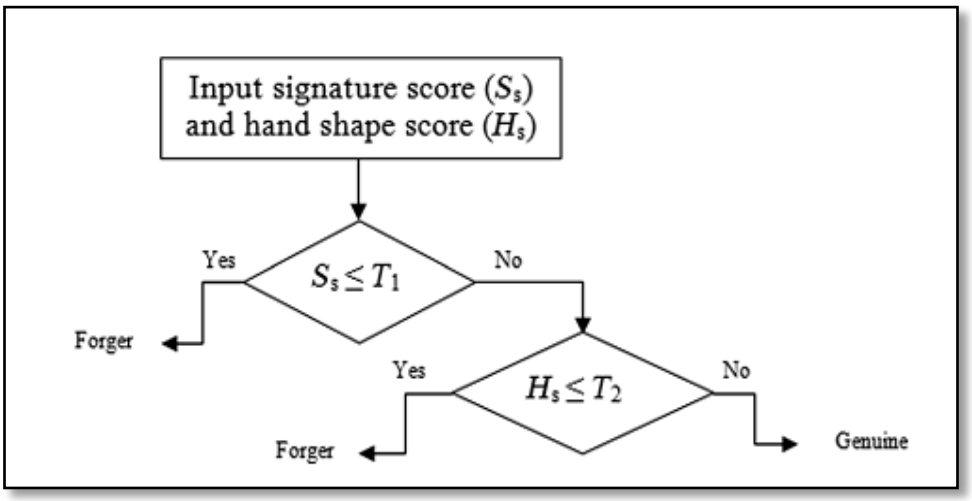


FIGURE 4.11 - Arbre de décision adoptée

Les résultats obtenus présentés sur les *Figure 4.12 et 4.13* et le *Tableau 4.5* montrent que l'inclusion du descripteur forme de la main permet une amélioration considérable dans les performances d'authentification.

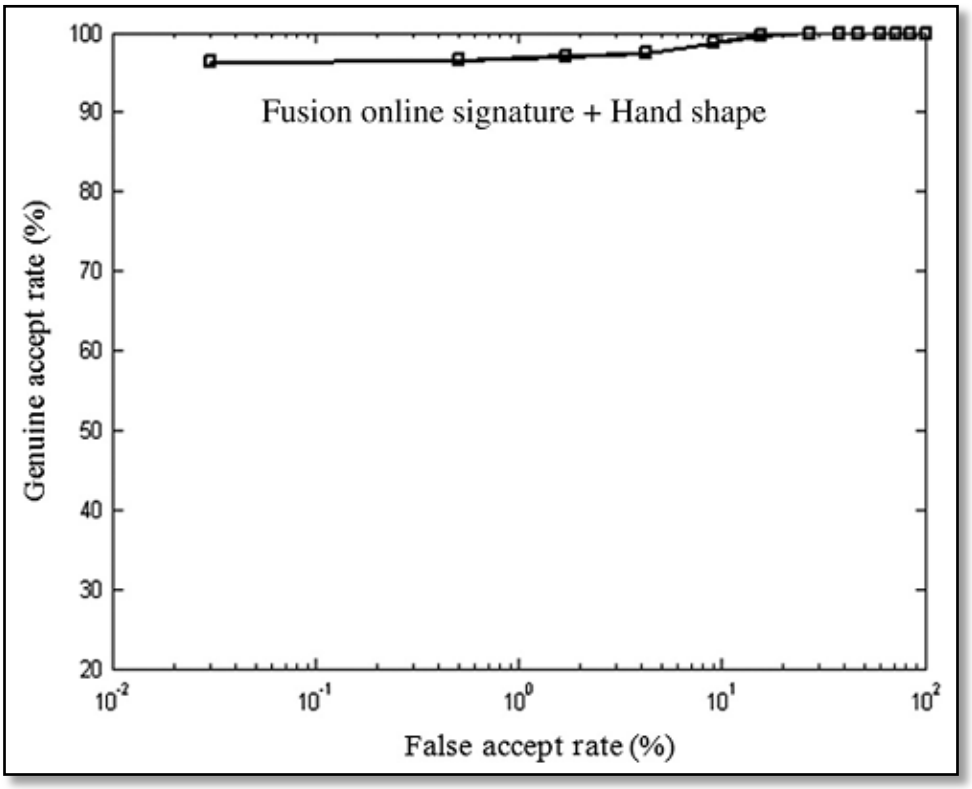


FIGURE 3.12 - Courbe ROC montrant l'amélioration des performances en combinant les deux modalités signature et forme de la main

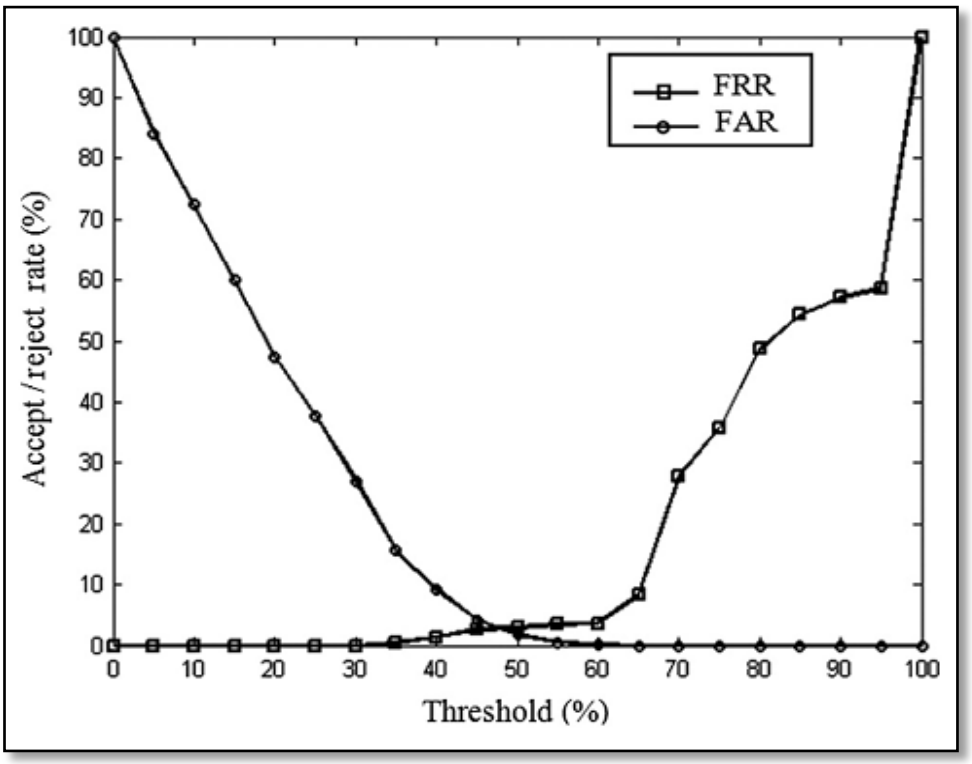


FIGURE 4.13 - Taux de faux rejet et acceptation par rapport au seuil de la combinaison de deux modalités signature et forme de la main

Tableau 4.5 - Résultats des tests d'authentification de la combinaison de deux modalités signature et forme de la main

Seuil	Véritable taux d'acceptation GAR (%)	Taux de fausses acceptations FAR(%)
30	100	27
35	99.7	15.6
50	97.1	1.70
55	96.6	0.50
60	96.4	0.03
65	91.7	0.00
88	58.9	0.00

4.4.4 Avantages du descripteur de la forme de main proposé

4.4.4.1 Détection des changements d'habitudes du signataire

Le descripteur forme de la main proposé permet au système de faire la différence entre les mains des signataires d'une part, et d'autre part, de détecter tout changement dans les habitudes des signataires. En effet, le signataire conserve généralement la même disposition de sa main et la manière de tenir le stylo lors de la signature.

Par conséquent, tout changement dans les habitudes des signataires diminuera automatiquement le degré de similitude entre la main testée et celle inscrite. L'exemple suivant (*Figure 14*) montre les différentes dispositions de la main de la même personne au début d'un processus de signature: *Figure 4.14 (a)* représente la main inscrite; *Figure 4.14 (b) - 4.14 (c) et 4.14 (d)* sont les mains du test.

Les scores de similarité rapportés de la main (H_S) montre que si la disposition de la main du signataire change, le degré de similitude diminue.

En conséquence, une signature déclarée authentique peut donc être considérée comme fausse tout simplement parce que le signataire a changé sa façon de signer.

Cette caractéristique intéressante est bénéfique pour l'authentification, car elle ajoute aux habitudes de l'écriture, qui se concrétisent par la signature produite, une habitude de la disposition de la main complémentaire et sélective. En d'autres termes, toute personne est déclarée authentique seulement si elle effectue le même geste de signature avec la même disposition de la main, sinon elle est déclarée comme faussaire.

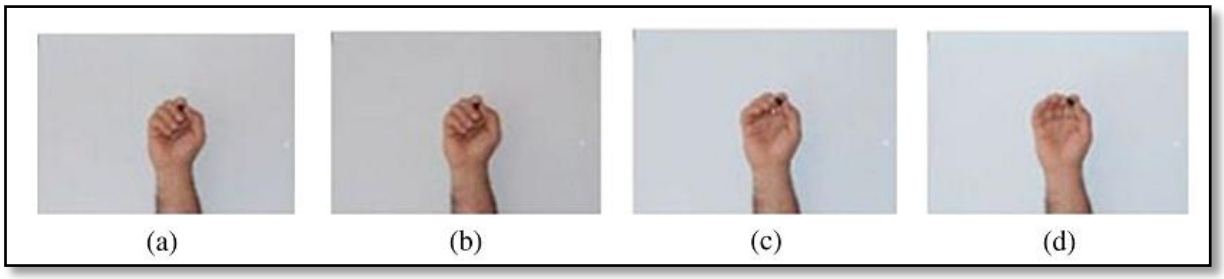


FIGURE 3.14 - Exemple des scores de similarité de la main (H_S) entre une main inscrite et une main d'essai: (a) la main de référence, (b) *Hs* = 100%, (c) *Hs* = 80%, (d) = 66%

4.4.4.2 Détection efficiente des contrefaçons

Une autre caractéristique intéressante concerne le score de dissimilitude obtenu par le descripteur développé dans le cas où le faussaire et le véritable signataire sont des personnes de sexes différents. Comme ce dernier présente généralement des morphologies de mains différentes, la probabilité d'avoir la main d'un homme semblable à celle de la main d'une femme est très faible. De ce fait, la probabilité d'accepter l'imitation, même si elle est parfaite, sera également très faible.

Afin de vérifier, nous avons rassemblé les imitations réalisées par un groupe de 20 hommes sur les signatures de 20 femmes et vice-versa. Le nombre total d'imitations est 2000 (20 × 10 × 10) pour chaque sexe.

Les résultats expérimentaux, présentés sur les *Figures 4.15* et *4.16* et *Tableau 4.6*, montrent que l'exploitation d'un tel descripteur dans un système d'authentification de signature limite de manière significative les tentatives d'imitation frauduleuse, par exemple, par la violation de la confiance entre les couples et entre collègues ou des membres proches ou distants de la même famille. Les meilleurs résultats ont été obtenus avec un seuil fixé à 64 [taux d'acceptation véritable (*GAR*) = 96% et *FAR* = 0].

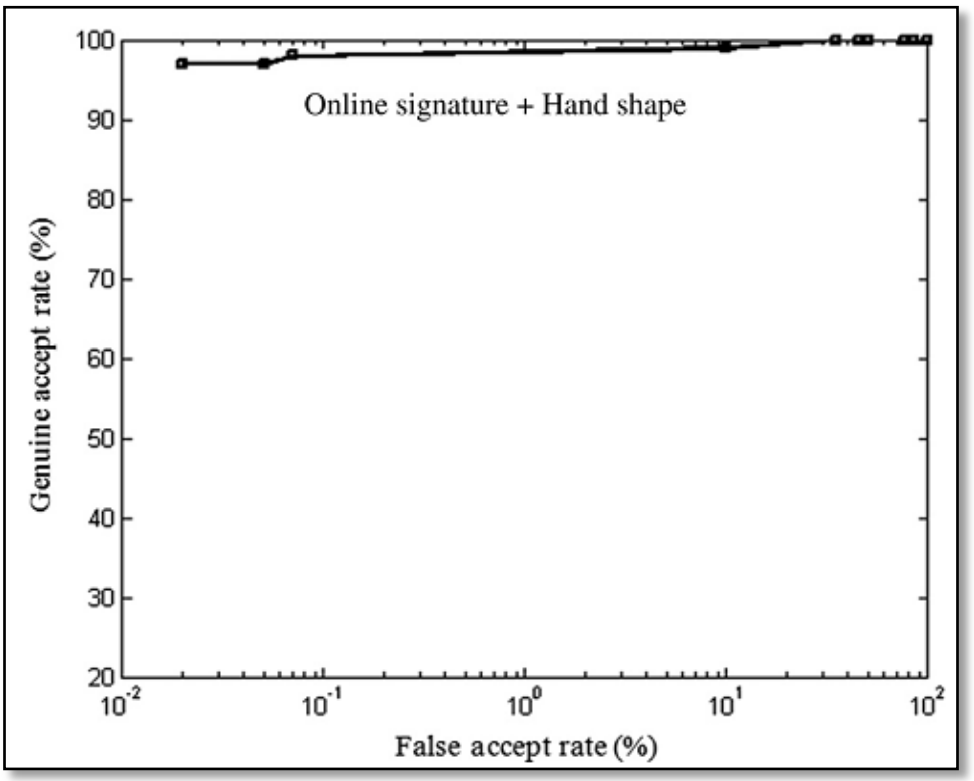


FIGURE 4.15 - Courbe ROC montrant l'amélioration des performances en combinant les deux modalités signature et forme de la main.

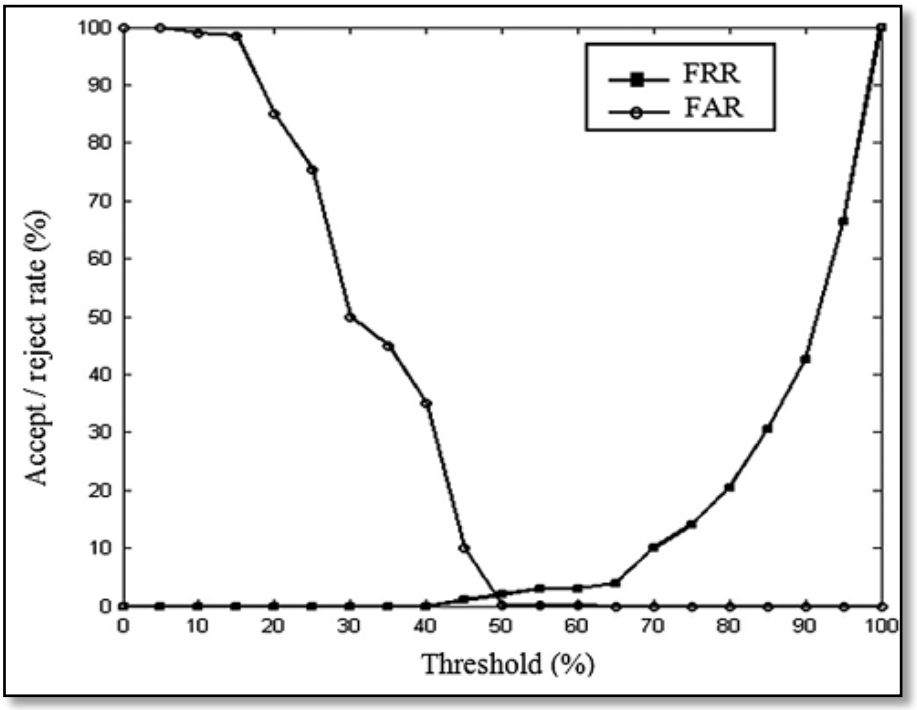


FIGURE 4.16 - Taux de faux rejet et acceptation par rapport au seuil de la combinaison de deux modalités signature et forme de la main

Tableau 4.6- Résultats des tests d'authentification de la combinaison de deux modalités signature et forme de la main

Seuil	Véritable taux d'acceptation GAR (%)	Taux de fausses acceptations FAR(%)
41	100	35
46	99	10
51	98	0.07
56	97	0.05
60	97	0.02
63	96	0.00

4.4.5 Calcul de la complexité

La complexité de la méthode proposée est due au calcul du vecteur de différence (4.1) et le pourcentage de similitude (4.2). Ces valeurs sont calculées par des opérations mathématiques simples. Considérons le cas où la taille du vecteur de différence est égale à neuf. Le calcul de (4.1) et (4.2) exige 9 soustractions, une division et une multiplication.

Nous avons implémenté et testé notre méthode d'authentification dans l'environnement *MATLAB R2012* sur un *PC Dual Core 2,10 GHz, 2- GB de RAM*. La complexité du calcul est

évaluée par la mesure de la vitesse de traitement pour différentes tailles du descripteur forme de la main. Les résultats obtenus sont résumés dans le *Tableau 4.7*.

Tableau 4.7 - Temps de calcul pour le traitement

Taille du descripteur la forme de la main	Temps de traitement (ms)
9	0.215
17	0.280
21	0.310

4.5 Comparaison de l'approche proposée avec d'autres techniques avancées

Une étude comparative avec quelques méthodes d'authentification bimodale existantes est présentée dans le *Tableau 4.8*. La comparaison concerne: les caractéristiques utilisées, le nombre de participants (P), le nombre de capteurs utilisés, et les scores obtenus *FAR*, *FRR*, ou *EER*.

Même si les trois premières méthodes [Park2013] [Kuma2003] [Poin2011] ont de bonnes performances d'authentification (*EER* <1), elles exploitent des descripteurs physiques et sont plus vulnérables aux attaques que les descripteurs comportementaux [Namb2004] [Buha2005]. En effet, ces approches peuvent être usurpée par la présentation d'une fausse main et / ou un visage enregistré.

Le reste des méthodes déclarées (y compris la méthode proposée) combinent les deux descripteurs physiques et comportementaux dans un système d'authentification unique.

Comme mentionné précédemment, la particularité de la méthode proposée est que le descripteur physique forme de la main fermée peut être considéré comme un descripteur de comportement parce qu'il donne des informations supplémentaires sur les habitudes de la disposition de la main du signataire.

Les informations et les résultats recueillis dans les articles [Humm2006] [Elmi2012] [Park2013] [Kuma2003] [Poin2011] [Namb2004] montrent que notre approche présente le meilleur compromis entre l'efficacité (*EER*=2) et la simplicité (un seul capteur est utilisé). En effet, contrairement aux autres systèmes bimodaux, le système proposé exige seulement une sonde pour capturer simultanément la forme de la main et de signature requises. En outre, imiter la disposition de main fermée et la signature simultanément sera certainement une tâche difficile pour les faussaires expérimentés.

Tableau 4.8 - Comparaison avec d'autres techniques principales

Référence et année	Caractéristiques utilisées	Base de données	Nombre de capteurs	Performances
[Park2013] et 2013	Vasculaire et géométrie de la main	100 P	1	EER = 0.06
[Kuma2003] et 2003	Empreinte de la paume et géométrie de la main	100 P	1	FAR = 0, FRR = 1.41
[Poin2011] et 2011	Empreinte de la paume et le visage	130 P	2	EER = 0.79
[Humm2006] et 2006	Signature et parole	70 P	2	EER aléatoire = 3.5 EER qualifié = 6.9
[Namb2004] et 2004	Signature et visage	100 P	2	EER = 2.2
[Elmi2012] et 2012	Signature et visage	40 P	2	EER = 3
2014	Notre approche	100 P	1	EER = 2

4.6 Discussion et conclusion

Dans ce chapitre, nous avons montré qu'il est préférable de considérer la signature comme une couple habitude d'écriture/disposition de la main plutôt qu'une simple habitude d'écriture.

Une approche heuristique d'authentification efficace basée principalement sur l'exploitation de la signature de la main et le descripteur forme de la main a été validée.

Contrairement aux approches d'authentification multimodales existantes, le procédé d'authentification proposé ne nécessite qu'un seul capteur en ligne puisque la signature reconstruite et le descripteur forme de la main sont extraits de la même source vidéo.

Basé sur l'hypothèse que la même personne a les mêmes habitudes concernant la pose initiale de sa main au moment de la signature, on peut extraire et utiliser un descripteur forme de la main pour effectuer une authentification de la signature précise. Ainsi, une signature authentique ou une

bonne contrefaçon est déclarée comme une véritable signature que si la main du signataire est similaire à celle de la main de la personne inscrite.

La méthode d'authentification DTW a été utilisée pour l'authentification de la signature, mais en raison de sa complexité de calcul, elle ne sera pas choisie pour effectuer en temps réel l'authentification des signatures en ligne. Un procédé d'authentification dédié, basé sur le calcul des vecteurs de mouvement, est en cours de développement en fonction de contraintes du temps réel. En outre, l'approche d'authentification de la forme de la main développée, présente une faible complexité de calcul et est donc bien adaptée pour un traitement en temps réel.

Même si elle repose entièrement sur un système d'acquisition dédié, l'approche proposée permet d'effectuer une authentification de signature précise, qui est nécessaire pour les transactions bancaire et les applications de contrôle d'accès à des sites sensibles.

Chapitre 5

Méthodes de fusion

Chapitre 5

Méthodes de fusion

Dans ce chapitre, nous traitons la fusion multimodale, les types de fusion et aussi expliquer les différents niveaux de fusion possibles. Nous portons notre attention sur la fusion au niveau de score (choisie pour notre cas). Dans le même cadre, nous rappelons les principales méthodes de normalisation des scores et de combinaisons de ces derniers.

Sommaire

5.1 Introduction 83

5.2 Les types de fusions 83

5.2.1 Système multi- échantillons 83

5.2.2 Système multi- capteurs 83

5.2.3 Système multi- algorithmes 84

5.2.3 Système multi-instances 84

5.2.3 Système multi-biométries 84

5.3 Les différents niveaux de fusion 85

5.4 La fusion au niveau des scores 88

5.4.1 Normalisation des scores 88

5.4.1.1 Les différentes techniques de normalisation de scores 89

5.4.2 Approche par classification de scores 90

5.4.3 Combinaison des scores 90

5.5 Conclusion 92

5.1 Introduction

Le procédé de reconnaissance biométrique est la manière avec laquelle le système procède à l'authentification pour aboutir à une décision unique à propos de l'authenticité d'un intrus. Cette manière dépend de la nature de données biométriques transmises, tout au long de la chaîne de reconnaissance. Les données biométriques, manipulées dans chaque étape de la chaîne proviennent d'une ou de plusieurs sources. La (*Figure5.1*) représente les cinq types de sources de données biométriques qui caractérisent une telle modalité de reconnaissance.

Les systèmes de reconnaissance biométrique, dits monomodaux, disposent d'une seule source d'informations biométriques dans chacune de leur phase de traitement. Les limites rencontrées dans ce type de systèmes peuvent être surpassées, en fusionnant plusieurs données biométriques de natures différentes, ceci a donné naissance à de nouveaux systèmes composés appelés « système multimodaux » [Ross2003].

5.2 Les types de fusions

La (*Figure 5.1*) illustre les sources d'information de différents types de fusion de trais biométriques qui peuvent être considérées dans un système biométrique multimodal.

5.2.1 Systèmes multi–échantillons

Un seul capteur peut être utilisé pour acquérir plusieurs échantillons de la même modalité biométrique. Par exemple, un système de reconnaissance faciale peut capturer la face du visage d'une personne ainsi que les profils gauches et droits afin de tenir compte des variations de la pose faciale.

5.2.2 Systèmes multi–capteurs

Dans ces systèmes, la même modalité biométrique est analysée à l'aide de plusieurs capteurs afin d'extraire diverses informations provenant de l'enregistrement des images. Par exemple, un système peut enregistrer le contenu (2D) du visage avec une caméra (CCD[1] ou CMOS[2]), et la forme de la surface (3D) du visage avec une autre gamme de capteurs camera (3D). Dans ce cas, le coût du système biométrique multimodal augmente.

[1] **CCD**: **C**harge **C**oupled **D**evice – **D**ispositif à **T**ransfert de **C**harge (**DTC**).
[2] **CMOS**: **C**omplementarity **M**etal-**O**xide-**S**emiconductor.

5.2.3 Systèmes multi–algorithmes

Dans ces systèmes, les mêmes données biométriques sont traitées avec plusieurs algorithmes.

Par exemple, des algorithmes d'analyse de texture et de minuties peuvent être associés pour traiter la même image d'empreintes digitale afin d'extraire les caractéristiques qui peuvent améliorer la performance du système. Ainsi, ce genre de système ne nécessite pas de capteurs supplémentaires.

5.2.4 Systèmes multi–instances

Ces systèmes utilisent plusieurs instances d'un même trait biométrique. Par exemple, l'iris gauche et droit d'un individu**.**

5.2.5 Systèmes multi–biométriques

Ces systèmes ont attiré l'attention des chercheurs, car ces derniers permettent de combiner les résultats de différentes modalités biométriques afin de reconnaitre un individu. Les premiers systèmes multimodaux ont utilisé les caractéristiques du visage et de la voix [Jain2008]. Souvent, des traits biométriques décorrélés (comme les empreintes digitales et l'iris...) fournissent de meilleurs résultats que des traits biométriques associés (comme les mouvements des lèvres et la voix).

Les systèmes de reconnaissance biométrique multimodaux sont prévus pour être plus fiables et assez robustes, grâce à la présence de plusieurs solutions indépendantes pour la preuve d'identité [Kunn2000]. D'un côté, cette approche s'adresse aux problèmes liés au manque d'universalité dans une population ou à l'instabilité d'une caractéristique chez la même personne. En général, ces problèmes conduisent à des taux TFR importants. En se basant sur plusieurs critères de reconnaissance, le système peut assurer le recouvrement d'un maximum des personnes légitimes.

D'un autre côté, les systèmes multimodaux sont susceptibles de répondre aux exigences strictes imposées par les applications critiques. Pour ces dernières, les fausses acceptations dues à une falsification ou une similarité à l'intérieur d'une population sont intolérables. Comme il est difficile d'imiter simultanément plusieurs traits caractéristiques, les systèmes multimodaux sont efficaces pour la réduction des tentatives frauduleuses et la minimisation des conséquences négatives des fausses acceptations. Par ailleurs, la performance des systèmes monomodaux est sensible aux informations brouillées, à cause des mauvaises conditions d'acquisition, d'imperfection

des capteurs ou d'une altération temporaire de la caractéristique biométrique. Pour les systèmes multimodaux, le défaut d'une modalité peut être compensé par d'autres modalités [Viel2006].

Enfin, on peut noter que l'on utilise le terme de systèmes hybrides [Chan2005] pour se référer aux systèmes qui intègrent un sous-ensemble des 5 scénarios.

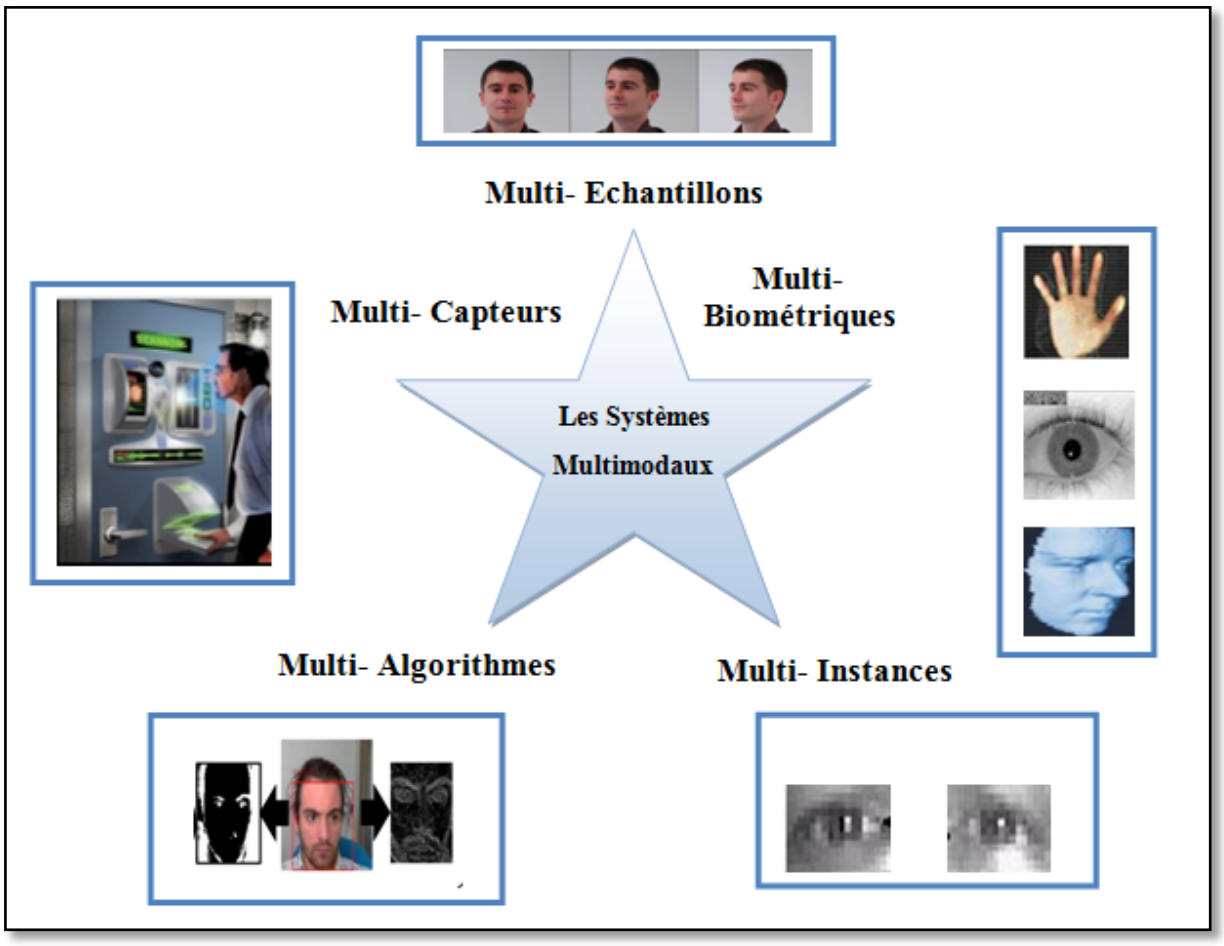


FIGURE 5.1- Sources de différents types de fusion de trais biométriques

5.3 Les différents niveaux de fusion

Dans un système biométrique multimodal, une ou plusieurs étapes sont approvisionnées par plusieurs sources de données. Afin d'arriver à une décision unique, le système doit traiter les données biométriques provenant de chaque source, comme une seule entité, en les fusionnant. La fusion de données peut avoir lieu dans l'une des étapes qui suivent l'étape recevant les données biométrique de plusieurs sources.

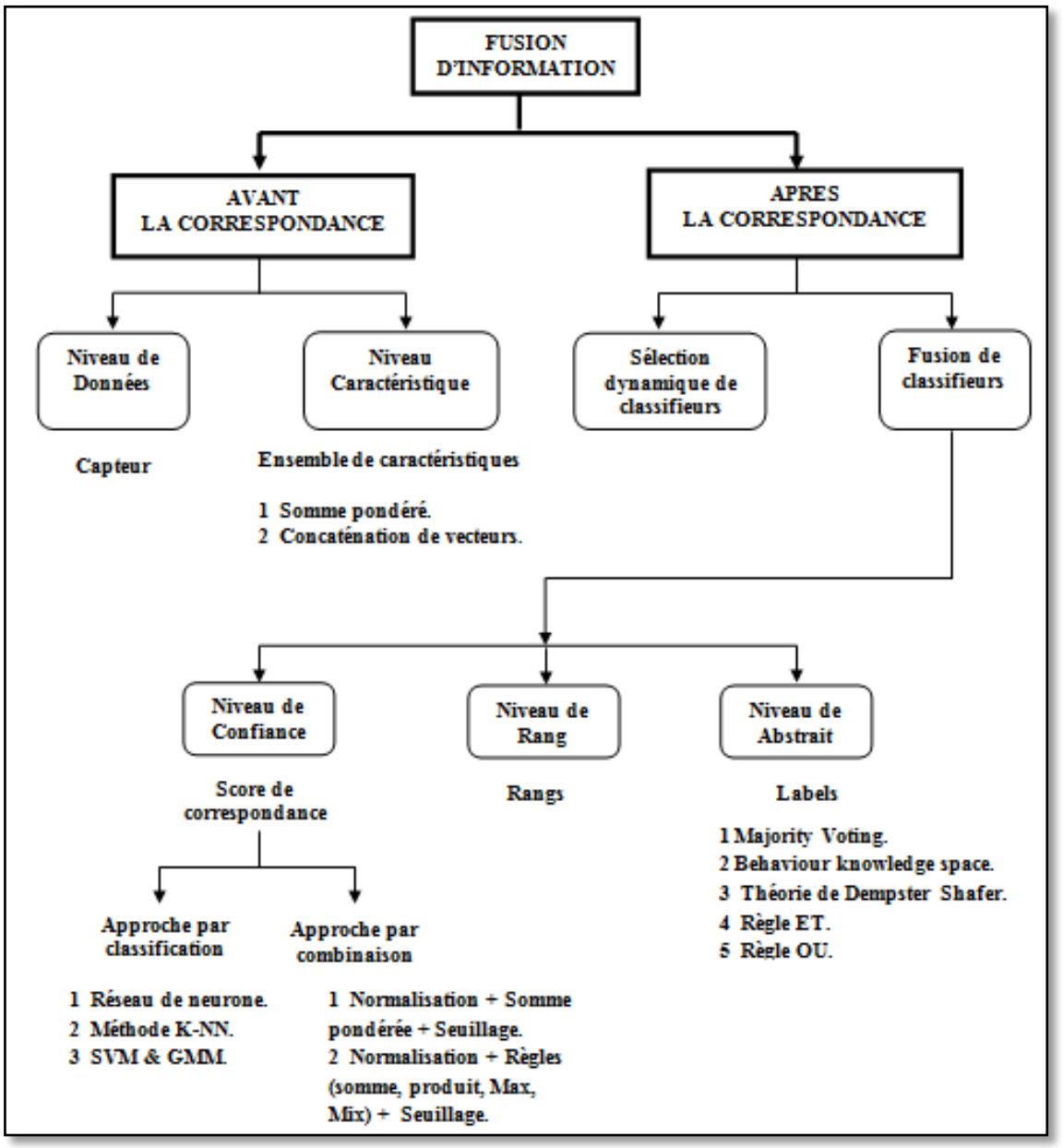


FIGURE 5.2 – Résumé des approches de fusion dans les systèmes biométriques multimodaux [Jain2005]

Comme le processus de reconnaissance biométrique se fait en quatre étapes, il existe quatre stratégies de fusion de données biométriques, et qui sont détaillées en (*Figure 5.2*):

- ✓ ***La fusion au niveau capteur (données) :*** les données brutes provenant des capteurs sont combinées par fusion au niveau capteur. La fusion au niveau capteur peut se faire uniquement si les diverses captures sont des instances du même trait biométrique obtenu à partir

de plusieurs capteurs compatibles entre eux ou plusieurs instances du même trait biométrique obtenu à partir d'un seul capteur.

✓ ***La fusion au niveau descripteurs :*** l'ensemble des vecteurs de descripteurs qui correspondent aux différentes modalités mises en œuvre, sont combinés afin de former un seul vecteur qui sera utilisé pour la classification (*Figure 5.3*).

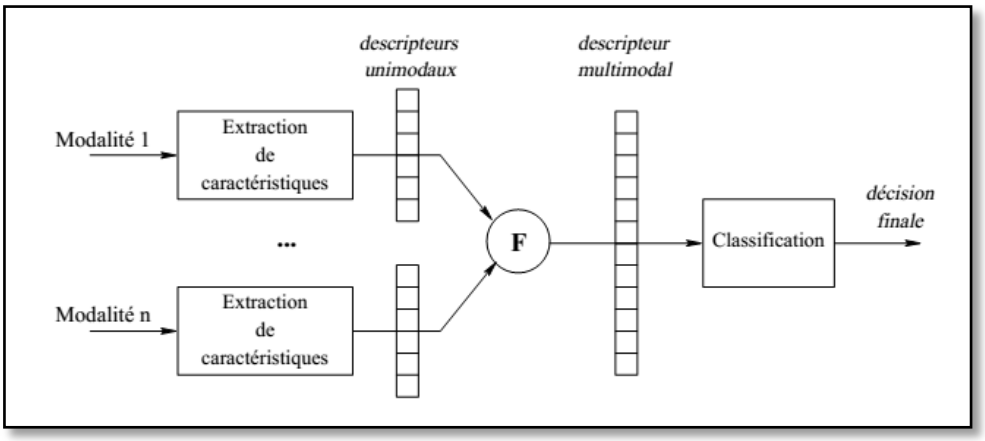


FIGURE 5.3- Organisation générale d'un processus multimodal basé sur la fusion de caractéristiques

✓ ***La fusion des scores :*** chaque modalité est traitée par un sous-système à part. La décision est basée sur un score unique qui est obtenu en effectuant une pondération sur les scores issus de chaque sous-système (*Figure 5.4*).

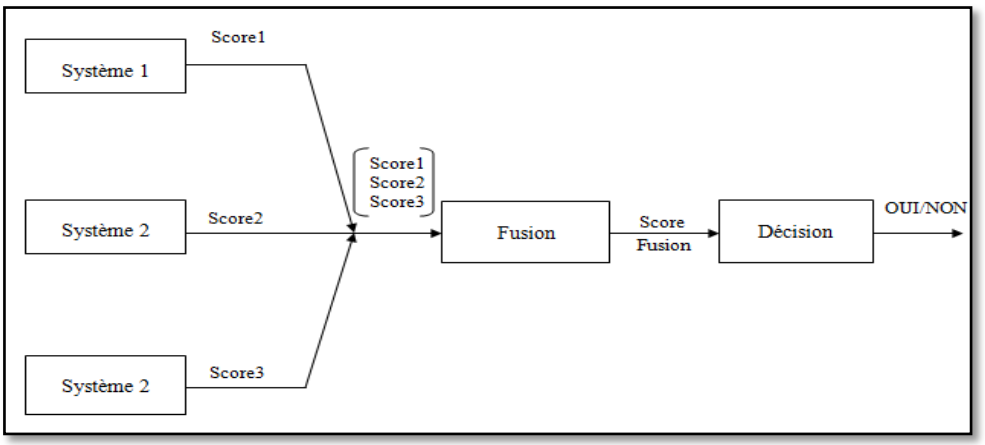


FIGURE 5.4- Schéma de la fusion de scores

✓ ***La fusion des décisions :*** la décision finale est prise par la fusion des décisions élémentaires provenant de chaque sous-système. Ainsi, une règle de fusion est requise (*Figure 5.5*).

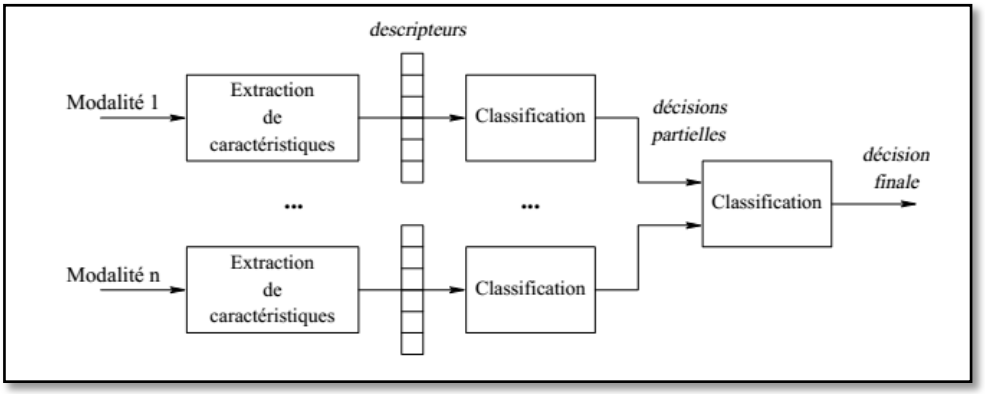


FIGURE 5.5- Organisation générale d'un processus multimodal basé sur la fusion de décisions

5.4 La fusion au niveau des scores

Il existe deux approches pour combiner les scores obtenus de différentes modalités :

- ✓ ***Approche par classification :*** dans l'approche par classification, un vecteur de caractéristiques est construit en utilisant les scores de correspondance donnés en sortie de différentes modalités ; ce vecteur est ensuite attribué à une des deux classes : "*accepté*" (utilisateur authentique ou "genuine user") ou "*rejeté*" (utilisateur imposteur ou "impostor user").

- ✓ ***Approche par combinaison :*** dans l'approche par combinaison, les scores de correspondance 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 de scores provenant de différentes modalités soit cohérente, les scores doivent normaliser.

Jain et al. ont montré que les approches par combinaison sont plus performantes que la plupart des méthodes de classification [Jain2005] [Ross2000].

5.4.1 Normalisation de score

La normalisation des scores est une étape nécessaire pour résoudre les problèmes de la fusion au niveau des scores :

- ✓ les scores en sortie de différentes modalités peuvent ne pas être homogènes. Par exemple, une première modalité donne un score de dissimilarité (une mesure de distance) tandis qu'une deuxième modalité donne un score de similarité (une mesure de proximité).

✓ les scores en sortie de différentes modalités peuvent ne pas être inclues dans le même intervalle.

✓ les scores retournés par différentes modalités peuvent suivre des distributions statistiques différentes.

5.4.1.1 Les différentes techniques de normalisation de scores

Le *Tableau 5.1* résume les différentes techniques de normalisation de scores en termes de robustesse et d'efficacité [Jain2005]:

Tableau 5.1- Résumé des techniques de Normalisation de Scores

Technique de Normalisation	Robustesse	Efficacité	Fonction de normalisation
MinMax	Non	N/A	$s' = \frac{s - min_i(s_i)}{max_i(s_i) - min_i(s_i)}$ où ***s*** représente le vecteur de scores.
Decimal Scaling	Non	N/A	$s' = \frac{s}{10^n}$ où $n = \log_{10} \max s$.
Z-Score	Non	Elevée (optimale pour des données gaussiennes)	$s' = \frac{s - \mu}{\sigma}$ où μ est la moyenne de la distribution calculée ou estimée, et σ l'écart–type.
Médiane et MAD	Oui	Modérée	$s' = \frac{s - median}{MAD}$ où $MAD = \text{median}(\lvert s - \text{median}(s)\rvert)$.
QLQ	Oui	Elevée	$s' = \begin{cases} \frac{1}{(c-\frac{w}{2})}s^2, & si\ s \le (c-\frac{w}{2}) \\ s & (c-\frac{w}{2}) < s \le (c+\frac{w}{2}) \\ (c+\frac{w}{2}) + \sqrt{(1-c-\frac{w}{2})(s-c-\frac{w}{2})} & sinon \end{cases}$ ***QLQ*** prend comme paramètres le centre *c* et la largeur *w* de la zone

			de recouvrement entre les distributions des imposteurs et des authentiques.
Double Sigmoïde	Oui	Elevée	$s' = \begin{cases} \frac{1}{1+\exp\left(-2\left(\frac{s-t}{r_1}\right)\right)} & si\ s < t \\ \frac{1}{1+exp\left(-2\left(\frac{s-t}{r_2}\right)\right)} & sinon \end{cases}$ où t est un point de référence et r_1 et r_2 sont des paramètres permettant de définir les deux fonctions sigmoïdes.

5.4.2 Approche par classification de scores

Les méthodes basées sur la modélisation multidimensionnelle des distributions utilisent la théorie de la décision bayésienne pour effectuer une classification des scores en fonction de leur probabilité à posteriori [Kitt1998]. Parmi celles-ci on peut citer : les méthodes de fusion à base de

GMM (Gaussian Mixture Model) [Rayn 1994] et les méthodes de fusion à base de classifieurs ***SVM*** (Support Vector Machine) [Woo2006] [Vapn1995] (*Figure 5.2*).

5.4.3 Combinaison des scores

Différentes règles de combinaison de scores formalisées dans [Kitt1998] ont jeté les bases de la fusion multimodale au niveau scores. Un nouveau score c est produit à partir des scores s_i des M matchers.

5.4.3.1 La règle produit (Product rule)

Cette règle définit les nouveaux scores comme étant le produit des scores de chaque matcher :

$$c = \prod_{i=1}^{M} s_i \qquad (\mathbf{5.1})$$

5.4.3.2 La règle somme (Sum rule) :

Cette règle définit les nouveaux scores comme étant la somme des scores de chaque matcher :

$$c = \sum_{i=1}^{M} s_i \qquad (\mathbf{5.2})$$

5.4.3.3 La règle maximum (Max rule)

La règle maximum se contente de définir un nouveau score comme étant le score maximal des scores de chaque mtcher :

$$c = \max_i(s_i) \qquad (\mathbf{5.3})$$

5.4.3.4 La règle minimum (Min rule)

La règle minimum se contente de définir un nouveau score comme étant le score minimal des scores de chaque matcher :

$$\mathrm{c} = \min_i(s_i) \qquad (\mathbf{5.4})$$

5.4.3.5 La somme pondérée

Les scores issus des différents matchers peuvent également être combinés par une somme pondérée.

$$s = \sum_{i}^{M} w_i s_i \qquad (\mathbf{5.5})$$

M : nombre de termes utilisés (matchers).

w: poids $w = \frac{eer_i}{\sum_i^N eer_i}$

S : score

Dans [Jain2000], des poids spécifiques à chaque utilisateur sont utilisés pour réaliser une somme pondérée des scores issus de différentes modalités. L'idée de cette technique est que certaines personnes peuvent avoir certains traits biométriques de moins bonne qualité que d'autres personnes. Ainsi, certains ouvriers par exemple peuvent, à force de travaux manuels, présenter des empreintes digitales altérées. Un faible poids pour les empreintes digitales peut, dans ce cas, réduire les probabilités de faux–rejet. Ce type de méthode requiert cependant un apprentissage spécifique des poids pour chaque utilisateur, et nécessite donc de nombreux échantillons d'apprentissage.

Jain et Ross [Jain2000] ont proposé l'utilisation de poids spécifiques à chaque utilisateur afin de calculer la somme pondérée de scores provenant de différentes modalités.

La motivation qui se cache derrière cette idée est qu'une petite partie de la population ne peut pas fournir de manière fiable certains traits biométriques. Par exemple, on ne peut pas obtenir d'empreintes digitales de bonne qualité à partir de personnes possédant des doigts abîmés par des opérations manuelles répétées. Pour de tels utilisateurs, assigner un poids plus faible au score d'empreinte digitale et un poids plus élevé aux scores d'autres modalités réduit leurs probabilités d'être faussement rejetés par le système biométrique.

5.5 Conclusion

La plupart des travaux de recherche en fusion dans les systèmes biométriques multimodaux se sont concentrés sur la fusion au niveau score, en particulier, l'approche par combinaison de scores a reçu une attention considérable [Jain2005].

De plus, la plupart des techniques de fusion au niveau score peuvent être appliquées seulement si les modalités individuelles peuvent fournir une performance de reconnaissance raisonnablement bonne (pas de modalité faillible).

Chapitre 6

Vers une prise de décision incrémentale

Chapitre 6

Vers une prise de décision incrémentale

Ce chapitre traite la mise en œuvre de l'ensemble des modalités en vue d'une prise de décision incrémentale allant d'une simple authentification vocale ou visuelle jusqu'à une authentification bimodale de la signature online.

Sommaire

6.1 Introduction 93

6.2 Comportement autonome 93

6.3 Architecture proposée 94

6.3.1 Mécanisme de prise de décision incrémentale 95

6.3.2 Environnement de validation 96

6.4 Principales limites du système développé 98

6.1 Introduction

Les besoins en intelligence artificielle pour la résolution des problèmes liés à l'utilisation des systèmes informatiques n'ont cessé de croitre et de toucher une variété d'applications qui requièrent une autonomie de comportement, d'authentification et de communication ainsi qu'une adaptabilité avec les contraintes du milieu environnant.

Aussi et avec l'augmentation de la puissance des machine actuelles, il est désormais possible de fédérer l'ensemble de ses tâches à un personnage virtuel capable d'imiter les comportements intelligents et intuitifs de l'être humain, donnant ainsi à la machine un aspect humaniste et permettant ainsi d'accroître les performances des systèmes qui les utilisent.

C'est dans cette optique que nous avons décidé de doter notre système d'authentification avec un personnage virtuel capable de mettre en bonne condition les intrus et permettre ainsi une meilleure authentification de ces derniers.

Dans ce qui suit nous aborderons de façon générale les principales caractéristiques d'un personnage virtuel performant pouvant jouer un rôle primordial dans l'amélioration des performances de notre système d'authentification.

6.2 Comportement autonome

Le développement des personnages virtuels a connu un intérêt grandissant surtout avec le développement des applications tels que les jeux vidéo et interfaces homme machine. Bien qu'ils soient performants, ces derniers n'ont pas le libre choix de contrôler leurs actions. Par contre, et en ce qui concerne les applications temps réels, les personnages virtuels doivent à la base de certaines règles prédéfinies décider seules de l'action qu'il faudra entreprendre.

Il est à noter que l'autonomie peut être vue sur les trois volets suivants :

- ***Perception de l'environnement*** : C'est l'aptitude du personnage à distinguer les changements sonores et visuels au sein de l'environnement qu'il contrôle

- ***Prise de décision et adaptation*** : C'est l'évaluation de ce qui est perçu à travers un raisonnement et un choix approprié des actions à entreprendre. Cette évaluation peut ne pas être basée que sur ce qui est perçu, et peut prendre en considérations d'autres paramètres tels que l'intelligence, l'expérience passée ainsi que l'état émotionnel.

Plusieurs approches de prise de décision existent dans la littérature : Les premières approches étaient basées sur des raisonnements symboliques résolus avec des décisions logiques et des démonstrations de théorèmes qui ne se prêtent pas du tout à l'aspect temps réel [Project2006].

Afin de combler les lacunes des approches symboliques, de nouvelles approches réactives et mieux adaptées aux environnements dynamiques furent développées. Parmi ces approches on peut citer l'architecture de brooks [Broo2001] dans laquelle les comportements sont représentés par de simples structures IF-THEN ELSE [wool2009]. Nous avons aussi des approches qui utilisent les machines d'états pour lesquels les changements de conditions sur un état conduisent vers un autre état et des approches probabilistiques et floues [Cham2003].

- ***Contrôles des actions* :** Afin de donner au personnage virtuel un aspect naturel et intelligent, ce dernier doit être capable d'effectuer des actions visuelles qui peuvent être scindées en deux groupes : le premier groupe concerne les mouvements durant la conversation comme par exemple l'expression faciale, la gestuelle et les changements de posture. Le second groupe concerne les mouvements complexes comme par exemple : marcher ou prendre un objet. Plus le personnage et capable d'exécuter des mouvements riches et variés plus ce dernier se rapproche du réel et mieux il sera adopté par les utilisateurs.

6.3 Architecture proposée

En s'inspirant du processus de prise de décision complexe adopté par l'être humain pour authentifier une personne, une architecture multi Agents est en cours de développement. Cette dernière s'articule autour d'un module de prise de décision incrémentale capable d'interagir de façon souple et intelligente avec le milieu qu'il contrôle. Ce dernier reçoit en continu des informations des différents agents, et en fonction de ces derniers, procède à des actions appropriées visant à :

- *Autoriser une personne non enregistrée dans la base à s'enrôler (moyennant un mot de passe fourni)*

- *Enclencher l'opération d'authentification vocale et récupération d'un degré de similarité*

- *Enclencher l'opération d'authentification faciale et récupération d'un degré de similarité*

- *Effectuer la fusion bimodale (face/voix) et calcul du résultat d'authentification.*

- *Enclencher l'opération d'authentification par la signature dans le cas d'échec de la vérification bimodale.*

Le schéma d'interactivité entre les différents modules du système est présenté en *Figure 6.1*.

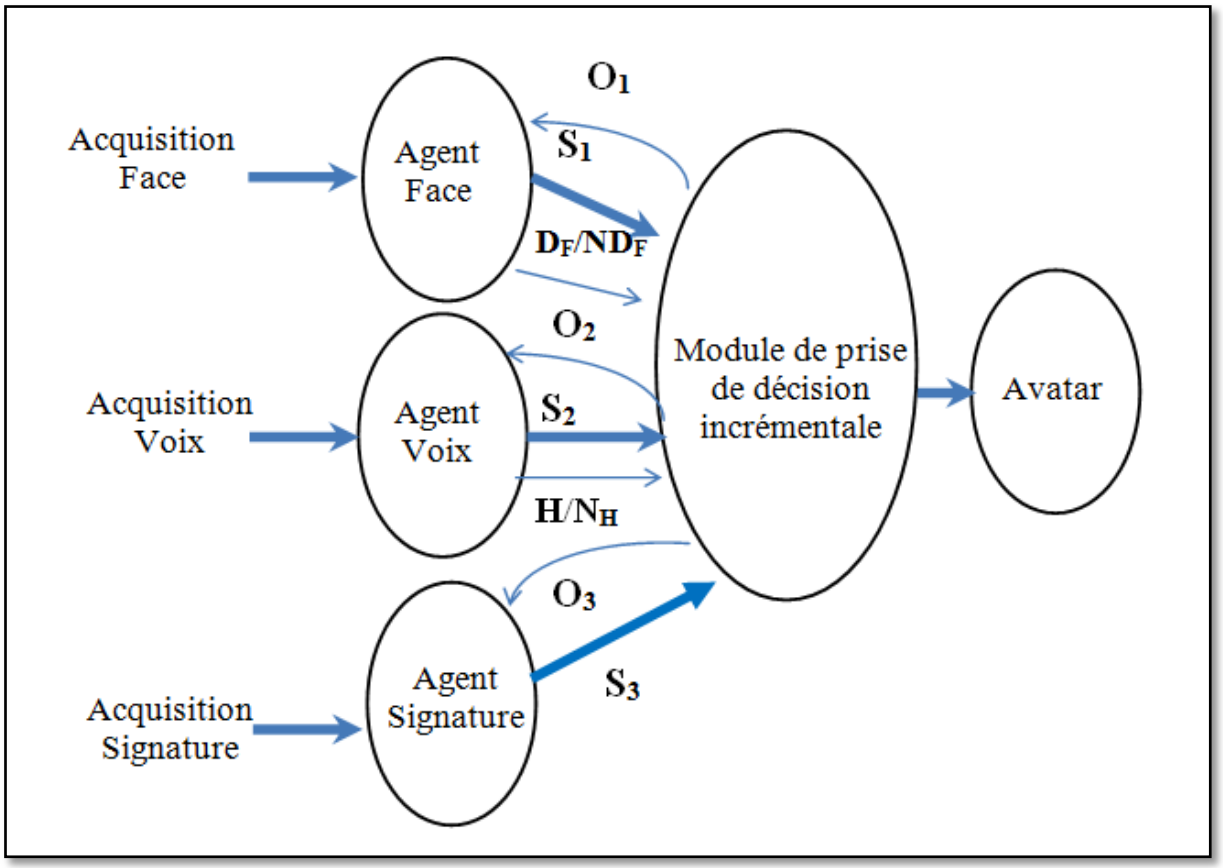


FIGURE 6.1 - Architecture proposée

D_F/ND_F : Détection du visage / Non détection du visage.

H/N_H: La voix humaine / la voix Non-humaine.

S_1, S_2 et S_3: Les scores de similarité.

O_1, O_2 et O_3: Ordres d'inscription/Authentification.

6.3.1 Mécanisme de prise de décision incrémentale

En s'inspirant de la démarche humaine pour authentifier une personne nous avons dégagé trois niveaux de prise de décision à savoir :

Un premier niveau enclenché suite à un changement sonore et/ou visuel au niveau de la scène sous surveillance.

Dans le cas où les conditions d'accessibilités ne sont pas trop élevées, une bonne authentification monomodale peut alors suffire pour l'acceptation de l'intrus. Dans le cas où une seule modalité ne permet pas d'authentifier la personne, on passe au deuxième niveau qui consiste à fusionner les résultats obtenus par les deux modalités (voix et face). En fin et dans le cas d'échec d'authentification on passe au niveau trois qui consiste à utiliser l'authentification bimodale de la signature.

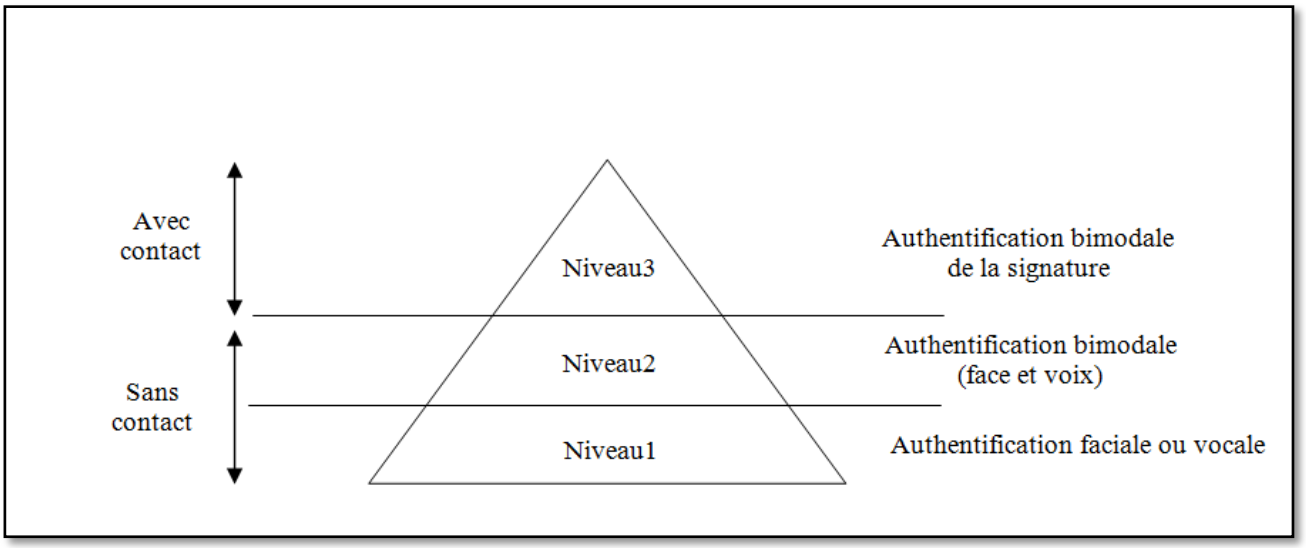


FIGURE 6.2 - Niveaux de prise de décision

6.3.2 Environnement de validation

La validation de l'architecture proposée rentre dans le cadre de travail de thèse d'un autre membre du laboratoire qui a choisi d'utiliser l'environnement JADE [Ferb1995] comme plateforme d'expérimentation des interactivités entre agents.

Jade plate-forme Java pour les systèmes multi-agents respectant le standard FIPA. Jade a été développée par l'université de Parme et C-SELT – centre de recherche télécom italien.

L'utilisation de cette plateforme, facilite la programmation d'un système multi agents, de plus, elle garantie la distributivité et la communication sur divers postes de travail sur le réseau. Cette plate forme propose une riche bibliothèque de modèles d'architectures d'agents modulaire. Chaque agent peut être représenté par un composant simple ou multiple qui gère l'interaction de l'agent avec son environnement.

La *Figure 6.3* présente quelques états du personnage virtuel développé en fonction des situations qui se présentent.

FIGURE 6.3 - Exemple d'états du personnage virtuel

La *Figure 6.4* présente l'interface de validation des scénarios d'interactivité entre agents.

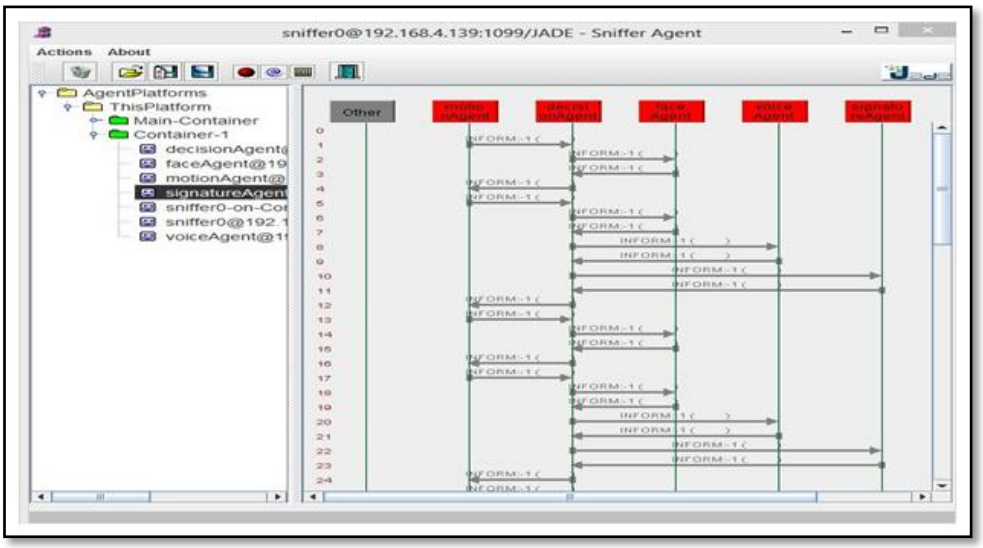


FIGURE 6.4 - Interface de validation des scénarios d'interactivité entre agents

6.4 Principales limites du système développé

Le système développé est capable d'interagir avec son milieu pour une meilleure mise en conditions des sujets à authentifier. Malheureusement cette mise en condition est sujette au bon vouloir de la personne à authentifier et qui dans certains cas, est dans l'incapacité de comprendre ce que le système exige d'elle. C'est le cas par exemple d'un sourd muet ou d'une personne ne comprenant pas la langue utilisée.

Au lieu de demander aux sujets à authentifier de s'adapter au système, c'est au système de s'adapter au sujets et ceci quel que soit les conditions dans lesquelles ils se trouvent. Il est donc fort nécessaire de travailler sur des mécanismes d'adaptation aux changements de contexte que d'imposer des contextes de travail idéaux. Cette nouvelle approche connue sous le nom de Concept Drift vise donc à doter les systèmes d'authentification de mécanismes d'adaptation inspirés de ceux de l'être humain.

Nous espérons dans le futur proche investir cette approche et montrer ses atouts dans le domaine de prise de décision en général et l'authentification biométrique en particulier.

Conclusion

Conclusion Générale

Dans ce travail de thèse nous avons présenté une expérience de construction d'un système d'authentification biométrique multimodale, destiné à travailler de façon autonome dans un milieu soumis aux contraintes de changement de contextes. L'interactivité avec le milieu est assurée par un personnage virtuel ayant un comportement inspiré de celui d'un être humain.

Afin de garantir une authentification robuste face aux attaques intentionnelles, nous avons proposé l'ajout de la modalité signature et renforcé cette dernière par une nouvelle approche d'authentification bimodale basée sur l'exploitation conjointe des informations issues de la signature et de la morphologie de la main. A cet effet, un nouveau descripteur fut développé et validé de façon online. En plus d'être efficace contre les attaques intentionnelles, la solution proposée est très économique car elle n'utilise qu'un seul capteur vidéo pour les besoins de l'acquisition. De plus, les traitements développés sont d'une complexité faible et ce prêtent bien à une implémentation matérielle pour un traitement en temps réel.

L'exploitation des trois modalités est assurée par un module de prise de décision incrémentale qui a pour rôle la conjugaison des modalités mises en jeu en vue d'une authentification souple et efficace des individus.

Il faut noter que les exigences en fiabilité et en autonomie nous ont poussés à travailler en groupe sur les deux volets modalités mises en œuvre et interactivité. Pour ce qui est du premier volet, la solution basée sur la combinaison des modalités (Face-voix et signature) nous a permis d'obtenir (comparativement avec ce qui existe sur le marché) un système d'authentification performant. Par contre, et pour ce qui est de l'interactivité du système avec son milieu, beaucoup de choses restent à faire pour atteindre l'autonomie désirée. En effet, le personnage virtuel développé présente actuellement beaucoup de limites surtout pour un fonctionnement online. L'architecture multi agents proposée et validés sous Jade est relativement simple, et Les scénarios proposés ne traitent que certains cas.

Un travail plus approfondi pour le traitement des cas de changement de contexte débouchera très certainement sur la thématique Concept Drift, qui a pour philosophie, la prise de décision au fur et à mesure de l'arrivée des données.

Aussi, et afin d'améliorer les performances du système, il s'avère indispensable d'inclure des capteurs intelligents capables d'intégrer une partie du traitement global, rendant le système plus léger et plus rapide.

Enfin, et bien qu'il ait permis la finalisation de quatre sujets de thèse de doctorats, ce projet est loin d'être achevé et reste demandeur de chercheurs pluridisciplinaire capables de s'impliquer dans cet objectif d'humanisation du processus d'authentification.

Références

A

[Abed2010] M. El-Abed, R.Giot, B.Hemery and C.Rosenberger, "A study of users' acceptance and satisfaction of biometric systems", In 44th IEEE International Carnahan Conference on Security Technology, San Jose, California, USA, 2010.

[Akro2010] S.Akrouf, A. Bouziane, A. H. Gharbi, M. Mostefai and Y. Chahir, "Towards an Intelligent Multimodal Biometric Identification System", International Journal of Computer and Electrical Engineering, 2010.

[Alla2009] L.Allano, " La biométrie mulimodale: Stratégie de fusion de scores et mesures de dépendance. Appliquées aux bases de personnes virtuelles", Thèse de doctorat,Institue national des télécommunication, 2009.

[Alon2005] F. Alonso-Fernandez, J. Fierrez-Aguilar, and J. Ortega-Garcia, "Sensor Interoperability and Fusion in Signature Verification: A Case Study using Tablet PC," Proc. Int. Workshop Biometric Recognit. Syst., Beijing, China, Oct. 22−23, 2005, pp. 180–187.

[Asma2012] K. Asma, M.Messaoud, B. Fateh, C.Youssef "Efficient Multimodal Biometric Database Construction and Protection Schemes" J. Electron Imaging (2012).

[Aliz2010] A. Alizadeh, T. Alizadeh, and Z. Daei, "Optimal Threshold Selection for Online Verification of Signature," Proc. Int. Multi-Conf. Eng. Comput. Sci. (IMECS), Kowloon, Hong Kong, Mar. 17–19, 2010, pp. 98−102.

[Alma2011] W. Almayyan et al.,"A multimodal biometric approach based on binary particle optimization," Research and Development in Intelligent Systems, pp. 139–152, Springer, London (2011).

B

[Bae1995] Y. J. Bae, M. C. Fairhurst, "Parallelism in dynamic time warping for automatic signature verification," in Proc. 3rd Int. Conf. Doc. Anal. Recog, IEEE Comput. Soc, Montreal, Canada vol. 1, 1995.

[Bail2003] E. B. Bailliére, S. Bengio, F. Bimbot, M. Hamouz, J. Kittler, J. Mariéthoz, J.Matas, K. Messer, V. Popovici, F Porée, B. Ruíz, and J-P. Thiran, "The BANCA database and evaluation protocol", In AVBPA, 2003.

[Bell1957] R. Bellman, "Dynamic Programming", Princeton University Press, 1957.

[Bene1990] J. A. Benediktsson, P. H. Swain and O.K. Ersoy,"Neural network approaches versus statistical methods in classification of multisource remote sensing data ", IEEE Trans. On Geoscience and Remote Sensing, 1990.

[Bhat2009] J. Bhatnagar, A. Kumar, "On estimating performance indices for biometric identifcation", Pattern Recognition, 2009.

[Bolm2003] D. Bolme, R. Beveridge, M. Teixeira, and B. Draper, "The CSU Face Identification Evaluation System: Its Purpose, Features and Structure", International Conference on Vision Systems, Graz, Austria Springer-Verlag, 2003.

[Boye2007] K. W. Boyer, V. Govindaraju, and N. K. Ratha, Eds, "Special issue on recent advances in biometric systems", IEEE Trans. Syst, Man, Cybern.B, Cybern, 2007,pp. 1091–1095.

[Bouz2013] A. Bouziane, Y. ChahirR,M. Molina and F. Jouen , "Unified Framework for Human behaviour recognition : An Approach using 3D Zernike momentsh", Neurocomputing journal , Elsevier, 2013.

[Bunk2002] H. Bunke, A. Kandel, "Hybrid methods in pattern recognition", Series in machine perception and artificial intelligence, USA, 2002.

[Brau1989] J.Brault, R.Plamondon, "How to Detect Problematic Signers for Automatic Signature Verification", Int Carnahan Conf on Security Technology, 1989.

[Brau1993] J. Brault, R. Plamondon, "A Complexity Measure of Handwritten Curves: Modeling of Dynamic Signature Forgery", IEEE Trans on Systems, Man, and Cybernetics, 1993.

[Broe1999] A. P. Broeders, A. G. V. Amelsvoort, "Lineup construction for forensic ear witness identification: A practical approach", International Conference in Phonetic Sciences, Leeds, 1999.

[Broe2004] Y. Bulatov, S. Jambawalikar, P. Kumar, , and S. Sethia, "Hand recognition using geometric classifiers," in 1st Int'l Conference on Biometric Authentication (ICBA), Hong Kong, China, July 2004, pp. 753–759.

[Baha2010] Bahareh. Aghili, Hamed.Sadjedi, "Personal Identification/Verification by Using Four Fingers", 3rd International Congress on Image and Signal Processing ,IEEE ,pp. 2619-2623, 2010.

[Buha2005] I. Buhan and P. Hartel,"The state of the art in abuse of biometrics," Technical Report TR-CTIT-05-41 Centre for Telematics and Information Technology, University of Twente (2005).

C

[Cher2009] F. Cherif, B. Hemery, R. Giot, M. Pasquet, and C. Rosenberger, "Performance evaluation of behavioral biometric systems", In Behavioral Biometrics for Human Identification: Intelligent Applications, 2009.

[Chik2012] R. Chikioui, A. Kebbeb, M. Mostefai, and "Dévelopement d'une architecture multi-agents pour une identification multimodale interactive", ICIEM'12 Inernational Conference on Industrial Engineering and Manufacturing. Batna University, Algeria, 2012.

[Cris2000] N. Cristianini, J-S. Taylor, "An Introduction to Support Vector Machines", Cambridge University Press, 2000.

[Chen2002] Y. Chen and X. Ding, "Online Signature Verification using Direction Sequence String Matching," Proc. SPIE 4875, 2ndInt. Conf. Imag. Graph., Hefei, China, July 16, 2002, pp. 744–749.

[Cova2005] N. Covavisaruch, P. Prateepamornkul, P. Ruchikachorn, P. Taksaphan, "Personal verification and identification using hand geometry," ECTI Transactions on Computer and Information Technology 1 (2) (2005) 134–139.

[Carl2014] Carlos M. Travieso, Jaime R. Ticay-Rivas , Juan C. Briceno , Marcos del Pozo-Banos , "Hand shape identification on multirange images" , Information Sciences,2014.

D

[Daug2004] J. Daugman, "Iris Recognition for Personal Identification", IEEE Transactions on circuits & systems for video technology, The Computer Laboratory, University of Cambridge, 2004.

[Daug2000] J. Daugman, "Mathematical Explanation of Iris Technologies", The Computer Laboratory, University of Cambridge, 2000.

[Dima1994] G. Dimauro, S. Impedovo, and G. Pirlo, "Component-Oriented Algorithms for Signature Verification", Int Journal of Pat Rec and Art, 1994.

[Duda2000] O. R. Duda, P. E. Hart, and D. G. Stork. "Pattern Classification" (2nd Edition).Wiley-Interscience, 2000.

E

[Egan1975] J. P. Egan, "Signal detection theory and ROC-analysis", by Academic Press, New York, 1975.

[Erns1971] R. H. Ernst, "Hand ID system", US Patent No.3576537, 1971.

[Erik2007] E. J. Erikson, "That voice sounds familiar: Factors in speaker recognition", Thèse de Doctorat, Umea University, 2007.

[Elmi2012] Y. Elmir et al.,"A multi-modal face and signature biometric authentication system using a max-of-scores based fusion,"Lect. Notes Comput.Sci.7667, 576–583 (2012).

F

[Find2005] L. J. Findley, W. C. Koller, "Handbook of Tremor Disorders", Taylor & Francis: New York, NY, USA, 2005.

[Fren2003] H. Feng and C. C. Wah, "Online signature verification using a new extreme points warping technique," Pattern Recognit. Lett. vol. 24, 2003.

[Fuen2002] M. Fuentes, S. Garcia-Salicetti, and B. Dorizzi, "On line signature verification: fusion of a Hidden Markov Model and a Neural Network via a Support Vector Machine", Proceeding of the 8th International Workshop on Frontiers in Handwriting Recognition Ontario, Canada, Aug. 6−8, 2002 .

[Fair1997] M.C. Fairhurst, "Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology," Eng. Electron. Commun. Eng. J., IEEE, vol. 9, no. 6, Dec. 1997, pp. 273–280.

G

[Gele1987] D.Gelernter, "Les nouvelles méthodes de programmation", Pour la science, 1987.

[Gait2005] GAITS: Global Analytic Information Technology Services, "Signature Recognition",2005.

[Gold1971] A. J. Goldstein, L. D. Harmon, and A. B. Lesk, "Identification of Human Faces", Proc. IEEE, 1971.

[Gorm2003] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication", In Proceedings of the IEEE, 2003.

[Goh2003] M.. Goh Kah Ong,Tee Connie, Andrew Teoh Beng Jin, David Ngo Chek Ling, "A single-sensor hand geometry and palm print verification system", Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications, Berkley, California , 2003 .

[Gupt1997] G. Gupta, R. C. Joyce, " A Study of Shape in Dynamic Handwritten Signature Verification", technical Report , Computer Science Dept, James Cook University of North Queensland, 1997.

[Gupt2006] G. K. Gupta,"The state of the art in the on-line handwritten signature verification," Clayton School of Information Technology, Monash University, Melbourne, Technical Report 200 (2006).

H

[Harr1958] W.Harrison, "Suspect Documents. Praeger Publishers", New York, 1958.

[Hast1992] T. Hastie, E. Kishon, M. Clark, and J. Fan, "A Model for Signature Verification", Rapport technique, AT&T Bell Laboratories, 1992.

[Herb1977] N. M. Herbst, C. N. Liu, "Automatic signature verification based on accelerometry", IBM J. Res. 1977.

[Hill2003] M.Hill, "ANAT2310: Eye Development", the University of New South Wales, 2003.

[Hilt1956] O. Hilton, "Scientific Examination of Documents", Callaghan and Co, Chicago, 1956.

[Huan1995] K. Huang, H. Yan, "On-line signature verification based on dynamic Segmentation and global and local matching", Optical Engineering, vol.34, no.12, 1995.

[Han2004] C.C. Han, "A hand-based personal authentication using a coarse-to-fine strategy", Image and Vision Computing, vol. 22, no. 11, pp. 909-918, 2004.

[Humm2006] A. Humm, J. Hennebert, and R. Ingold,"Scenario and survey of combined handwriting and speech modalities for user authentication,"in Proc. of the 6th Int. Conf. on Recent Advances in Soft Computing (RASC 2006), K. Sirlantzis, Ed., pp. 496–501 (2006).

[Hogb2010] G. Hogben, "Behavioural biometrics," Technical Report, ENISA (European Network and Information Security Agency) (2010).

I

[IBG2010] International Biometric Group, "Comparative market share by technologie", http // www.biometricgroup.com//, 2010.

[Impe2008] D. Impedovo, G. Pirlo, "Automatic Signature Verification: The State of the Art", IEEE Transactions on systems, Application and reviews, 2008.

[ISO2006] ISO/IEC 19795-1. Information technology, "Biometric performance testing and reporting", part 1: Principles and framework, 2006.

J

[Jain1999] A.K. Jain, S. Prabhakar, and S. Chen, "Combining multiple matchers for a high security fingerprint verification system", Pattern Recognition Letters, 1999.

[Jain2000] A. K. Jain, S. Pankanti, "Fingerprint Classification and Matching", Handbook for Image and Video Processing, A. Bovik (ed.), Academic Press, 2000.

[Jain2000] A. K. Jain, L. Hong, and S. Pankanti, "Biometrics Promising frontiers for emerging identification market", Technical report, Michigan State University, USA, 2000.

[Jain2002] A. K. Jain, A. A. Ross, "Learning user-specific parameters in a multibiometric system", In ICIP (1), 2002.

[Jain2002] A. K. Jain, F. D. Griess, and S. D. Cornell, "On-line Signature Verification", Pattern Recognition, 2002.

[Jain2004] A.K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition", IEEE Transactions on Circuits and Systems for Video Technology, 2004.

[Jain2008] A.K. Jain, F. Patrick, and A. Ross, "Handbook of biometrics", Michigan State University Dept. of Computer Science & Engineering Springer Science, 2008.

[Jaya2009] R. Jayadevan, R, K, Satish, M, P, Pradeep, "Dynamic Time Warping based static hand printed signature verification", Journal of Pattern Recognition Research1, 2009.

[Jeso2001] O. Jesorsky, K.J. Kirchberg, and R. W. Frischholz, "Robust Face Detection Using the Hausdorff Distance", In Josef Bigun and Fabrizio Smeraldi, editors, Audio and VideoBased Person Authentication, Sweden, 2001.

[Jing2007] Xiao-Yuan Jing, Yong-Fang Yao, David Zhang, Jing-Yu Yang, and Miao Li, "Face and palm print pixel level fusion and kernel DCV-RBF classifier for small sample biometric recognition", Pattern Recognition, 2007.

[Jaco1972] I.H. Jacoby, A.J. Giordano, W.H. Fioretti, Personnel identification apparatus, U.S. Patent no. 3648240, 1972.

[Jing2012] Jing-Ming Guo , Chih-Hsien Hsia, Yun-Fu Liu, Jie-Cyun Yu, Mei-Hui Chu, Thanh-Nam Le, "Contact-free hand geometry-based identification system", Expert Systems with Applications 39, pp. 11728–11736,2012

K

[Kame2008] N.S. Kamel, S. Sayeed, and G. A. Ellis, "Glove-Based Approach to Online Signature Verification". IEEE Transactions on Pattern Analysis and Machine Intelligence, 2008.

[Kash1997] R. S. Kashi, J. Hu, W. L. Nelson et W. Turin, " On-line Handwritten Signature Verification using Hidden Markov Model Features", Proceedings of International Conference on Document Analysis and Recognition, Germany, 1997.

[Kash1997] R. S. Kashi, J. Hu, W. L. Nelson, and W. Turin, "On-line handwritten signature verification using hidden Markov model features", in Proc. 4th Int. Conf. Doc. Anal. Recognit. (ICDAR-4), Ulm, Germany, 1997.

[Kash1998] R. S. Kashi, J. Hu, W. L. Nelson, and W. L. Turin, "A hidden Markov model approach to online handwritten signature verification",Int. J.Doc. Anal. Recognit. (IJDAR), vol. 1,1998.

[Kawa2002] M. Kawamoto, T. Hamamoto, and S. Hangai, "Improvement of on-line signature verification system robust to intersession variability", Lecture Notes in Computer Science, in Biometric Authentication, Germany: Springer-Verlag, 2002.

[Kiku2001] M. Kikuchi, N. Akamatsu, "Development of Speedy and High Sensitive Pen System for Writing Pressure and Writer Identification", Proceedings of the International Conference on Document Analysis and Recognition, 2001.

[Kirc2002] K. J. Kirchberg, O. Jesorsky, R. W. Frischholz, "Genetic Model Optimization for Hausdorff Distance-Based Face Localization", International Workshop on Biometric Authentication, Lecture Notes in Computer Science, Copenhagen, Denmark, 2002.

[Kitt1998] J. Kittler, M. Hatef, R. P. W. Duin, and Jiri Matas, "On combining classiffiers", IEEE Trans. Pattern Anal. Mach. Intell., 1998.

[Kuku2009] E. P. Kukula, C. R. Blomeke, S. K. Modi, and S. J. Elliott, " Effect of human biometric sensor interaction on fingerprint matching performance", image quality and minutiae count. International Journal of Computer Applications in Technology, 2009.

[Kuma2003] A. Kumar, D. C. M. Wong, H. C. Shen and A. K.Jain, "Personal Verification Using Palmprint and HandGeometry Biometric", Proc. of 4th Int'l Conf. on Audioand Video-Based Biometric Person Authentication (AVBPA), Guildford, UK, June 9-11, 2003, pp. 668-678.

L

[Lecc1999] V. Di Lecce, G. Dimauro, A. Guerriero, S. Impedovo, G. Pirlo, A. Salzo, and L. Sarcinella, "Selection of reference signatures for automatic signature verification", in Proc. 5th Int. Conf.Doc. Anal. Recognit. (ICDAR-5), Bangalore, India, 1999.

[Lecl1994] F. Leclerc, R. Plamondon, "Automatic Signature Verification", The State of the Art .1989-1993, Int Journal of Patt Rec and Art, 1994.

[Lee1996] L. L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems", IEEE Trans. Pattern Anal.Mach. Intell. (T-PAMI), vol. 18, 1996.

[Lejt2001] D. Z. Lejtman, S. E. George, "On-line handwritten signature verification using wavelets and back-propagation neural networks", Proceedings of the International Conference on Document Analysis and Recognition (ICDAR'01), 2001.

[Lero2004] J. Leroux, P. Lamadelaine, and B. Dorizzi, C.Guerrier, "La biométrie Techniques et usages", April, 2004.

[Lorr1999] G. Lorrette, "Handwriting Recognition or Reading ? Situation at the Dawn of the 3rd Millennium", Rennesl University, Advances in Handwriting Recognition, ed. Seong-Whan Lee (Singapore: World Scientific Publishing), 1999.

[Lyen1995] S. S. Iyengar, L. Prasad, and H. Min, "Advances in Distributed Sensor Technology ", Prentice Hall. (1995).

[Lei2005] H. Lei, S. Palla, and V. Govindaraju, "Mouse Based Signature Verification for Internet Based Transactions," Proc. IS&T/SPIE Symp. Electron. Imag. Sci. Technol. Electron. Imag. Vis., San Jose, CA, USA, Jan. 2005, pp. 153–160.107.

[Lesz2006] J.P. Leszczyska, "Online Signature Verification using Dynamic Time Warping with Positional Coordinates," Proc. SPIE, Photonics Applications in Astronomy, Communications, Industry, and High-Energy Physics Experiments, Oct. 12, 2006, pp. 634724-1–634724-08.

[Lip2012] C.C. Lip and D.A. Ramli,"Comparative study on feature, score and decision level fusion schemes for robust multi biometric systems,"in Frontiers in Computer Education, Vol. 133, pp. 941–948, Springer, Berlin Heidelberg (2012).

M

[Mahi2008] J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo, "Biometric authentication", Encyclopedia of Information Science and Technology, 2008.

[Malc2009] Jo. Malcolmson, Q.Quiet, " What is security culture?", IEEE Conference publication, 2009.

[Malt2003] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Handbook of Fingerprin Recognition", Springer-Verlag, 2003.

[Mart1997] R. Martens, L. Claesen, "Dynamic Programming Optimisation for On-line Signature Verification", Proceedings of the International Conference on Document Analysis and Recognition, 1997.

[Mart1998] R. Martens, L. Claesen, "Incorporating local consistency information into the online signature verification process, " International Journal on Document Analysis and Recognition, 1998.

[Mauc1965] A. J. Mauceri, "Feasibility Studies of Personal Identification by Signature Verification", Report, Space and Information System Division, North American Aviation Co., Anaheim, USA, 1965.

[Mill1971] R.P. Miller, Finger dimension comparison identification system, U.S. Patent no. 3576538, 1971.

[Mill1994] B. Miller, "Vital Signs of Identity", IEEE Spectrum, vol. 31, no. 2, Feb. 1994, pp. 22–30.

[Moha1999] N. Mohankrishnan, W. Lee, and M. Paulik, "A performance evaluation of a new signature verification algorithm using realistic forgeries", Proceedings of the International Conference on Image Processing, 1999.

[Mont1999] J. J. MONTOIS, " Gestion des processus industriels temps réel", Edition Ellipses ,1999.

[Muni2003] M. E. Munich and P. Perona, "Visual Identification By Signature Tracking", IEEE Transaction on Patern Analysis And Machine Intelligence, 2003.

[Marc2014] Marcia V. P. do Nascimento, et. al. "Comparative study of learning algorithms for recognition by hand geometry", IEEE International Conference on Systems, Man, and Cybernetics, pp. 423-428,2014.

[Migu2007] Miguel A. Ferrer, Aythami Morales, Carlos M. Travieso, Jesws B. Alonso, "Low Cost Multimodal Biometric identification System Based on Hand Geometry, Palm and Finger Print Texture", IEEE, pp. 52-58, 2007.

[Migu2008] Miguel Adan, Antonio Adan, Andre´s S. Va´zquez, Roberto Torres, "Biometric verification/identification based on hands natural layout", Image and
Vision Computing 26, pp. 451–465, 2008.

N

[Naka2011] I. Nakanishi et al., "DWT Domain On-Line Signature Verification," Chapter 9 in Biometrics, J. Yang, Ed, 2011.

[Nalw1997] V. Nalwa, "Automatic on-line Signature Verification," Proc. IEEE 85(2), 215–239 (1997).

[Nist2005] NIST Speech Group, "NIST Speaker Recognition Evaluations", 25 April 2005, 23 June 2005.

[Newh2000] E. Newham, "Survey: Signature Verification Technologies," in Signature Verification, Amsterdam, The Netherlands: Elsevier, 2000, pp. 8–10.

[Namb2004]A. M. Namboodiri et al.,"Skilled forgery detection in on-line signatures: a multimodal approach,"Lect. Notes Comput. Sci.3072, 505–511 (2004).

O

[Ogle1995] J. Oglesby, "What's in a number? Moving beyond the equal error rate", Speech communication, 1995.

[Orte2003] J. G. Ortega, J. A. Fierrez, D. Simon. J. Gonzalez, and M. Faudez, "MCYT Baseline Corpus: A Bimodal Biometric Database", IEE Proceedings on Vision, Image and Signal Processing, Special Issue on Biometrics on the Internet, 2003.

[Osbo1929] A.Osborn, "Questioned Documents", Boyd Printing Co, Albany, NY, 2nd Edition, 1929.

[Oden2003] C. Oden, A. Ercil, and B. Buke, "Hand recognition using implicit polynomials and geometric features,"Pattern Recognition Letters, vol. 24, no. 13, pp. 2145–2152, 2003.

[Oule2013] A. Oulefki et al., "New online signature acquisition system,"J. Electron Imaging 22(1), 010501 (2013).

P

[Paal1995] P. Paalanen, J. Ilonen, J-K. Kamarainen, and H. Kalviainen. " Feature representation and discrimination based on Gaussian mixture model probability densities ", Research Report, Lappeenranta University of Technology, 1995.

[Perr2002] F. Perronnin, J.L. Dugelay, "Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo", Revue Traitement du Signal, 2002.

[Piar2012] J. Pearson, M. L. Platt, "Dynamic decision making in the brain", Nature neuroscience, 2012.

[Pirl1993] G. Pirlo, "Algorithms for signature verification: Fundamentals in Handwriting Recognition", Chateau de Bonas, France, 1993.

[Plam1989] R. Plamondon, G. Lorette, "Automatic Signature Verification and Writer Identification", The State of the Art. Pattern Recognition, 1989.

[Plam1995] R. Plamondon, "A kinematic theory of rapid human movements: Part I: Movement representation and generation", Biol. Cybern. vol. 72, no. 4, Jan. 1995, pp. 295–320.

[Plam1997] R .Plamondon, "A kinematic theory of rapid human movements: Part III: kinetic outcomes", Biol. Cybern. 1995.

[Plam2000] R. Plamondon and S.N. Srihari, "Online and On-line Handwriting Recognition: A Comprehensive Survey," IEEE Trans. on Pattern Anal. Mach. Intel., vol. 22, no. 1, Jan. 2000,pp. 63–84.

[Prab2003] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns", IEEE Security & Privacy. 2003.

[Prab2007] S. Prabhakar et al., "Special Issue on Biometrics: Progress and Directions," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, Apr. 2007, pp. 513–516.

[Priv1986] G. Privat, "Architectures spécialisées de circuits VLSI", pour le traitement numérique du signal ", Thèse de Doctorat, ENST, 1986.

[Purz1963] S. Pruzansky, "Pattern-matching procedure for automatic talker recognition", JASA (26) 1963.

[Pave2004] N. Pavešic, S. Ribaric, D. Ribaric, Personal authentication using hand-geometry and palmprint features: the state of the art, in: Proceedings of the Workshop on Biometrics at ICPR04, Cambridge, UK, 2004.

[Poin2011] A. Poinsot, F. Yang, and V. Brost, "Palmprint and face score level fusion: hardware implementation of a contactless small sample biometric system,"Opt. Eng.50(2), 027002 (2011).

[Park2013] G. Park and S. Kim,"Hand biometric recognition based on fused hand geometry and vascular patterns,"Sensors13, 2895–2910 (2013).

R

[Rabb1991] M. Rabbani, P. W.Jones , "Digital Image Compression Techniques", Edition-4, 1991.

[Rayn1994] D. A. Reynolds. "Speaker identification and verification using gaussian mixture speaker models". Speech Comm, 1994.

[Rayn2000] D. A. Reynolds, L.P. Heck, "Automatic Speaker Recognition: Recent Progress, Current Applications and Future Trends", 19 February 2000. Presented at the AAAS 2000 Meeting: Humans, Computers and Speech Symposium, 2000.

[Rayn2005] D. A. Reynolds, "Automated Speaker Recognition: Current Trends and Future Direction", Biometrics Colloquium 17 June 2005.

[Rhee2001] T. H. Rhee, S. J. Cho, and J. H. Kim, " On-line signature verification using model guided segmentation and discriminative feature selection for skilled forgeries", Proceedings of the International Conference on Document Analysis and Recognition, 2001.

[Roco2007] E. Rocon, M. Manto, J. Pons, S. Camut, J. M. Belda, "Mechanical suppression of essential tremor", Cerebellum 2007.

[Ross1999] A. Ross, A. K. Jain, and S. Pankanti, "A Hand Geometry-Based Verification System", Conference on Audio- and Video-based Biometric Person Authentication, Washington D.C, 1999.

[Reil2000] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, "Biometric identification through hand geometry measurements," IEEE Trans. Pattern Anal. and Mach. Intell., vol. 22, no. 10, pp. 1168–1171, 2000.

[Ross2003] A. Ross, A.K. Jain, and Engineering, "Information fusion in biometrics", Department of Computer Science, Michigan State University, Pattern Recognition, Letters, 2003.

[Ross2006] A. Ross, K. Nandakumar, and A. K. Jain, "Handbook of Multibiometrics", Springer, 2006.

[Rigo1998] G. Rigoll and A. Kosmala, "A Systematic Comparison Between Online and Offline Methods for Signature Verification with Hidden Markov Models," Proc. 14th Int. Conf. Pattern Recognit. Brisbane, Australia, Aug. 16−20, 1998, pp. 1755–1757.

[Rong2012] Rong-Xiang Hua,, Wei Jia, David Zhang c, Jie Gui, Liang-Tu ,"Hand shape recognition based on coherent distance shape contexts", Pattern Recognition45,pp.3348–3359,2012.

[Rafa2013] Rafael M. Luque-Baena , David Elizondo, Ezequiel López-Rubio, Esteban J. Palomo , Tim Watson, "Assessment of Geometric Features for Individual Identification and Verification in Biometric Hand Systems", Expert Systems with Applications 40 ,pp. 3580–3594,2013.

S

[Sako1978] H. Sakoe, S. Chiba, "Dynamic programming algorithm optimization for spoken word recognition," IEEE Transactions on Acoustics, Speech, and Signal Processing, 1978.

[Sher1992] R. Sherman, "Biometric Futures. Computers & Security", 1992.

[Siro1987] L. Sirovich and M. Kirby, "A Low-Dimensional Procedure for the Characterization of Human Faces", J. Optical Soc. Am. A, 1987.

[Shim2004] H. Shimizu et al., "An Electrical Pen for Signature Verification using a TwoDimensional Optical Angle Sensor," Sensors and Actuators, vol. 111, no. 2−3, Mar. 2004, pp. 216–221.

[Shef2015] Shefali Sharma, Shiv Ram Dubey , Satish Kumar Singh,Rajiv Saxena , Rajat Kumar Singh, "Identity verification using shape and geometry of human hands" , Expert Systems with Applications 42,pp. 821–832, 2015

(SVC 2004) http://www.cs.ust.hk/svc2004/download.html

T

[Turk1999] M. A. Turk, A. P. Pentland, "Face Recognition Using Eigenfaces", Proc. IEEE, 1991.

[Tolb1999] S. Tolba, "Glove Signature: A Virtual Reality Based System for Dynamic Signature Verification," Digit. Signal Process., vol. 9, no. 4, Oct. 1999, pp. 241–266.

U

[Urec1999] O. Ureche and R. Plamondon, "Document Transport, Transfer, and Exchange, Security and Commercial Aspects," Proc. 5th Int. Conf. Document Anal. Recognit. (ICDAR '99), Bangalore, India, Sep. 20−22 1999, pp. 585–588.

V

[Vapn1995] V. N. Vapnik, "The nature of statistical learning theory". Springer- Verlag New York, Inc., New York, NY, USA, 1995.

[Viel2006a] C. Vielhauer and J. Dittmann, "Biometrics for User Authentication" in Encyclopedia of Multimedia," Boca Raton, FL, USA: Springer US, Berlin, 2008, pp. 48-55.

[Viel2006b] C. Vielhauer, "Biometric User Authentication for IT Security From Fundamentals to Handwriting," New York, NY, USA: Springer Science+Business Media, Inc., 2006.

[Varc2007] Varchol , D. Levický, " Using of Hand Geometry in Biometric Security Systems", Radioengineering , vol. 16, no. 4,pp.82-87,DEC 2007.

W

[Waym2005] J. Wayman, "Biometric Systems Technology Design and Performance Evaluation", London, 2005.

[West1998] B. Westmoreland, M. Lemp, and R. Snell, "Clinical Anatomy of the Eye 2nd ed", Oxford: Blackwell Science Inc, 1998.

[Wick 2004] L. K. Wickramasinghe and L.D. Alahakoon , "A Novel Adaptive Decision Making Agent Architecture Inspired by Human Behavior and Brain Study Models", Proceedings of the Fourth International Conference on Hybrid Intelligent Systems (HIS'04), 2004.

[Wiro2005] M.Wirotius, "Authentification par signature manuscrite sur support nomad ", Thèse de doctorat,Université François Rabelais Tours, 2005.

[Wirt1997] B. Wirtz, "Average prototypes for stroke-based signature verification", Proceedings of the International Conference on Document Analysis and Recognition, 1997.

[Wisk1997] L.Wiskott , J.M.Fellous, N.Kruger , and V.Malsburg, "Face recognition by elastic bunch graph matching.," IEEE Trans. Pattern Anal. Mach. Intell, 1997.

[Woo2006] N. Woo, H. Kim, "Multiple-biometric fusion methods using support vector machine and kernel discriminate". In 6th International Conference on Recent Advances in Soft Computing (RASC 2006), 2006.

[Wood2003] J. D. Woodward, Jr. N. M. Orlans, and P. T. Higgins, "Biometrics", New York: McGraw Hill Osborne, 2003.

[Wood1997] K. Woods, W. P. Kegelmeyer Jr, K. Bowoyer, "Combination of multiple classifiers using local accuracy estimation", IEEE Transactions on pattern analysis & machine intelligence, 1997.

[Wije2001] W.S. Wijesoma et al., "Online Handwritten Signature Verification for Electronic Commerce over the Internet," Proc. 1st Asia-Pacific Conf., Maebashi, Japan, Oct. 23–26, 2001, pp. 227–236.

[Wong2002] L. Wong, P. Shi, Peg-free hand geometry recognition using hierarchical geometry and shape matching, in: Proceedings of the IAPR Workshop on Machine Vision Applications, Nara, Japan, 2002, pp. 281–284.

Y

[Yang1995] L. Yang, B. K. Widjaja, and R. Prasad, "Application of Hidden Markov Models for signature verification", Pattern Recognition, 1995.

[Yamp2008] R.V. Yampolskiy and V. Govindaraju, "Behavioural biometrics: a survey and classification," Int. J. Biometrics, vol. 1, no. 1, June 2008, pp. 81−113.

[Yoru2006] E. Yoruk, E. Konukoglu, B. Sankur, J. Darbon, Shape-based hand recognition, IEEE Transactions on Image Processing 15 (7) (2006) 1803–1815.

[Yoru2006] E. Yoruk, H. Dutagaci, B. Sankur, Hand biometrics, Image and Vision Computing 24 (2006) 483–497.

Z

[Zhao1996] P. Zhao, A. Higashi, and Y. Sato, "On-line signature verification by adaptively weighted DP matching", IEICE Transactions on Information and Systems, no.5, 1996.

[Zogh2009] M. Zoghi and V. Abolghasemi, "Persian signature verification using improved dynamic time warping-based segmentation and multivariate autoregressive modeling," Proc. IEEE 15th workshop of Statistical Signal Processing (SSP'09), Cardiff, pp. 329–332 (2009).