

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

UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU



FACULTE DU GENIE ELECTRIQUE ET D'INFORMATIQUE
DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes De MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**

Filière : **Informatique**

Spécialité : **Réseau, Mobilité et Systèmes
Embarqués**

Présenté par

Mohamed YOUNSI

Younes MEDJTOUH

Thème

Développement d'un système biométrique pour la reconnaissance de visages, basé sur les ondelettes.

Mémoire soutenu publiquement le 28/09/ 2016 devant le jury composé de :

Présidente : M^{elle} AIT-ADDA Samia

Encadreur : M^{me} FERHAOUI-CHERIFI Chafia

Examineur : M^{elle} YESLI Yasmine

Examineur : M^{me} BOUSNINA Lila

Remerciements :

Nous tenons tout d'abord à remercier DIEU, tout puissant, de nous avoir donné la force de réaliser ce projet tout au long de cette année. Nous adressons nos plus vifs remerciements à notre promotrice C.FERHAOUI-CHERIFI pour la confiance qu'elle nous a accordée en nous proposant ce sujet, pour ses précieux conseils, pour ses remarques pertinentes, ainsi que son encouragement sans lequel ce travail n'aurait jamais vu le jour.

Nos remerciements vont également à tous les enseignants de l'université Mouloud Mammeri (département informatique) pour le savoir qu'ils nous ont permis d'acquérir et pour l'esprit d'analyse qu'ils nous ont permis de développer. Nous présentons nos gratitude au président et aux membres du jury qui nous font l'honneur de juger notre travail.

Nous remercions tous ceux, qui de près ou de loin, nous ont apporté leur contribution pour la réalisation de ce travail.

Dédicaces

Je dédie ce travail à :

Ma très chère mère celle qui m'a aidée du mieux qu'elle pouvait pour réussir, celle qui a toujours été derrière moi pour me guider dans la bonne direction,

A mon père qui m'a toujours soutenu dans tout ce que j'ai entrepris, qui m'a accompagné et encouragé tout au long du parcours de mes études.

A mes sœur Sarah, Yousra et mes très chers frères Abdarahmane, Ilyane qui ont toujours été là pour me soutenir durant mon parcours,

Je dédie, aussi, ce travail à tous les membres de ma famille, grands et petits, pour leur soutien, et particulièrement à mon binôme Mohamed avec qui j'ai eu le bonheur de partager des moments de travail et d'amitié.

Younes.

Dédicaces

Je dédie ce travail à :

Ma très chère mère celle qui m'a aidée du mieux qu'elle pouvait pour réussir, celle qui a toujours été derrière moi pour me guider dans la bonne direction,

A mon père qui m'a toujours soutenu dans tout ce que j'ai entrepris, qui m'a accompagné et encouragé tout au long du parcours de mes études.

A ma sœur Souad, et mon très cher frère TAHAR, qui ont toujours été là pour me soutenir durant mon parcours,

Je dédie, aussi, ce travail à tous les membres de ma famille, grands et petits, pour leur soutien, et particulièrement à mon binôme YOUNES avec qui j'ai eu le bonheur de partager des moments de travail et d'amitié.

Mohamed.

Résumé :

Afin de répondre aux besoins en sécurité qui deviennent de plus en plus importantes avec les avancements économiques, le développement des systèmes de contrôle d'accès physiques ou biométriques ne cessent de croître.

Plusieurs modalités biométriques peuvent être utilisées et chacune présente un intérêt particulier suivant l'application visée.

Dans le cadre de notre travail, nous nous sommes intéressées à l'étude de la modalité visage en développant un système de reconnaissance facial basé sur l'approche DWT, afin d'analyser et profiter des avantages de la technique implémentée dans un même système.

Le développement a été fait en passant par trois étapes à savoir : l'acquisition des images, l'extraction des paramètres et enfin leurs modélisations.

D'une part, l'extraction des paramètres est réalisée par la transformation DWT (transformée en ondelette discrète) qui a prouvé sa robustesse.

D'autre part, après l'extraction des paramètres, la modélisation de ces derniers est réalisée par l'approche PCA (Analyse en composantes principales) (Eigen face).

En effet, la notion d'orthogonalité fait des DWT une approche plus robuste du point de vue complexité, et d'optimalité (temps de réponse).

L'évaluation de l'approche DWT a été faite à travers plusieurs tests comparatifs par rapport aux systèmes : DWT-cos, DWT-euc, DWT-mahco, DWT-ctb sur la base de données notamment ORL. L'ensemble des résultats a mis en évidence l'intérêt que cette approche apporte en termes d'efficacité et de robustesse face aux variations d'éclairage et les expressions du visage.

Mots clefs : modalité biométrique, système de reconnaissance facial, ondelettes, analyse en composante principale(PCA), transformée en ondelette discrète, distance (euclidienne, cosine, mahalanobis, ...).

Abstract:

Security needs are becoming increasingly important with the economic advancements. That is why the development of biometric systems based on different modalities continue to grow.

In our work, we are interested in the study of the face modality by developing a face recognition system based on DWT approach to analyze the benefits of both techniques implemented on the same system.

The development can be divided into three main parts namely: image acquisition features extraction and finally features modeling.

On the one hand, extraction of parameters is performed by the DWT (Discrete Wavelet Transform) that has proven its robustness.

Moreover, after the extraction of parameters, modeling of these is performed by the PCA approach (Principal Component Analysis) (Eigen face).

Indeed, the notion of orthogonal DWT made a more robust approach from the point of view complexity and optimality (response time).

The evaluation of the DWT approach was made through several comparative tests over systems: DWT-cos, DWT-euc, DWT-mahco, DWT-ctb on the database ORL. The overall results showed the interest that this approach brings in terms of efficiency and robustness against lighting changes and facial expressions.

Keywords: biometric modality, facial recognition system, wavelets, principal component analysis (PCA), Discrete Wavelet Transform, distance (Euclidean, cosine, mahalanobis ...).

Sommaire :

Introduction générale :	1
-------------------------------	---

PARTIE I : BIOMETRIE ET RECONNAISSANCE DE VISAGES.

Chapitre I : BIOMETRIE : CONCEPT, APPLICATIONS ET ENJEUX

I.1	Introduction :	3
I.2	Modalités biométriques :	3
I.2.1	Modalités biométriques physiques :	3
I.2.1.1	Empreintes digitales (finger-scan) :	3
I.2.1.2	Géométrie de la main / du doigt (hand-scan) :	4
I.2.1.3	Iris (iris-scan) :	5
I.2.1.4	Rétine (retina-scan) :	6
I.2.1.5	Visage (facial-scan) :	6
I.2.1.6	Système et configuration des veines (vein pattern-scan) :	7
I.2.2	Modalités comportementales :	7
I.2.2.1	Dynamique des frappes au clavier (keystroke-scan) :	7
I.2.2.2	Reconnaissance vocale (voice-scan) :	8
I.2.2.3	Dynamique des signatures (signature-scan) :	8
I.2.3	Modalités biologiques :	8
I.2.3.1	Odeur :	8
I.2.3.2	Acide Désoxyribose Nucléique (ADN) :	9
I.2.4	Multi modalité :	9
I.3	Les caractéristiques d'une modalité biométrique :	10
I.4	Les systèmes biométriques :	10
I.4.1	Module d'apprentissage :	11
I.4.2	Module de reconnaissance :	11
I.4.3	Module d'adaptation :	12
I.5	Évaluation de performance :	12
I.5.1	Évaluation de l'identification :	13
I.5.2	Évaluation de la vérification :	13
I.6	Applications des systèmes biométriques :	15
I.7	La place de la reconnaissance faciale parmi les autres techniques biométriques :	15
I.8	La part de marche par technologie :	16

I.9	Les enjeux pour de la biométrie de demain :	16
I.10	Conclusion :	17

Chapitre II : SYSTEME DE RECONNAISSANCE DE VISAGES.

II.1.	Introduction:	19
II.2.	La place de la reconnaissance de visage parmi les autres modalités :	19
II.3.	Le système de reconnaissance de visages :	20
II.3.1.	Acquisition de l'image :	21
II.3.2.	Prétraitement :	21
II.3.3.	Extraction des paramètres et Classification :	21
II.3.4.	L'apprentissage :	21
II.3.5.	Décision :	21
II.4.	État de l'art des méthodes de reconnaissances de visages :	22
II.4.1.	Méthodes globales :	22
II.4.2.	Méthodes locales :	25
II.4.3.	Méthodes hybrides :	26
II.5.	Principales difficultés de la reconnaissance de visage :	26
II.6.	Performances d'un système de reconnaissances de visage :	29
II.6.1.	Performance d'un système d'identification :	29
II.6.2.	Performance d'un système de vérification :	29
II.8.	Conclusion :	31

PARTIE II : EXTRACTION DES PARAMETRES ET CLASSIFICATION.

Chapitre III : APPLICATION DES ONDELETTES POUR L'EXTRACTION DES PARAMETRES.

III.1.	Introduction:	32
III.2.	Pourquoi les ondelettes(contribution) :	32
III.3.	Qu'est-ce qu'une ondelette :	33
III.4.	Les principales caractéristiques d'une ondelette mère :	33
III.4.1.	L'admissibilité :	34
III.4.2.	Localisation :	34
III.4.3.	L'oscillation :	34
III.4.4.	La translation et la dilatation :	34
III.5.	La transformée en ondelettes :	35
III.5.1.	La transformation en ondelettes continues :	36

III.5.2.	La transformation en ondelettes discrètes :	37
III.6.	Propriétés des ondelettes :	37
III.6.1.	Sélectivité en fréquence :	37
III.6.2.	Similarité :	37
III.6.3.	Symétrie :	37
III.6.4.	Orthogonalité :	38
III.6.5.	Régularité :	38
III.6.6.	Nombre de moments nuls :	38
III.6.7.	Facteur d'échelle minimal :	38
III.6.8.	Relation entre fréquence et échelle :	38
III.7.	Présentation des ondelettes multidimensionnelles :	38
III.8.	Famille d'ondelettes :	39
III.8.1.	Ondelette de Haar :	41
III.8.2.	Ondelettes de Daubechies :	41
III.8.3.	Ondelettes de Symlets :	45
III.8.4.	Ondelettes de Coiflets :	47
III.9.	Les avantages de la transformée en ondelettes :	49
III.10.	Conclusion :	50

Chapitre IV : MODELISATION DES PARAMETRES ET DECISION.

IV.1.	Introduction :	51
IV.2.	Réduction de dimensionnalité :	51
IV.2.1.	Définition d'analyse en composantes principale :	52
IV.2.2.	Modélisation par la méthode PCA :	53
IV.2.3.	Représentation de l'image du visage dans l'espace des Eigen faces :	55
IV.2.4.	Décision :	55
IV.2.5.	Seuil :	55
IV.3.	Différentes distances utiliser pour la classification [50] :	56
IV.3.1.	Distances Euclidiennes :	56
1.	Distance City Block (L1) :	56
2.	Distance Euclidienne (L2) :	56
IV.3.2.	Distance Cosine (cosinus) :	56
IV.3.3.	Distances dans l'Espace de Mahalanobis :	57
1.	De l'espace des images à l'espace de Mahalanobis :	57
2.	Mahalanobis L1 (MahL1) :	57
3.	Mahalanobis L2 (MahL2) :	57
4.	Cosinus de Mahalanobis (MahCosine) :	58

IV.4.	Conclusion :	58
-------	--------------	----

Chapitre V : CONCEPTION ET REALISATION.

V.1.	Introduction :	59
V.2.	Conception :	59
V.2.1.	Les acteurs du système :	59
1.	L'Administrateur :	59
1.	L'individu Test :	59
V.2.2.	Les diagrammes de cas d'utilisation du système :	59
1.	Description du diagramme de contexte « Apprentissage » :	60
2.	Description du cas d'utilisation « Identification » :	61
3.	Description du cas d'utilisation « Authentification » :	61
4.	Description du cas d'utilisation « test des performances » :	62
V.2.3.	Architecture et fonctionnement du système :	63
1.	L'Apprentissage :	63
2.	Découpage modulaire :	64
3.	Module d'acquisition :	65
4.	Module de prétraitement :	65
5.	Module d'extraction des paramètres :	65
6.	Module de modélisation :	66
7.	Module de sauvegarde :	67
V.2.4.	Phase de reconnaissances (Test et décision) :	67
1.	Identification :	67
2.	Authentification :	68
V.2.5.	Calcul des performances du système :	70
1.	Mode identification :	70
2.	Mode authentification :	70
3.	Test de performances :	73
V.2.6.	Schéma conceptuel de la base de données :	73
V.3.	Réalisation :	74
V.3.1.	Introduction :	74
V.3.2.	Outils de développement :	74
1.	Matlab :	74

V.3.3.	Structures de données et implémentation :	74
1.	Acquisition :	75
2.	Extraction de paramètre :	75
3.	Identification :	75
4.	Authentification :	76
V.3.4.	Présentation de l'application :	76
1.	Interface apprentissage :	77
2.	Tests de performance :	77
3.	Interface identification :	78
4.	Interface authentification :	78
V.3.5.	Conclusion :	79

Chapitre VI : TEST ET EVALUATION DES RESULTATS.

VI.1.	Introduction :	80
VI.2.	La Base de données ORL :	80
VI.3.	Protocole d'évaluation :	81
VI.4.	Résultats des Tests :	82
VI.4.1.	Mode identification (vecteurs caractéristiques concaténés) :	82
VI.4.2.	Mode authentification (vérification) :	83
VI.4.3.	Mode identification (vecteur image détaillé) :	85
VI.4.4.	Mode authentification (vérification) :	86
VI.5.	Comparaison entre l'utilisation de vecteur image détaillée et le vecteur concaténé :	88
VI.6.	Comparaison entre les quatre distances de classification :	89
VI.7.	Temps d'exécution :	90
VI.8.	CONCLUSION :	91

Conclusion et Perspectives :	92
------------------------------	----

Liste des figures:

Chapitre I :

Figure I.1 : Empreinte digitale.	4
Figure I.2 : Géométrie de la main.....	5
Figure I.3 : L'iris.	5
Figure I.5 : La rétine.	6
Figure I.6 : Visage en plusieurs images faites de nuances de gris "Eigen face".	7
Figure I.7 : Architecture d'un système de reconnaissance biométrique.....	11
Figure I.8 : Distributions des taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système biométrique.	13
Figure I.9 : Courbe ROC.	14
Figure I.10 : Part de marche de chaque technologie.	16

Chapitre II

Figure II.1 : Le processus de reconnaissance de visage.....	20
Figure II.2 : Classification des méthodes principales utilisées dans la reconnaissance de visage.....	22
Figure II.3 : Image moyenne et les 15èmes eigenfaces.	24
Figure II.4 : Exemple de six classes utilisant LDA.....	25
Figure II.5 : Exemple de variation d'éclairage.	27
Figure II.6 : exemple de variation de pose.	27
Figure II.7 : Exemples de variation d'expressions faciale.	28
Figure II.8 : Seuil de décision et taux d'erreurs.	30
Figure II.9 : Relation entre FAR et FRR.	30

Chapitre III:

Figure III.1 : Exemples d'ondelette $\phi(t)$. (D'après Charles, 2003).	33
Figure III.2 : Quelques exemples d'ondelettes 1D.....	34
Figure III.3 : Exemple d'une ondelette dilatée et translatée.....	35
Figure III.4 : Exemple d'une ondelette 2D.....	39
Figure III.5 : Filtre h_0 de Haar.	41
Figure III.6 : La fonction d'échelle et la fonction d'ondelette de haar.	42
Figure III.7 : Les ondelettes de Daubechies.....	43
Figure III.8 : Ondelettes de Daubechies (<i>db4</i>).....	44

Figure III.9 : Ondelettes de Daubechies (<i>db8</i>).	44
Figure III.10 : Les ondelettes de symlets.	45
Figure III.11 : Ondelettes de Symlets (<i>sym4</i>).	46
Figure III.12 : Ondelettes de Symlets (<i>sym8</i>).	47
Figure III.13 : Les ondelettes de coiflets.	48
Figure III.14 : Ondelettes de Coiflet (<i>coif3</i>).	48
Figure III.15 : Ondelettes de Coiflet (<i>coif5</i>).	49

Chapitre IV :

Figure IV.1 : Exemple d'Eigenfaces (MIT 2012).	53
Figure IV.2 : Transformation de la matrice image $N * N$ en vecteur $N2 * 1$.	54
Figure IV.3 : Les deux vecteurs m et n dans l'espace de Mahalanobis.	58

Chapitre V :

Figure V.1 : Diagramme de contexte du système.	60
Figure V.2 : Description du cas d'apprentissage pour un nouveau client.	61
Figure V.3 : Description du cas d'apprentissage d'un client.	61
Figure V.4 : Description du cas d'authentification d'un client.	62
Figure V.5 : Description du cas d'authentification d'un client.	62
Figure V.6 : Diagramme d'activité du système.	63
Figure V.7 : Diagramme de séquence Apprentissage.	64
Figure V.8 : Représentation modulaire de la phase d'apprentissage.	64
Figure V.9 : Processus d'acquisition.	65
Figure V.10 : Représentation de l'étape prétraitement.	65
Figure V.11 : Algorithme DWT.	66
Figure V.12 : Algorithme PCA.	66
Figure V.13 : Diagramme de séquence du cas Identification.	67
Figure V.14 : Description du procédé d'identification.	68
Figure V.15 : Description du procédé d'authentification.	69
Figure V.16 : Description du procédé d'authentification.	70
Figure V.17 : Calcul du TID.	70
Figure V.18 : calcul du Seuil.	71
Figure V.19 : calcul du score client.	71
Figure V.20 : calcul du score imposteur.	71
Figure V.21 : calcul du FAR.	72
Figure V.22 : calcul du FRR.	72

Figure V.23 : Diagramme de séquence du cas test de performances.....	73
Figure V.24 : Schéma conceptuel de la base de données.	73
Figure V.25 : variables et fonction de la partie acquisition.....	75
Figure V.26 : variables et fonction de la partie apprentissage.....	75
Figure V.27 : variables et fonction de la partie identification.....	76
Figure V.28 : variables et fonction de la partie authentification.	76
Figure V.29 : interface apprentissage.	77
Figure V.30 : interface tests de performance.	77
Figure V.31 : interface identification.....	78
Figure V.32 : interface authentification	78

Chapitre VI :

Figure VI.1 : Exemple de visages de la base ORL.....	81
Figure VI.2 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance.....	83
Figure VI.3 : Variation du taux de fausse acceptation FAR (%) en fonction de type d'ondelette et la distance ...	84
Figure VI.4 : Variation du taux de faux rejet FAR (%) en fonction de type d'ondelette et la distance.....	85
Figure VI.5 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance	86
Figure VI.6 : Variation du taux de fausse acceptation FAR (%) en fonction de type d'ondelette et la distance ...	87
Figure VI.7 : Variation du taux de faux rejet FRR (%) en fonction de type d'ondelette et la distance	88
Figure VI.8 : vecteur image détaillé Vs vecteur concaténé TID (%).....	89
Figure VI.9 : comparaison des quatre distances de classification en TID (%).....	90

Liste de tableaux:

Chapitre I :

Tableaux I.1 : Avantages et inconvénients de la Reconnaissance de Visage.	16
--	----

Chapitre II

Tableau II.1 : Avantages et Inconvénients de la Reconnaissance de visage.	20
--	----

Chapitre III:

Tableau III.1 : Familles d'ondelettes.	40
Tableau III.2 : Les propriétés principales des ondelettes.	40

Chapitre VI :

Tableau VI.1 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance	82
Tableau VI.2 : Variation du taux fausse acceptation FAR (%) en fonction de type d'ondelette et la distance	83
Tableau VI.3 : Variation du taux de faux rejet FRR (%) en fonction de type d'ondelette et la distance	84
Tableau VI.4 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance	85
Tableau VI.5 : Variation du taux de fausse acceptation FAR (%) en fonction de type d'ondelette et la distance	86
Tableau VI.6 : Variation du taux de faux rejet FRR (%) en fonction de type d'ondelette et la distance	87
Tableau VI.7 : vecteur image détaillé Vs vecteur concaténé TID (%)	88
Tableau VI.8 : comparaison des quatre distances de classification en TID (%)	89
Tableau VI.9 : temps d'exécutions en mode identification et authentification en (seconds)	90

La croissance internationale des communications, les déplacements des individus, les transactions financières et les accès au service implique le besoin de s'assurer de l'identité des individus. Il y a donc un intérêt grandissant pour les systèmes d'identification et d'authentification. Leur dénominateur commun, est le besoin d'un moyen simple, pratique et fiable pour vérifier l'identité d'une personne sans l'assistance d'une autre personne.

Aujourd'hui, l'identification automatique de l'homme basée sur la reconnaissance automatique des particularités physiques est en phase de transformer notre identité. Fini les lieux et dates de naissances, le nom des parents place à la détection du contour de la main, de l'empreinte ou de l'iris, rétine, ..., c'est ce qu'on appelle l'identification biométrique. Les différentes caractéristiques physiques nommées modalités biométriques sont à la fois sûres et faciles d'accès pour les usagers, elles pallient aux risques d'oubli et de vol des cartes ou des codes personnels. Toutefois, plusieurs contraintes dues à l'ergonomie et l'acceptabilité sont liées à certaines modalités. En effet, si la reconnaissance d'iris ou la rétine sont généralement mal perçues par le public, il existe d'autres modalités, moins intrusives, comme la reconnaissance automatique du locuteur ou du visage. Cette dernière modalité, présente l'avantage d'être naturelle, tout en apportant un niveau de sécurité suffisant pour un grand nombre d'applications, mais qui peut tout de même être sérieusement affectée lors d'une utilisation dans des `` environnements difficiles``.

Les ondelettes, comme nouvel outil mathématique notable, se sont imposées dans de divers domaines d'application. Par leur capacité extraordinaire de concentration de l'énergie et par leur pouvoir fascinant de détection d'irrégularités. L'analyse par ondelettes ne se limite plus à l'image telle qu'elle nous apparaît, mais permet l'étude des objets présents dans l'image à différentes échelles, elle permet de réduire la redondance pour améliorer la compression d'une image, elle peut également extraire les informations importantes (texture, contours, etc.) contenues dans une image et aussi de réduire le bruit contenu dans l'image.

C'est dans ce cadre que se place notre projet de fin d'études, qui a pour objectif la proposition d'un système de reconnaissance de visage basé sur une technique globale les ondelettes, qui se veut être fiable et adaptée à un environnement présentant des variabilités de luminance, de pose, expression de visage et présence ou absence des composants structurel. Il est nécessaire de travailler à tous les niveaux du système (détection, extraction des caractéristiques et reconnaissance) en apportant des contributions pertinentes à différents points de la chaîne de traitement. Nous on s'est base sur l'extraction des caractéristiques et de la reconnaissance en utilisant les ondelettes qui nous permettent d'extraire les donnes pertinentes d'une image puis les projeter dans un espace de vecteurs propres dans le but de réduire leur dimension et ce en utilisant la méthode dite analyse des composantes principales ACP.

Pour la partie reconnaissances on a opter pour plusieurs méthodes de classification par mesure de similarité a noté la distance euclidienne, cosine, mahalonobis et ctb.

Nous avons choisi d'articuler notre étude autour de six chapitres principaux. Le premier chapitre est consacré à la présentation générale de la biométrie concept et enjeux. Il décrit tout d'abord le principe de fonctionnement des systèmes biométriques puis définit les outils

utilisés pour évaluer leurs performances. Ensuite, la place de la reconnaissance faciale parmi les autres techniques biométriques est analysée. A travers ce chapitre, nous voulons positionner le problème de la reconnaissance faciale et présenter ses enjeux et intérêts par rapport aux autres techniques. Nous étudions également les principales composantes d'un système de reconnaissance faciale, notamment la détection, l'extraction de caractéristiques et la reconnaissance. Enfin, nous mettons en lumière les difficultés rencontrées par les systèmes de reconnaissance de visage.

Dans le second chapitre une analyse détaillée des différentes techniques développées au cours de ces dernières années dans les domaines de la détection de visage et de la reconnaissance 2D est présentée.

Dans le troisième chapitre nous présentons les ondelettes. Leur principe de fonctionnement et fondement mathématique ainsi que l'avantage apporté par les ondelettes pour la communauté scientifique.

Dans le quatrième chapitre nous présentons la modélisation des paramètres et décision notamment la méthode ACP et les différentes distances utilise pour la classification.

Dans le cinquième chapitre nous présentons la phase de conception et réalisation du système les cas d'utilisation de notre système ainsi que toutes les méthodes utilise pour réaliser notre système.

Dans le dernier chapitre nous présentons les test et résultat obtenue après réalisation et exécution de notre système toutes en donnant une synthèse de notre travail.

Enfin, la conclusion générale résumera nos contributions et donnera quelques perspectives sur les travaux futurs.

PARTIE I :

BIOMETRIE ET RECONNAISSANCE DE VISAGES.

Chapitre I :

BIOMETRIE : CONCEPT, APPLICATIONS ET ENJEUX.

I.1 Introduction :

La biométrie est une technique globale visant à établir l'identité d'une personne en mesurant une de ses caractéristiques physiques (humaine) préalablement enregistrée : physiologique, comportementale, biologique [1]. Il peut y avoir plusieurs types de caractéristiques physiques, les unes plus fiables que d'autres, mais toutes doivent être infalsifiables et uniques pour pouvoir être représentatives d'un et un seul individu. D'autre part, comme nous allons le voir, les caractéristiques physiques sont loin d'être si parfaites et si précises, et l'on atteint très vite des limites pour ces techniques.

Les techniques basées sur la biométrie jouissent à l'heure actuelle d'un engouement général favorisé par un phénomène de mode, principalement véhiculé par les films au cinéma et à la télévision. Ainsi, il n'est pas rare de voir des scanners rétinien avec de superbes lasers rouges, des lecteurs d'empreintes digitales avec de très jolis voyants -clignotants-, etc.... tout cela représentant le summum de la technologie du contrôle d'accès. Or, les techniques de biométrie sont belles et bien en train de se répandre dans notre vie quotidienne, et ce tout en gardant une image quelque peu trompeuse.

Ce mémoire ne se veut pas exhaustif sur un sujet aussi vaste que la biométrie, mais il a tout de même pour vocation de donner quelques bases indispensables pour les lecteurs.

I.2 Modalités biométriques :

Les modalités biométriques sont les caractéristiques humaines physiologiques, comportementales ou biologiques.

I.2.1 Modalités biométriques physiques :

Il existe plusieurs caractéristiques physiques qui se révèlent être uniques pour un individu, et il existe également pour chacune d'entre elles plusieurs façons de les mesurer :

I.2.1.1 Empreintes digitales (finger-scan) :

La donnée de base dans le cas des empreintes digitales [1] est le dessin représenté par les crêtes et sillons de l'épiderme. Ce dessin est unique et différent pour chaque individu. En pratique, il est quasiment impossible d'utiliser toutes les informations fournies par ce dessin (car trop nombreuses pour chaque individu), on préférera donc en extraire les caractéristiques principales telles que les bifurcations de crêtes, les "îles", les lignes qui disparaissent, etc... Une empreinte complète contient en moyenne une centaine de ces points caractéristiques (les "minuties"). Si l'on considère la zone réellement scannée, on peut extraire environ 40 de ces points. Pourtant, là encore, les produits proposés sur le marché ne se basent que sur une quinzaine de ces points (12 au minimum vis-à-vis de la loi), voire moins pour beaucoup d'entre eux (jusqu'à 8 minimum).



Figure I.1. Empreinte digitale.

Les techniques utilisées pour la mesure sont diverses : capteurs optiques (caméras CCD/CMOS), capteurs ultrasoniques, capteurs de champ électrique, de capacité, de température...

Ces capteurs sont souvent doublés d'une mesure visant à établir la validité de l'échantillon soumis (autrement dit, qu'il s'agit bien d'un doigt) : mesure de la constante diélectrique relative de l'échantillon, sa conductivité, les battements de cœur, la pression sanguine, voire une mesure de l'empreinte sous l'épiderme...

I.2.1.2 Géométrie de la main / du doigt (hand-scan) :

Ce type de mesure biométrique est l'un des plus répandus, notamment aux Etats Unis. Cela consiste à mesurer plusieurs caractéristiques [1] de la main (jusqu'à 90) tel que la forme de la main, longueur et largeur des doigts, formes des articulations, longueurs inter-articulations, etc... La technologie associée à cela est principalement de l'imagerie infrarouge ; d'une façon générale, le système présente des FAR (False Acceptation Rate, voir plus bas) assez élevés, surtout entre personnes de la même famille ou bien encore des jumeaux.

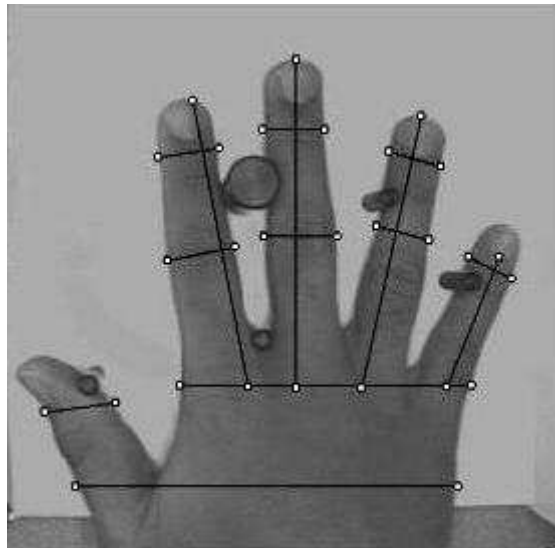


Figure 1.2. Géométrie de la main.

I.2.1.3 Iris (iris-scan):

En ce qui concerne l'iris, l'individu se place en face du capteur (caméra CCD/CMOS) qui scanne son iris. Celui-ci représente quelque chose de très intéressant pour la biométrie car il est à la fois toujours différent (même entre jumeaux, entre l'œil gauche et le droit, etc....), indépendant du code génétique de l'individu, et très difficilement falsifiable. En effet, l'iris présente une quasi-infinité de points caractéristiques (que certains comparent en nombre à ceux de l'ADN), qui ne varient pratiquement pas pendant la vie d'une personne contrairement à *la couleur de l'iris* qui, elle, peut changer. Mais cela n'a aucune influence car les images d'iris obtenues par les capteurs sont en noir et blanc. Le seul problème de cette technique est lié à la mesure en elle-même, qui peut être source d'erreurs ou de problèmes. Ainsi, on peut quasiment dire que le nombre de problèmes rencontrés lors de cette mesure augmente proportionnellement avec la distance entre l'œil et la caméra.

D'autres problèmes se posent à cause des reflets (nécessité d'avoir un éclairage restreint et maîtrisé), et lors de la détection de faux yeux (photos) et autres fraudes. Pour ces dernières, on peut faire appel à certaines caractéristiques dynamiques de l'œil qui prouveront son authenticité : réactivité de la pupille (dilatation/rétraction) par rapport à la quantité de lumière, étude de l'iris dans l'infrarouge et l'ultraviolet, etc...



Figure 1.4. L'iris.

I.2.1.4 Rétine (retina-scan):

Cette mesure biométrique est plus ancienne que celle utilisant l'iris, mais elle a été moins bien acceptée par le public et les utilisateurs, sans doute à cause de son caractère trop contraignant : la mesure doit s'effectuer à très faible distance du capteur (quelques centimètres), qui effectue ensuite un balayage de la rétine. Il est physiquement impossible d'effectuer une mesure rétinienne à une distance de 30cm ou plus sur un sujet mobile comme on peut le voir dans certains films. Cette méthode requiert des sujets coopératifs et entraînés.

Pourtant cette technique semble être tout aussi fiable que celle de l'iris ; elle se base sur le fait que le schéma et le dessin formé par les vaisseaux sanguins de la rétine (la paroi interne et opposée de l'œil) est unique pour chaque individu, différent entre jumeaux et assez stable durant la vie de la personne. La mesure peut ainsi fournir jusqu'à 400 points caractéristique du sujet, que l'on peut comparer aux 30 à 40 points fournis par une empreinte digitale ! En conclusion, la mesure rétinienne est la plus difficile à utiliser mais également la plus dure à contrefaire.

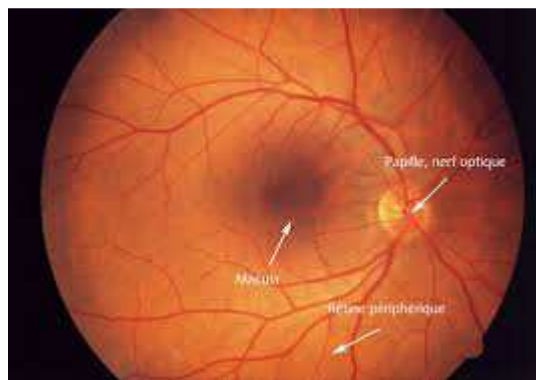
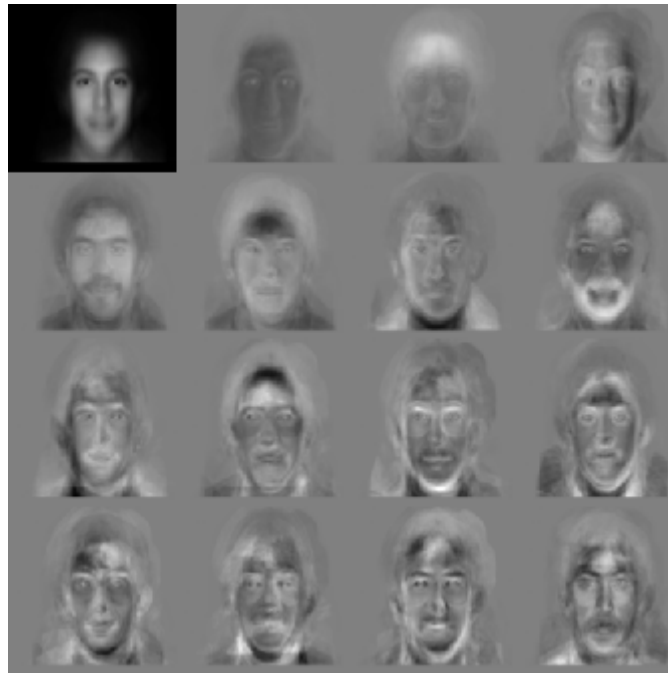


Figure I.5. La rétine.

I.2.1.5 Visage (facial-scan):

Il s'agit ici de faire une photographie plus ou moins évoluée pour en extraire un ensemble de facteurs qui se veulent propres à chaque individu [1]. Ces facteurs sont choisis pour leur forte invariabilité et concernent des zones du visage tel que le haut des joues, les coins de la bouche, etc.... on évitera d'autre part les types de coiffures, les zones occupées par des cheveux en général ou toute zone sujette à modification durant la vie de la personne. Il existe plusieurs variantes de la technologie de reconnaissance du visage.



Source : MIT Face Recognition Demo Page

Figure I.6. Visage en plusieurs images faites de nuances de gris "Eigenface".

La plupart des systèmes d'identification du visage utilisent du matériel standard, un ordinateur et une caméra pour capturer l'image.

I.2.1.6 Système et configuration des veines (vein pattern-scan):

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

I.2.2 Modalités comportementales :

Outre les caractéristiques physiques, un individu possède également plusieurs éléments liés à son comportement qui lui sont propres :

I.2.2.1 Dynamique des frappes au clavier (keystroke-scan):

La dynamique de la frappe au clavier est propre à chaque individu. Il s'agit en quelque sorte de la graphologie des temps modernes car nous écrivons plus souvent avec un clavier qu'avec un stylo. Cette technique repose sur les particularités de chaque individu lorsqu'il frappe sur un clavier, en particulier, la force et le rythme avec laquelle il frappe.

Cette technique biométrique est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à imiter. Lors de la mise en place de cette technique, il est demandé à l'utilisateur de saisir son mot de passe une dizaine de fois de suite. A l'aide d'un algorithme qui exploite le

temps d'appui sur chaque touche et le temps entre chaque touche [34], la dizaine de saisie est moyennée pour construire un profil de frappe de l'utilisateur qui servira de référence aux accès. En suivant la même approche, la saisie du mot de passe donné sera couplée à un profil de frappe qui sera comparé au profil de référence. Le droit d'accès est alors accordé en fonction du niveau de ressemblance de ce profil avec la référence. Suivant le degré de filtrage qu'un administrateur aura défini, cet accès sera plus ou moins difficile.

En l'état actuel des techniques, cette modalité biométrique peut difficilement être regardée comme une technique de haute sécurité, mais plus comme une technique de substitution à un code pour ouvrir un appareil électronique.

I.2.2.2 Reconnaissance vocale (voice-scan):

Les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux. Ils ne sont en général pas imitables.

I.2.2.3 Dynamique des signatures (signature-scan):

Ce type de biométrie est à l'heure actuelle peu utilisé mais ses défenseurs espèrent l'imposer assez rapidement pour des applications spécifiques (documents électroniques, rapports, contrats...). Le procédé est habituellement combiné à une palette graphique (ou équivalent) munie d'un stylo. Ce dispositif va mesurer plusieurs caractéristiques lors de la signature, tel que la vitesse, l'ordre des frappes, la pression et les accélérations, le temps total, etc... Bref tout ce qui peut permettre d'identifier une personne de la façon la plus sûre possible quand on utilise une donnée aussi changeante que la signature.

I.2.3 Modalités biologiques :

Il s'agit des techniques d'identification à partir des caractéristiques internes de chaque individu, telles que l'odeur, le sang, la salive, l'urine et l'ADN. Ici, nous allons uniquement parler de l'odeur et de l'ADN qui sont des techniques émergentes et en plein développement.

I.2.3.1 Odeur :

L'odeur corporelle provient d'un mélange complexe de substances chimiques. Le parfum naturel du corps se compose du sébum (notre propre huile essentielle), de la sueur, de l'activité des bactéries sur notre peau et des hormones que contiennent le sébum et la sueur.

En 1999, *CNR-Australia(Computer-News-Reseller)* évoquait dans un article de presse [20] les travaux entrepris par la société anglaise *Mastiff-Electronics* situé à Hampshire, sous le nom de code SCENTINEL, pour le développement d'un système biométrique d'identification d'individu s'appuyant sur l'odeur corporelle de la personne. A ce jour, même si aucun résultat ou information n'a été publié sur la technologie étudiée au cours de ce projet, le potentiel et la faisabilité d'un tel système ne peuvent être remis en cause quand on connaît la capacité des chiens pisteurs à identifier un individu parmi 6 milliards à partir de leur odeur corporelle.

I.2.3.2 Acide Désoxyribose Nucléique (ADN) :

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire. L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'Acide Désoxyribonucléique (ADN), constituant essentiel des chromosomes du noyau cellulaire. Le profil génétique, aujourd'hui couramment utilisé pour des identifications judiciaires, fut introduit officiellement pour la première fois dans une affaire criminelle en 1986 par l'universitaire anglais Alec Jeffreys [21], [22].

Selon les techniques d'analyse de l'ADN, l'identification est plus ou moins performante et/ou intrusive. L'identification d'un individu par analyse de son ADN s'avère complexe, coûteuse et lente à réaliser compte tenu des nombreuses manipulations biologiques (amplification + électrophorèse). Ceci explique qu'il n'existe toujours pas de solution technologique au grand-public qui permette de réaliser automatiquement cette analyse, d'autant plus qu'elle nécessite un prélèvement d'échantillon (sang, salive, sperme, cheveux, urine, peau, dents, etc.) qui rend cette technique très intrusive.

I.2.4 Multi modalité :

Bien que de nos jours il existe des techniques biométriques extrêmement fiables telles que la reconnaissance de la rétine ou de l'iris, elles sont coûteuses et, en général, mal acceptées par le grand public et ne peuvent donc être réservées qu'à des applications de très haute sécurité. Pour les autres applications, des techniques telles que la reconnaissance du visage ou de la voix sont très bien acceptées par les utilisateurs mais ont des performances encore trop peu satisfaisantes pour être déployées dans des conditions réelles [8]. Afin d'améliorer la sécurité des systèmes précédents, une première solution consiste à intégrer la biométrie avec l'identification basée sur une connaissance ou une possession. Cette méthode permet d'améliorer la sécurité du système, mais elle possède les faiblesses inhérentes à l'identification basée sur une connaissance ou une possession. La multi modalité est une alternative qui permet d'améliorer de manière systématique la performance d'un système biométrique [9]. Par performance, nous entendons à la fois la précision du système mais aussi son efficacité, plus particulièrement en mode identification [10]. En effet, des classificateurs différents font en général des erreurs différentes, et il est possible de tirer parti de cette complémentarité afin d'améliorer la performance globale du système. Nous exposerons d'abord les différentes formes de multi modalité possibles, puis les bases de données multimodales existantes, et enfin, les moyens de fusionner les informations obtenues par les différents classificateurs.

I.3 Les caractéristiques d'une modalité biométrique :

Pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle répond aux critères suivants :

- **Universalité** : Chaque personne doit présenter cette caractéristique.
- **Caractère distinctif** : La caractéristique doit être suffisamment différente chez deux personnes.
- **Permanence** : La caractéristique doit être suffisamment immuable pendant une période donnée.
- **Perceptibilité** : La caractéristique doit pouvoir être mesurée quantitativement.

Il faut prendre en compte plusieurs autres facteurs pour savoir si l'on doit utiliser un système de reconnaissance biométrique des personnes, notamment :

- **La performance** : Fiabilité et rapidité de reconnaissance du système ; ressources requises pour obtenir la fiabilité et la rapidité de reconnaissance voulues ; facteurs opérationnels et environnementaux qui influent sur la fiabilité et la rapidité du système.
- **L'acceptabilité** : Mesure dans laquelle les gens sont disposés à accepter l'utilisation d'une technologie de reconnaissance biométrique à des fins d'identification.
- **La facilité de contournement** : Facilité avec laquelle le système peut être induit en erreur par des méthodes frauduleuses.

I.4 Les systèmes biométriques :

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individu, en amenant un ensemble de caractéristiques à partir des données acquises lors d'apprentissage et en comparant ces caractéristiques lors de reconnaissance. Les systèmes biométriques permettent de reconnaître une personne (ou d'authentifier son identité) dont l'identité a préalablement été enregistrée dans une base de données (de N personnes « autorisées »). Les termes généraux d'*authentification* ou de *reconnaissance* et l'*identification* sont deux processus bien différents.

Il existe toujours au moins deux modules dans un système biométrique : le module d'apprentissage et celui de reconnaissance [7], [2]. Le troisième module (facultatif) est le module d'adaptation. Pendant l'apprentissage, le système va acquérir une ou plusieurs mesures biométriques qui serviront à construire un modèle de l'individu. Ce modèle de

référence servira de point de comparaison lors de la reconnaissance. Le modèle pourra être réévalué après chaque utilisation grâce au module d'adaptation.

I.4.1 Module d'apprentissage :

Au cours de l'apprentissage, la caractéristique biométrique est tout d'abord mesurée grâce à un capteur ; on parle d'acquisition ou de capture. En général, cette capture n'est pas directement stockée et des transformations lui sont appliquées. En effet, le signal contient de l'information inutile à la reconnaissance et seuls les paramètres pertinents sont extraits. Le modèle est une représentation compacte du signal qui permet de faciliter la phase de reconnaissance, mais aussi de diminuer la quantité de données à stocker. Il est à noter que la qualité du capteur peut grandement influencer les performances du système. Meilleure est la qualité du système d'acquisition, moins il y aura de pré- traitements à effectuer pour extraire les paramètres du signal.

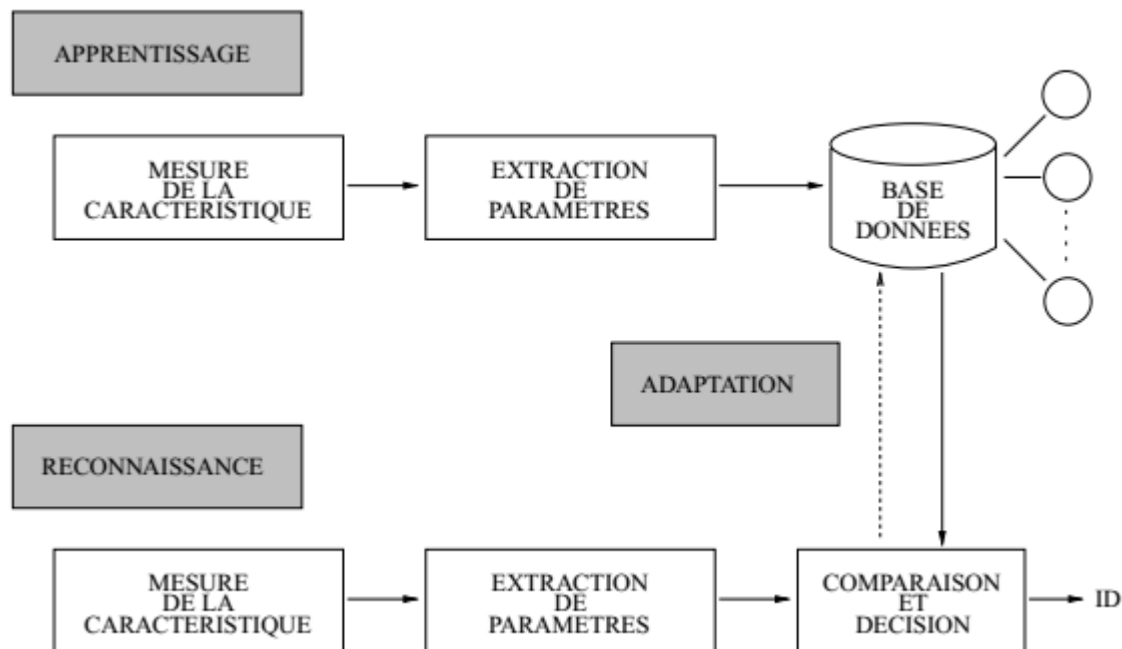


Figure I.7 : – Architecture d'un système de reconnaissance biométrique.

Cependant, les capteurs de qualité sont en général coûteux et leur utilisation est donc limitée à des applications de haute sécurité pour un public restreint. Le modèle peut être stocké dans une base de données comme représenté sur la figure 1 ou sur une carte de type carte à puce.

I.4.2 Module de reconnaissance :

Au cours de la reconnaissance, la caractéristique biométrique est mesurée et un ensemble de paramètres est extrait comme lors de l'apprentissage. Le capteur utilisé doit avoir des propriétés aussi proches que possibles du capteur utilisé durant la phase d'apprentissage. Si les deux capteurs ont des propriétés trop différentes, il faudra en général appliquer une série de prétraitements supplémentaires pour limiter la dégradation des performances. La suite de la reconnaissance sera différente suivant le mode opératoire du système : identification ou vérification. En mode identification, le système doit deviner l'identité de la personne. Il répond donc à une question de type : « Qui suis-je ? ». Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données (problème de type 1 : n). En général, lorsque l'on parle d'identification, on suppose que le problème est fermé, c'est-à-dire que toute personne qui utilise le système possède un modèle dans la base de données. En mode vérification, le système doit répondre à une question de type : « Suis-je bien la personne que je prétends être ? ». L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposée. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (problème de type 1 :1). En mode vérification, on parle de problème ouvert puisque l'on suppose qu'un individu qui n'a pas de modèle dans la base de données (imposteur) peut chercher à être reconnu. Identification et vérification sont donc deux problèmes différents. L'identification peut-être une tâche redoutable lorsque la base de données contient des milliers, voire des millions d'identités, tout particulièrement lorsqu'il existe des contraintes de type « temps réel » sur le système. Ces difficultés sont analogues à celles que connaissent par exemple les systèmes d'indexation de documents multimédia.

I.4.3 Module d'adaptation :

Pendant la phase d'apprentissage, le système biométrique ne capture souvent que quelques instances d'un même attribut afin de limiter la gêne pour l'utilisateur. Il est donc difficile de construire un modèle assez général capable de décrire toutes les variations possibles de cet attribut. De plus, les caractéristiques de cette biométrie ainsi que ses conditions d'acquisition peuvent varier. L'adaptation est donc nécessaire pour maintenir voire améliorer la performance d'un système utilisation après utilisation. L'adaptation peut se faire en mode supervisé ou non-supervisé mais le second mode est de loin le plus utile en pratique. Si un utilisateur est identifié par le module de reconnaissance, les paramètres extraits du signal serviront alors à ré-estimer son modèle. En général, le taux d'adaptation dépend du degré de confiance du module de reconnaissance dans l'identité de l'utilisateur. Bien entendu, l'adaptation non-supervisée peut poser problème en cas d'erreurs du module de reconnaissance. L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix [3] [4].

I.5 Évaluation de performance :

La performance d'un système d'identification peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque locuteur. Nous nous concentrerons dans cette section sur le premier aspect. Comme nous l'avons vu précédemment, l'identification et la vérification sont des modes opératoires différents. Elles nécessitent donc des mesures de précision différentes que nous étudierons dans les deux sous-sections suivantes. Le lecteur pourra aussi se référer à l'article de P. Phillips et al. Sur l'évaluation des systèmes biométriques [5].

I.5.1 Évaluation de l'identification :

Le taux d'identification est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les N premiers. On trace alors le score cumulé (cumulative match score) qui représente la probabilité que le bon choix se trouve parmi les N premiers [6]. Dans le cas où il existe plusieurs modèles pour chaque individu dans la base de données, les mesures classiques des systèmes de recherche dans une base de données peuvent être utilisées. La précision est le rapport entre le nombre de modèles correctement retrouvés par le système dans la base de données et le nombre total de modèles retrouvés. Le rappel est le rapport entre le nombre de modèles correctement retrouvés dans la base de données et le nombre total de modèles qui auraient dû être retrouvés.

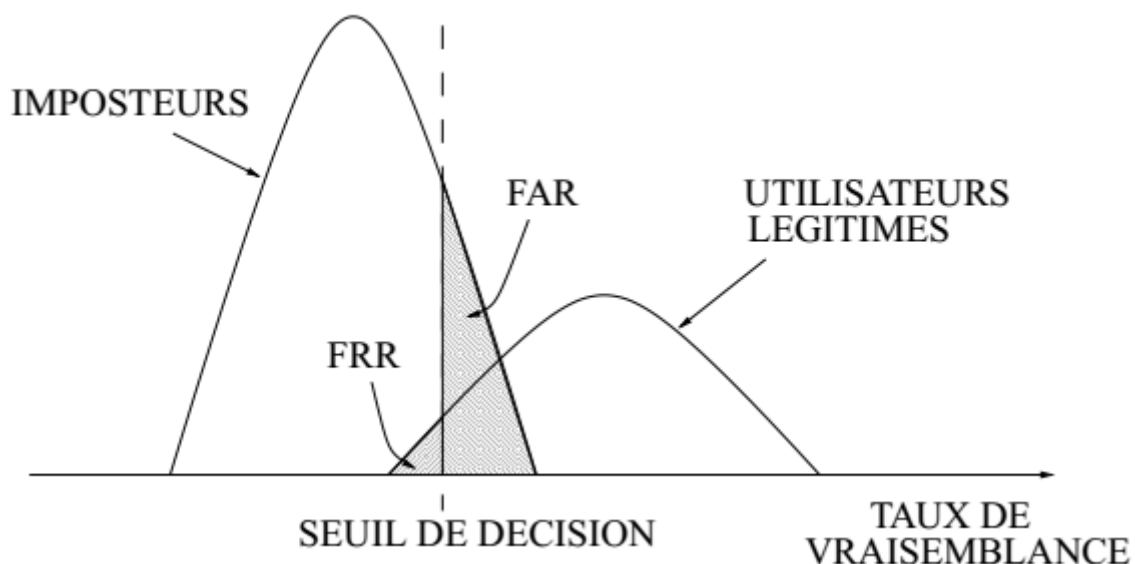


Figure I.8. – Distributions des taux de vraisemblance des utilisateurs légitimes et des imposteurs d'un système biométrique.

I.5.2 Évaluation de la vérification :

Lorsqu'un système fonctionne en mode vérification, celui-ci peut faire deux types d'erreurs. Il peut rejeter un utilisateur légitime et dans ce premier cas on parle de faux rejet (false

rejection). Il peut aussi accepter un imposteur et on parle dans ce second cas de fausse acceptation (false acceptance). La performance d'un système se mesure donc à son taux de faux rejet (False Rejection Rate ou FRR) et à son taux de fausse acceptation (False Acceptance Rate ou FAR). La vérification est un problème de décision similaire à la détection d'un signal dans le bruit en théorie de l'information [40]. Il peut être formulé de la manière suivante. Soient H_0 l'hypothèse : « la capture C provient d'un imposteur » et H_1 l'hypothèse : « la capture C provient de l'utilisateur légitime ». Il faut donc choisir l'hypothèse la plus probable. On considère que la capture C provient d'un utilisateur légitime si $P(H_1|C) > P(H_0|C)$. En appliquant la loi de Bayes on obtient :

$$P(C|H_1) P(H_1)/P(C) > P(C|H_0)P(H_0) /P(C) \text{ et donc : } P(C|H_1) /P(C|H_0) > P(H_0)/ P(H_1)$$

Le taux de vraisemblance (likelihood ratio) $P(C|H_1) /P(C|H_0)$ est comparé à un seuil θ appelé seuil de décision. Les valeurs $P(H_0)$ et $P(H_1)$ qui représentent respectivement la probabilité pour qu'un imposteur ou un utilisateur légitime essayent d'accéder au système sont des valeurs difficiles à estimer. Nous avons représenté sur la figure 2 la distribution hypothétique des taux de vraisemblance qu'obtiendraient les utilisateurs.

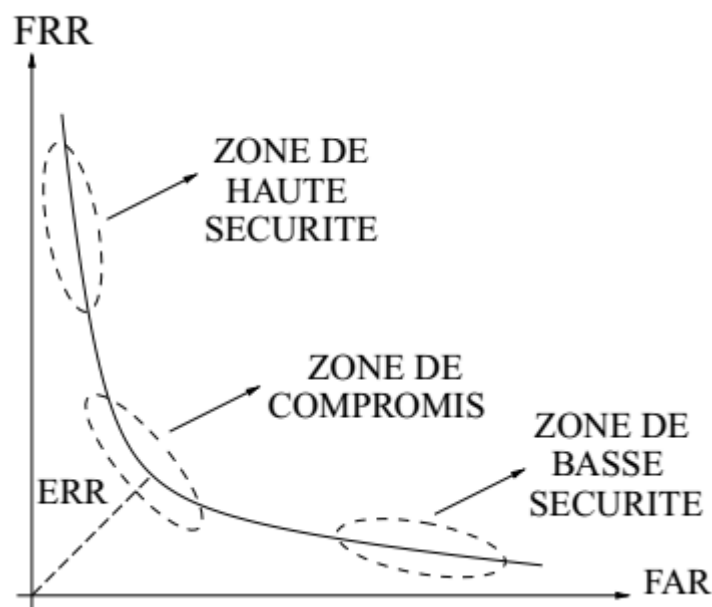


Figure I.9. – Courbe ROC.

Légitimes et les imposteurs d'un système de vérification donné. Les FAR et FRR sont représentés en hachuré. Idéalement, le système devrait avoir des FAR et FRR égaux à zéro. Comme ce n'est jamais le cas en pratique, il faut choisir un compromis entre FAR et FRR. Plus le seuil de décision θ est bas, plus le système acceptera d'utilisateurs légitimes mais plus il acceptera aussi d'imposteurs. Inversement, plus le seuil de décision θ est élevé, plus le système rejettera d'imposteurs mais plus il rejettera aussi d'utilisateurs légitimes. Il est donc impossible en faisant varier le seuil de décision de faire diminuer les deux types d'erreurs en même temps. C'est l'une des raisons qui a motivé l'introduction de la multi modalité puisqu'il

est possible de diminuer les deux types d'erreur à la fois en combinant correctement plusieurs modalités (c.f. section 5). La courbe dite ROC (Receiver Operating Characteristic), représentée à la figure 5, permet de représenter graphiquement la performance d'un système de vérification pour les différentes valeurs de θ [10]. Le taux d'erreur égal (Equal Error Rate ou EER) correspond au point $F_{AR} = F_{RR}$, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Cependant, il est important de souligner que le EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique. Le seuil θ doit donc être ajusté en fonction de l'application ciblée : haute sécurité, basse sécurité ou compromis entre les deux.

I.6 Applications des systèmes biométriques :

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

- **Applications commerciales :**

Telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-Commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

- **Applications gouvernementales :**

Telles que la carte d'identité nationale, le permis de conduire, la sécurité sociale, le contrôle des frontières, le contrôle des passeports, etc.

- **Applications légales :**

Telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, etc. De nos jours les systèmes biométriques sont de plus en plus utilisés dans des applications civiles. Par exemple, le dispositif de Schiphol Privium à l'aéroport d'Amsterdam, utilise un capteur de l'iris pour accélérer la procédure de contrôle des passeports et des visas [11]. Les passagers insèrent leur carte dans un lecteur et se mettent en face d'un appareil-photo ; ce dernier acquiert l'image de l'œil. Des processus de traitement d'images sont alors lancés afin de localiser l'iris et de calculer une signature appelée « Iris code » [12]. Une fois l'Iris code calculé, il est comparé aux données stockées dans la carte pour identifier le passager. Un dispositif semblable est également employé pour vérifier l'identité des employés de l'aéroport qui travaillent dans des secteurs de haute sécurité. Un autre exemple d'utilisation à grande échelle de la reconnaissance faciale est celui de la ville de Newham, dans la banlieue de Londres. Il s'est vu décerner le trophée Big Brother Awarden 1998 par l'organisation non gouvernementale Privacy International.

I.7 La place de la reconnaissance faciale parmi les autres techniques biométriques :

La reconnaissance de visages est la technique la plus commune et populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle; et par rapport aux autres méthodes, la reconnaissance du visage s'avère plus avantageuse, d'une part c'est une méthode non intrusive, c'est-à-dire elle n'exige pas la coopération du sujet (en observant les individus à distance), et d'une autre part les capteurs utilisés sont peu coûteux (une simple caméra) contrairement à l'empreinte digitale et l'iris où le sujet devra être très proche du capteur et devra coopérer pour l'acquisition de l'image sans oublier le coût de l'équipement nécessaire pour l'acquisition (équipement spécial coûteux). Malgré que certains disent que la reconnaissance de visages est une biométrie relativement peu sûre, sur le fait que le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques, comme la variation de l'éclairage, le changement de la position du visage, la présence ou l'absence de lunettes et autres; mais, au cours de ces dernières années plusieurs techniques de traitements d'images sont apparues, telle que la détection du visage, la normalisation de l'éclairage, etc. Sans oublier le développement considérable des technologies des caméras numériques, ce qui néglige l'effet de ces problèmes.

Avantages	Inconvénients
Bien accepté par le public. Aucune action de l'utilisateur (peu intrusive). Pas de contact physique. Technique peu coûteuse.	Technologie sensible à l'environnement (éclairage, position, expression du visage...). Difficultés de différencier de vrais jumeaux. Sensible aux changements. (Barbe, moustache, lunettes, piercing, chirurgie...).

Tableaux I.1 : Avantages et inconvénients de la Reconnaissance de Visage.

I.8 La part de marche par technologie :

Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 50% de chiffre d'affaire total (hors applications judiciaires). La reconnaissance faciale avec 12% de part (hors applications judiciaires) dépasse la reconnaissance de la main qui avait avant la deuxième place en termes de sources de revenu après les empreintes digitales.

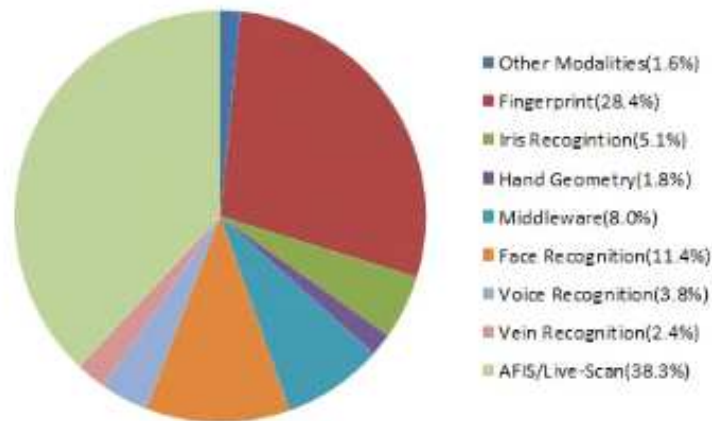


Figure I.10.Part de marché de chaque technologie.

I.9 Les enjeux pour de la biométrie de demain :

- Besoin de tests de systèmes et évaluation sur de grandes bases de données standardisées.
- Grand potentiel pour améliorer notre sécurité mais des lois et réglementations sont nécessaires.
- Aucun système de sécurité, biométrique inclus, n'est infaillible "foolproof".
- Besoin d'analyse de coût / bénéfice pour le déploiement de systèmes biométriques.
- Adaptation aux utilisateurs : observation des interactions avec le dispositif biométrique.
- Utilisation des caractéristiques : couleur des yeux, des cheveux, genre pour renforcer l'identité.
- Suivi : suivre le comportement de l'utilisateur pendant une session entière pour valider l'identité.

I.10 Conclusion :

Comme le fait remarquer Bill Spence de Recognition Systems Inc. [13] : « Chaque fois que vous utilisez votre clef, vous vous identifiez auprès de votre maison. Chaque fois que vous utilisez votre carte de crédit, chaque fois que vous vous connectez à un système, vous vous identifiez. » [14]. À terme, tous les mots de passe, codes confidentiels, badges, clefs, etc. seront amenés à être remplacés par des systèmes biométriques. La recherche en biométrie est donc un domaine à très fort potentiel. Cependant, nombreuses sont les personnes qui craignent que l'essor de la biométrie ne s'accompagne d'une atteinte généralisée à la vie privée des individus. Tout d'abord le manque de fiabilité des systèmes biométriques inquiète. Après les attentats du 11 Septembre 2001, beaucoup ont vu dans la biométrie, et plus précisément dans la reconnaissance de visages, le meilleur moyen de surveiller les lieux publics tels que les aéroports [15]. Mais supposons, par exemple, que le système Facelt de

Visionics [16], l'un des systèmes de reconnaissance du visage les plus populaires à l'heure actuelle, soit déployé dans le Hartsfield Atlanta International Airport (ATL), premier aéroport au monde en termes de passagers. Sachant que, d'une part, selon les chiffres fournis par Visionics, le EER de Facelt est de 0.68 % et que, d'autre part, le Airports Council International [17] estime à 80 millions le nombre de passagers de ATL en 2000, un rapide calcul aboutit à une moyenne de 1 500 personnes « rejetées » à tort quotidiennement et à plus d'un demi-million de personnes par an ! Même si aujourd'hui les passagers sont prêts à faire des concessions pour garantir leur sécurité, ils accepteront sans doute très mal ces erreurs à répétition. Et bien que des progrès constants soient enregistrés séparément pour chaque modalité, la performance des systèmes à un seul mode est encore loin d'être satisfaisante ce qui plaide en faveur du développement de systèmes biométriques multimodaux. Un problème très différent est le stockage de données personnelles dans des bases de données biométriques et l'utilisation malveillante qui pourrait en être faite. La meilleure solution à ce problème est d'abandonner l'idée d'une base de données centralisée au profit des cartes de type carte à puce dont l'utilisateur resterait possesseur [18]. Conscient de l'enjeu que représentent les libertés individuelles, c'est d'ailleurs l'un des arguments qu'utilise Mastercard pour promouvoir sa carte à puce intelligente (« Wewill not have a database of finger print sany where. » [19]). Quoi qu'il en soit, la biométrie peut apporter beaucoup dans la vie quotidienne en termes de sécurité mais également de confort. Comme pour d'autres « nouvelles technologies » (biotechnologie, réalité virtuelle, etc.) son essor devra s'accompagner d'une réflexion approfondie sur le respect des libertés individuelles.

Chapitre II :

SYSTEME DE RECONNAISSANCE DE VISAGES

II.1. Introduction:

Par la fréquence à laquelle on le rencontre dans l'environnement et par son contenu riche en information sociale de premier ordre [23]., le visage humain constitue un stimulus visuel de classe à part. En effet, il suffit d'un clin d'œil porté sur le visage d'un individu pour en distinguer le sexe, l'état émotionnel ou l'identité. Cette grande capacité à identifier les visages à pousser les chercheurs à tenter de rapprocher le cerveau humain dans sa rapidité, son exactitude et sa fiabilité par des systèmes de reconnaissance basés sur des approches statistiques ou non statistiques.

Cependant un système de reconnaissance de visage [24] consiste à identifier un individu à partir de la géométrie de son visage. Pour que ce système soit efficace, il faut disposer d'une image numérique de qualité du visage de l'individu en question, d'une base de données d'images numériques d'individus identifiés et d'un logiciel de reconnaissance de visage capable d'établir une correspondance exacte entre l'image d'un individu et une image d'un individu identifié qui est enregistrée dans la base de données.

Certaines applications de cette technologie à des fins de sécurité sont incontestablement bénéfiques et performantes, par exemple l'authentification des employés autorisés à avoir accès à une centrale nucléaire. Bien qu'elle soit plus en plus performante l'usage de cette technologie pose des problèmes éthiques selon certaines personnes et organisations. Le respect de la vie privée est, pour elles, bafoué lorsque des personnes totalement inconnues et sans que l'on en ait connaissance, peuvent avoir accès à des informations privées [23].

Dans ce présent chapitre on va expliquer bravement le mode de fonctionnement de la technologie de reconnaissance de visage et l'état de l'art de celle-ci.

II.2. La place de la reconnaissance de visage parmi les autres modalités :

La reconnaissance de visages est la technique la plus commune et populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle ; par rapport aux autres méthodes, la reconnaissance du visage s'avère plus avantageuse, d'une part c'est une méthode non intrusive, c'est-à-dire elle n'exige pas la coopération du sujet (en observant les individus à distance) d'autre part les capteurs utilisés sont peu coûteux. Depuis le 11 septembre 2002 un intérêt tout particulier est porté sur cette technologie, dont celui de pouvoir effectuer une identification à distance. Il ne faut cependant pas oublier les limites technologiques des systèmes actuels qui nécessitent pour l'instant un environnement (éclairage, position de la caméra, etc.) bien contrôlé pour pouvoir pleinement exprimer leurs performances [25].

Avantages	Inconvénients
Très bien accepté par le public Ne demande aucune action de l'utilisateur (Peu intrusive), pas de contact physique Technique peu coûteuse	Technologie sensible à l'environnement (éclairage, position, expression du visage...) Les vrais jumeaux ne sont pas différenciés Occultations partielles : Sensible aux changements (barbe, moustache, lunette, piercing, chirurgie...)

Tableau II.1 : Avantages et Inconvénients de la Reconnaissance de visage.

II.3. Le système de reconnaissance de visages :

La reconnaissance faciale est une tâche que les humains effectuent naturellement et sans effort dans leurs vies quotidiennes. La grande disponibilité d'ordinateurs puissants et peu onéreux ainsi que des systèmes informatiques embarqués ont suscité un énorme intérêt dans le traitement automatique des images et des vidéos numériques au sein de nombreuses applications [26], incluant l'identification biométrique, la surveillance, l'interaction homme-machine et la gestion de données multimédia. La reconnaissance faciale, en tant qu'une des technologies biométriques de base, a pris une part de plus en plus importante dans le domaine de la recherche, ceci étant dû aux avancées rapides dans des technologies telles que les appareils photo numériques, Internet et les dispositifs mobiles, le tout associé à des besoins en sécurité sans cesse en augmentation.

Dans un système de reconnaissance de visages, depuis son acquisition, l'image suit un processus bien précis pour arriver à déterminer ou à vérifier l'identité du porteur de visage. Ce processus peut être présenté par le diagramme suivant :

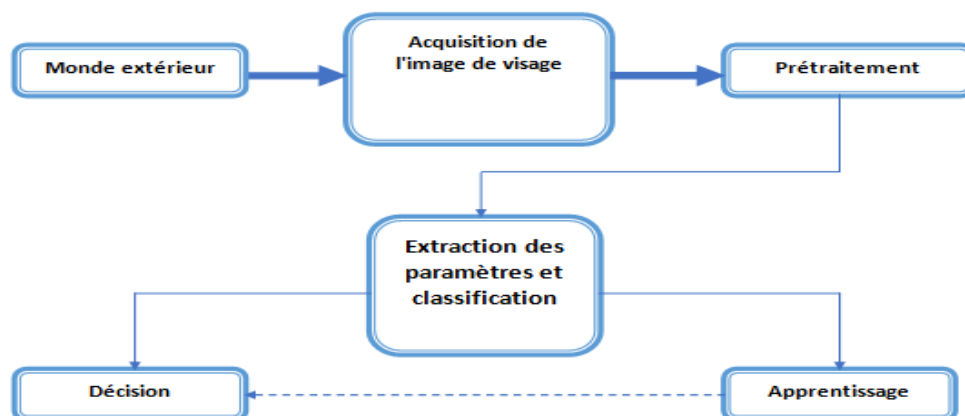


Figure II.1: Le processus de reconnaissance de visage.

Un système de reconnaissance du visage passe par plusieurs étapes qui sont :

II.3.1. Acquisition de l'image :

C'est l'opération qui permet d'extraire du monde extérieur (réel) une représentation matricielle (un ensemble de pixels) c'est-à-dire une image, cette opération peut être statique (Appareil photo, Scanner, etc.) ou dynamique (Caméra, Webcam) [27].

II.3.2. Prétraitement :

Les données brutes issues des capteurs sont les représentations initiales des données, à partir desquelles des traitements permettent de construire celles qui seront utilisées pour la reconnaissance. L'image brute peut être affectée par différents facteurs causant ainsi sa détérioration, elle peut être bruitée c'est à dire contenir des informations parasites à cause des dispositifs optiques ou électroniques. Pour pallier à ces problèmes, il existe plusieurs méthodes de traitement et d'amélioration des images, telle que : la normalisation, l'égalisation de l'histogramme...etc. [27].

II.3.3. Extraction des paramètres et Classification :

- **Extraction des paramètres** : On doit extraire les informations utiles qui reviennent à établir un modèle du visage (vecteur de caractéristiques). Ces informations nécessaires pour que le visage d'une personne ne ressemble pas à celui d'un autre, en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition [27].
- **Classification des paramètres** : Ces informations seront ensuite classées, autrement dit, affectés à la classe la plus proche, les individus ayant des similarités sont regroupés dans la même classe. Ces classes varient selon le type de décision. L'efficacité de cette étape a une influence directe sur la performance du système de reconnaissance de visage [27].

II.3.4. L'apprentissage :

Cette étape consiste à mémoriser les modèles calculés dans la phase d'analyse pour les individus connus. Un modèle est une représentation compacte des images qui permet de faciliter la phase de reconnaissance mais aussi de diminuer la quantité de données à stocker en quelque sorte l'apprentissage est la mémoire du système [27].

II.3.5. Décision :

Est la partie du système où l'on tranche sur l'appartenance (ou pas) d'un individu à l'ensemble des visages, si oui quelle est son identité. Donc la décision c'est l'aboutissement du processus. On peut le valoriser par le taux de reconnaissance (fiabilité) qui est déterminé par le taux de justesse de la décision [27].

II.4. État de l'art des méthodes de reconnaissances de visages :

Plusieurs méthodes de reconnaissance de visages ont été proposées durant les vingt dernières années. Elle est un axe de recherche ouvert attirant des chercheurs venants de disciplines différentes : psychologie, reconnaissance de formes, réseaux de neurone, vision artificielle et infographie. Les caractéristiques qui servent à la reconnaissance du visage sont les yeux, la bouche, la forme du visage (contour), etc.

Les méthodes de reconnaissance faciales peuvent être séparées en trois grandes familles, les méthodes globales (ou holistiques), les méthodes locales, basées sur des modèles et les méthodes hybrides. Le diagramme suivant fournit une classification des méthodes principales de reconnaissance faciale :

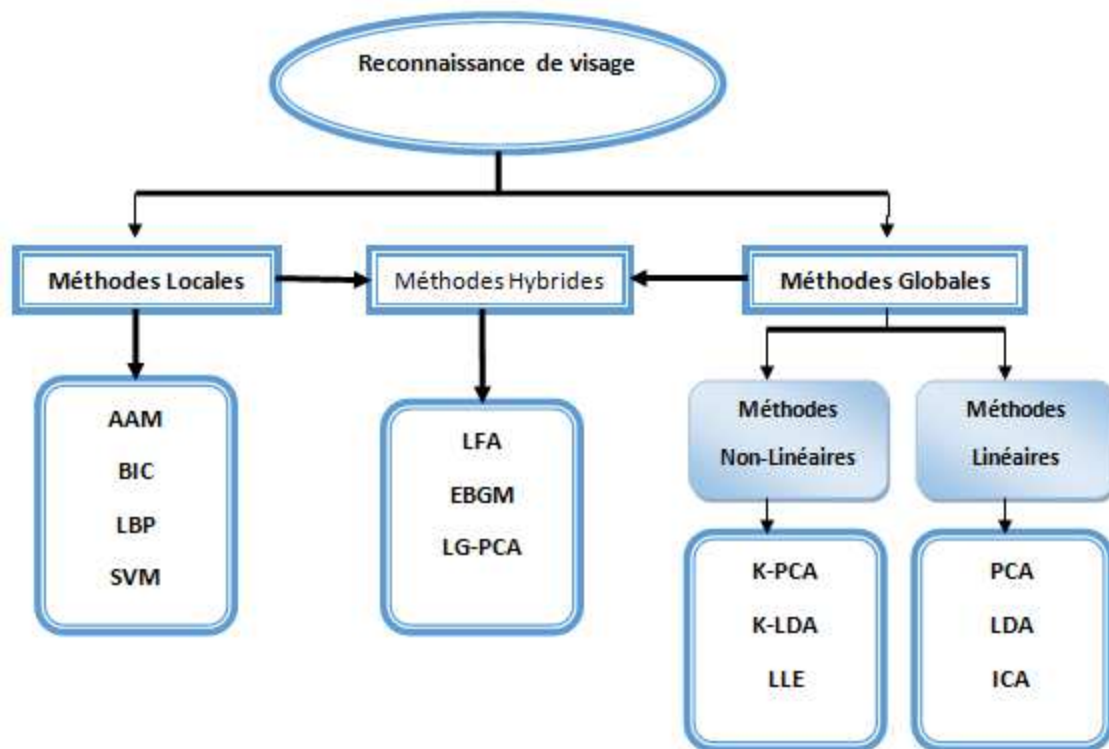


Figure II.2: Classification des méthodes principales utilisées dans la reconnaissance de visage.

II.4.1. Méthodes globales :

Les méthodes holistiques appelées aussi méthodes globales, sont des méthodes qui utilisent la région entière du visage comme entrée à l'algorithme de reconnaissance [28]. Ce sont des techniques très réussies et bien étudiées. L'avantage principal de ces méthodes est qu'elles sont relativement rapides à mettre en œuvre et que les calculs de base sont d'une complexité moyenne [29]. Bien que ces méthodes offrent de bonnes performances, ces

méthodes sont exposées aux problèmes de stockage d'informations extraites lors de la phase "apprentissage", de variations d'éclairage, pose, expressions faciales. Parmi ses méthodes nous citons : l'analyse en composantes principales (PCA), l'analyse discriminante linéaire (LDA).

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

L'algorithme PCA est né des travaux de MA.Turk et AP.Pentaland au MIT Media Lab [30]. Aussi connu sous le nom Eigen faces car il utilise des vecteurs propres et des valeurs propres (respectivement Eigen vectors et Eigen values en anglais). L'idée principale consiste à exprimer nos M images de départ selon une base de vecteurs orthogonaux particuliers ces fameux vecteurs propres contenant des informations indépendantes d'un vecteur à l'autre [31]. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage.

Les images originales peuvent être reconstituées par combinaison linéaire de ces vecteurs propres. Les représentations graphiques de ces vecteurs rappellent un peu des images fantômes, chacune mettant en avant une partie du visage, on les appelle Eigen faces. (Figure II.3). Tout d'abord, l'algorithme PCA est une méthode globale utilisant en premier lieu les niveaux de gris des pixels d'une image. Sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale [31].

Néanmoins, le PCA ne nécessite aucune connaissance a priori sur l'image et se révèle plus efficace lorsqu'il est couplé à la mesure de distance MahCosine.

Le principe selon lequel on peut construire un sous-espace vectoriel en ne retenant que les "meilleurs" vecteurs propres, tout en conservant beaucoup d'information utile, fait du PCA un algorithme efficace et couramment utilisé en réduction de dimensionnalité où il peut alors être utilisé en amont d'autres algorithmes (comme le LDA par exemple).

Enfin, l'étude théorique de l'algorithme PCA est très pédagogique et permet d'acquérir de solides bases pour la reconnaissance 2D du visage.

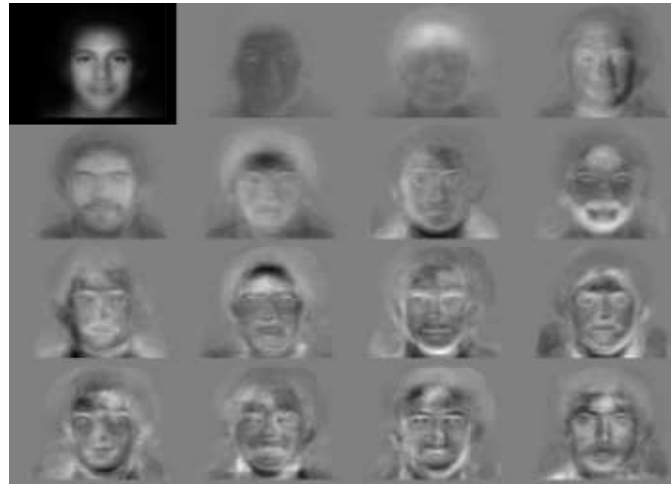


Figure II.3 : Image moyenne et les 15èmes Eigen faces.

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

L'algorithme LDA est né des travaux de Belhumeur et al. De la Yale University (USA), en 1997. Il est aussi connu sous le nom de Fisher faces.

Contrairement à l'algorithme PCA, le LDA effectue une véritable séparation de classes. Pour pouvoir l'utiliser, il faut donc au préalable organiser la base d'apprentissage d'images en plusieurs classes : une classe par personne et plusieurs images par classe. Le LDA analyse les vecteurs propres de la matrice de dispersion des données, avec pour objectif de maximiser les variations interclasses tout en minimisant les variations intra classes [31].

Tout d'abord, l'algorithme LDA permet d'effectuer une véritable séparation de classes, selon un critère mathématique qui minimise les variations entre les images d'un même individu (variations intra classe) tout en maximisant les variations entre les images d'individus différents (variations interclasses) (Figure. II.4). Cependant, pour des problèmes (sous-échantillonnés) en reconnaissance du visage, c'est-à-dire lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, il est difficile d'appliquer le LDA qui peut alors faire apparaître des matrices de dispersions singulières (non inversibles) [31]. Afin de contourner ce problème, certains algorithmes basés sur le LDA ont récemment été mis au point (les algorithmes ULDA, OLDA, NLDA).



Figure II.4 : Exemple de six classes utilisant LDA.

II.4.2. Méthodes locales :

Ce sont des méthodes géométriques [32], appelées aussi méthodes à traits, à caractéristiques locales, ou analytiques. L'analyse du visage humain est donnée par la description individuelle de ses parties et de leurs relations. Ce modèle correspond à la manière avec laquelle l'être humain perçoit le visage, c'est à dire, à nos notions de traits de visage, de parties caractéristiques comme les yeux, le nez ou la bouche. L'avantage principale de ces méthodes est de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression faciale contrairement aux méthodes dites globales. Bien que ces méthodes offrent de bonnes performances, mais leurs problèmes c'est qu'elles sont plus lourdes à utiliser puisqu'il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales (ou holistiques) ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection [33]. Parmi les algorithmes de reconnaissance de cette méthode nous citons le SVM.

- **Machine à Vecteurs de Support (SVM):**

C'est une nouvelle technique qui a été proposée par V.Vapnik en 1995 [34]., elle est utilisée dans plusieurs domaines statistiques (classement, régression, fusion,... etc.). Plusieurs travaux ont montré son efficacité et principalement en traitement d'images depuis son introduction dans le domaine de reconnaissance de formes.

L'idée essentielle de cette approche consiste à projeter les données de l'espace d'entrée (appartenant à des classes différentes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables [35]. Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la fonction de classement séparant les classes tels que :

Les vecteurs appartenant aux différentes classes se trouvent de différents côtés de l'hyperplan.

La plus petite distance entre les vecteurs et l'hyperplan (la marge) soit maximale.

II.4.3. Méthodes hybrides :

Les méthodes hybrides (ou méthodes de fusion) sont des approches utilisant à la fois des caractéristiques globales et des caractéristiques locales. Les facteurs clés qui influent les performances des méthodes de fusion comprennent le choix des caractéristiques pour la combinaison et la manière de les combiner de telle sorte que leurs avantages soient préservés et que leurs inconvénients soient évités. Les caractéristiques locales et les caractéristiques globales ont des propriétés très différentes et peuvent offrir des informations complémentaires utiles à la tâche de classification. Notons aussi que d'un certain point de vue, les méthodes locales peuvent être considérées comme des méthodes hybrides car des informations globales sont généralement prises en compte. Dans la méthode probabiliste locale [36] de nouveaux échantillons d'apprentissage sont d'abord produits pour chaque personne par méthode globale, puis une méthode locale est utilisée pour la reconnaissance. Parmi les algorithmes de reconnaissance de cette méthode nous citons le EBGM.

- **L'algorithme Elastic Bunch Graph Matching (EBGM):**

A partir d'une image de visage, cette méthode localise des points caractéristiques comme les coins des yeux, de la bouche et le nez. Un treillis élastique virtuel est ensuite appliqué sur l'image de visage à partir de ces points. Chaque point représente un nœud étiqueté auquel nous associons un jeu de coefficients d'ondelettes complexes de Gabor, appelés Jet [31]. Dans cette approche, la reconnaissance se fait par la mesure de similarité entre les différents Jets et les longueurs des segments du treillis de deux images.

La caractéristique de l'EBGM est qu'il ne traite pas directement les valeurs de niveaux de gris des pixels d'une image de visage, ce qui lui confère une plus grande robustesse aux changements d'éclairage, de pose et d'expression faciale. Cependant il est plus difficile à implémenter par rapport aux méthodes globales.

II.5. Principales difficultés de la reconnaissance de visage:

Pour l'être humain la reconnaissance de visage est un processus visuel de haut niveau, il détecte, il identifie des visages, objets, lieux dans des scènes différentes sans beaucoup de peine. Simuler le système de reconnaissance humain à un système automatique de reconnaissance de visages représente un vrai challenge pour les chercheurs Or, ce challenge semble plus en plus difficile lorsque les conditions d'acquisition des images sont dynamiques voire très variables. Il existe deux types de variation associées aux images de visage : inter et intra sujet, bien que, la variation inter est limitée vue la ressemblance physique des visages

humains. La variation intra sujet est plus vaste elle peut être influencé par plusieurs facteurs qui sont :

- **Changement d'illumination :**

L'apparence d'un visage dans une image varie énormément en fonction de l'illumination de la scène lors de la prise de vue (voir figure II.5). Les variations d'éclairage rendent la tâche de reconnaissance de visage très difficile [28]. En effet, le changement d'apparence d'un visage dû à l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entraîner une mauvaise classification des images d'entrée. Ceci a été expérimentalement observé dans Adini et al [37] où les auteurs ont utilisé une base de données de 25 individus. L'identification de visage dans un environnement non contrôlé reste donc un domaine de recherche ouvert. Les évaluations FRVT [38] ont révélé quelques problèmes de variation d'illumination constitue un défi majeur pour la reconnaissance faciale.



Figure II.5 : Exemple de variation d'éclairage [28].

- **Variation de pose:**

La variation de pose est considérée, comme un problème majeur pour les systèmes de reconnaissance faciale [28]. Quand le visage est de profil dans le plan image (orientation $< 30^\circ$), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30° , la normalisation géométrique n'est plus possible (voir figure II.6).



Figure II.6 : Exemples de variation de poses [28].

- **Expressions faciales:**

Un autre facteur qui affecte l'apparence du visage est l'expression faciale (voir figure II.7). La déformation du visage qui est due aux expressions faciales est localisée principalement sur la partie inférieure du visage [28]. L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraîne forcément une diminution du taux de reconnaissance. L'identification de visage avec expression faciale est un problème difficile qui est toujours d'actualité et qui reste non résolu. L'information temporelle fournit une connaissance additionnelle significative qui peut être utilisée pour résoudre ce problème [39].



Figure II.7 : Exemples de variation d'expressions faciale [39].

- **Présence ou absence des composants structurels:**

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance [28]. Par exemple, des lunettes opaques ne permettent pas de bien distinguer la forme et la couleur des yeux, et une moustache ou une barbe modifie la forme du visage.

- **Occultations partielles:**

Le visage peut être partiellement masqué par des objets dans la scène, ou par le port d'accessoire tels que lunettes, écharpe... Dans le contexte de la biométrie, les systèmes proposés doivent être non intrusifs c'est-à-dire qu'on ne doit pas compter sur une coopération active du sujet. Par conséquent, il est important de savoir reconnaître des visages partiellement occultés. Gross et al [39] ont étudié l'impact du port de lunettes de soleil, et du cache-nez occultant la partie inférieure du visage sur la reconnaissance faciale

ainsi, Leurs résultats expérimentaux semblent indiquer que, dans ces conditions, les performances des algorithmes de reconnaissance restent faibles.

II.6. Performances d'un système de reconnaissances de visage :

Chaque système de reconnaissance de visage a ses points forts et ses points faibles et cela dépend de la technologie utilisée et le domaine d'application de celui-ci, jusqu'à présent il n'existe aucun système " optimal " en termes des performances ce qui est due à plusieurs facteurs qui interviennent à plusieurs niveaux et qui peuvent limiter le degré de précision de ce dernier.

Néanmoins, il serait primordial d'observer ces facteurs avant de mesurer la performance d'un système de reconnaissance parmi ces facteurs on peut citer :

- L'environnement au moment de l'acquisition.
- La qualité des capteurs.
- Les différentes positions des capteurs.
- La mauvaise interaction entre l'utilisateur et les capteurs.

Généralement la performance d'un système biométrique se mesure par la performance de système d'identification et la performance de système de vérification.

II.6.1. Performance d'un système d'identification:

Pour évaluer les performances d'un système d'identification, on calcule le taux de reconnaissance du système par la formule suivante:

Taux de reconnaissance= nombre de décision correctes divisé par le nombre de décision totale.

II.6.2. Performance d'un système de vérification:

Dans ce cas, deux types d'erreurs peuvent être commises : Soit l'individu est rejeté alors qu'il s'agit bien d'un utilisateur enregistré dans la base de données, c'est ce qu'on appelle le Faux Rejet « **False rejection FR**», soit l'individu est accepté alors qu'il s'agit d'un imposteur, on l'appelle Fausse Acceptation « **False acceptance FA**».

La figure ci-après montre en fait la courbe de ce type d'erreurs :

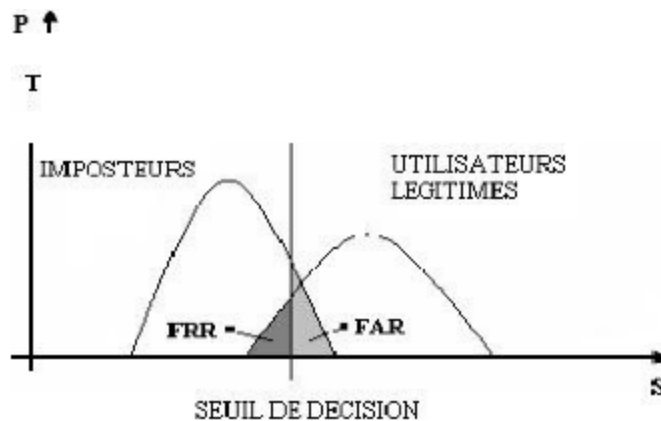


Figure II.8 : Seuil de décision et taux d'erreurs.

Dans un système idéal $FRR = FAR = 0$, mais ce n'est pas le cas dans la pratique ; quand FR augmente, FA diminue et vice versa. Par conséquent, il faut trouver un compromis entre les deux taux qui est la jonction des courbes, c'est-à-dire le point X (voir Figure II.9) où le couple (FAR, FRR) est minimal.

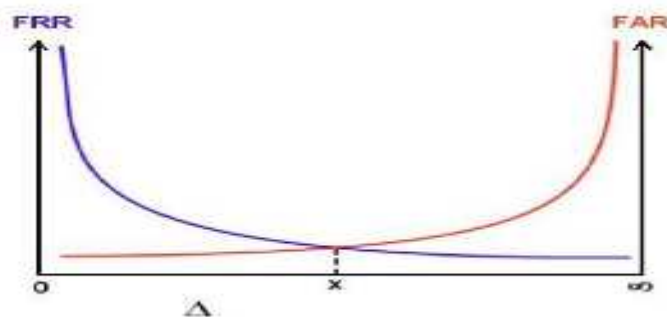


Figure II.9 : Relation entre FAR et FRR.

II.7. Nouvelles technologies améliorant la reconnaissance faciale:

La reconnaissance faciale de personnes est un sujet dont l'intérêt n'est plus à démontrer que ce soit dans la biométrie, vidéosurveillance, IHM avancées ou encore l'indexation d'images/vidéos. Cependant, elle se heurte encore à de nombreux problèmes, dont les plus connus le changement d'éclairage. Une possibilité pour pallier ce problème est l'utilisation d'autres nouvelles technologies telles que l'infrarouge, et la technologie 3D.

- **L'utilisation de la technologie infrarouge:**

L'infrarouge permet en outre à un système biométrique de fonctionner, même lorsque la capture dans le domaine visible est impossible ou de mauvaise qualité, lors d'une capture nocturne [40] par exemple. Le capteur infrarouge utilisé fonctionne dans le domaine des faibles longueurs d'ondes, générant ainsi une cartographie thermique des visages. La technologie infrarouge n'est pas sensible aux changements d'éclairage, mais plutôt à la température des corps capturés.

Néanmoins, le coût extrêmement élevé de cette technologie rend son utilisation prohibitive pour les applications.

- **L'utilisation de la technologie 3D:**

La quasi-totalité des systèmes de reconnaissance de visages travaillent à partir d'images fixes (images 2D)[41]. Bien que les approches 2D aient donné de bonnes performances, elles restent très sensibles aux problèmes de changements de conditions d'éclairage, de pose, d'expressions faciales et d'occultations. L'introduction de la forme 3D du visage dans la reconnaissance de personnes est considérée comme une voie très prometteuse pour remédier à ces problèmes.

L'imagerie à trois dimensions (3D) est moins sensible aux variations d'éclairage, à la modification d'apparence, volontaire ou involontaire, ou au fait que la personne ne fait pas face à la caméra. En effet, si quelqu'un se présente de biais, un logiciel fait « tourner » le modèle tridimensionnel pour le faire correspondre à l'image bidimensionnelle prise en conditions réelles.

II.8. Conclusion :

A travers ce chapitre, nous avons présenté un résumé sur l'état de l'art des systèmes de reconnaissance faciale, le processus de reconnaissance faciale depuis l'acquisition de l'image à l'identification. Ensuite, Nous avons mis en évidence les différentes difficultés inhérentes à la reconnaissance automatique de visages. Enfin, nous avons aussi donné un aperçu sur les techniques de mesure de performances d'un système de reconnaissance de visage et quelques nouvelles technologies améliorant ce dernier. Le chapitre suivant sera consacré à l'application des ondelettes pour l'extraction des paramètres.

PARTIE II :

EXTRACTION DES PARAMETRES ET CLASSIFICATION.

Chapitre III :

APPLICATION DES ONDELETTES POUR L'EXTRACTION DES PARAMETRES

III.1. Introduction:

L'analyse par ondelettes est apparue au début des années 80. En réalité, celle-ci ne repose pas sur une nouvelle idée originale. Cette théorie est un travail pluridisciplinaire qui a réuni des ingénieurs, des mathématiciens et des physiciens ayant développé des idées semblables dans leur domaine respectif. La synthèse mathématique a débouché sur des résultats nouveaux, qui ont apporté des perspectives plus larges dans chaque discipline originelle. A l'époque actuelle, la plupart des chercheurs scientifiques ont déjà entendu parler des ondelettes. Dans la majorité des congrès traitant de l'analyse du signal et de l'image, de la statistique, de la mathématique, etc., des conférences au sujet des ondelettes sont données.

Les transformations mathématiques sont appliquées aux signaux bruts pour obtenir davantage d'informations qui sont disponibles dans ces signaux.

En pratique, la plupart des signaux, sous leur format brut, sont représentés dans le domaine temporel. La représentation du signal est une représentation temps - amplitude. Cette représentation n'est pas toujours la meilleure pour toutes les applications en traitement du signal. Dans beaucoup de cas, l'information la plus pertinente est cachée dans la composante de fréquence du signal. Le *SPECTRE* de fréquence d'un signal est constitué par les composantes de fréquence de ce signal.

Intuitivement, nous savons que la fréquence est liée au régime de changement d'une variable physique ou mathématique. Cette variable peut

- changer **rapidement** : changement à **haute fréquence**,
- changer **lentement** : changement à **basse fréquence**, et
- **ne pas changer** du tout : **fréquence zéro**.

III.2. Pourquoi les ondelettes (contribution) :

Etant donné que notre travail s'inscrit dans le cadre de la reconnaissance de visages, On a choisi les ondelettes pour diverse avantage. Elles permettent de palier aux problèmes de variations d'éclairage, expressions faciales, position et aux changements des caractéristiques physiques (barbe, moustache, lunette, chirurgie ...) qui avant était un frein pour la reconnaissance faciales. Les ondelettes, comme nouvel outil mathématique notable, se sont imposées dans de divers domaines d'application. Par leur capacité extraordinaire de concentration de l'énergie et par leur pouvoir fascinant de détection d'irrégularités. L'analyse par ondelettes ne se limite plus à l'image telle qu'elle nous apparaît, mais permet l'étude des objets présents dans l'image à différentes échelles, elle permet de réduire la redondance pour améliorer la compression d'une image, elle peut également extraire les informations importantes (texture, contours, etc.) contenues dans une image et aussi de réduire le bruit contenu dans l'image.

III.3. Qu'est-ce qu'une ondelette :

Une ondelette [42] est une fonction oscillante (ce qui explique le mot "onde") de moyenne nulle, possédant un certain degré de régularité et dont le support est fini (ce qui explique le mot "ondelette", qui veut dire petite onde). Décomposition similaire à la transformée de Fourier à court terme, utilisée dans le traitement du signal. Cependant, elle comporte deux différences majeures avec la transformée de Fourier à court terme : * elle peut mettre en œuvre une base différente, non forcément sinusoïdale ; * il existe une relation entre la largeur de l'enveloppe et la fréquence des oscillations : on effectue ainsi une homothétie de l'ondelette, et non seulement de l'oscillation.

Toutefois, il ne s'agit pas d'un formalisme différent de la transformée de Fourier, mais complémentaire ; la décomposition en ondelettes utilisant le formalisme de Fourier.

La technique des ondelettes est particulièrement utilisée en compression de données informatiques. Plusieurs exemples sont montrés dans la figure III.1.

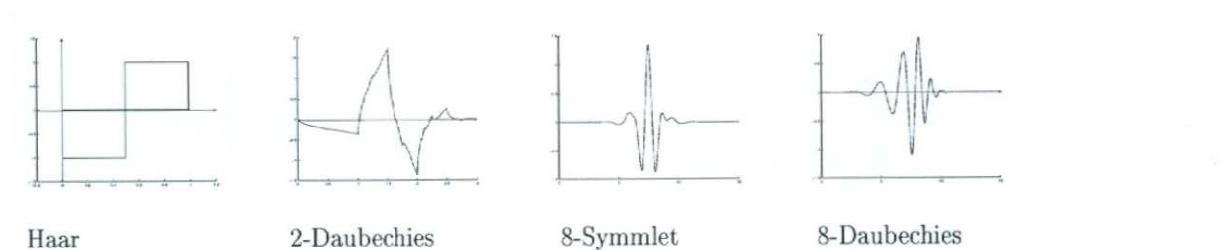


Figure III.1 : Exemples d'ondelette $\phi(t)$. (D'après Charles, 2003).

III.4. Les principales caractéristiques d'une ondelette mère :

Une ondelette mère ψ est une fonction de base que l'on peut traduire et dilater pour couvrir le plan temps-fréquences et analyser un signal. L'ondelette doit être une fonction de moyenne nulle, en d'autres termes, ψ doit être une onde ! Ce qui s'écrit mathématiquement par [42] :

$$\int \psi(x) dx = 0 \quad (2.8)$$

Toutes les ondelettes d'une famille, $\psi_{a,b}(x)$, ($a > 0$ et $b \in \mathbb{R}$) sont générées à partir d'une ondelette mère, en introduisant les paramètres de dilatation (échelle) a et de translation dans le temps b .

$$\psi_{a,b}(x) = \frac{1}{\sqrt{|a|}} \psi\left(\frac{x-b}{a}\right) \quad \text{Avec } a, b \in \mathbb{R} \quad (2.9)$$

Une ondelette mère doit remplir certaines propriétés dont les plus importantes sont :

III.4.1. L'admissibilité :

Soit ψ une fonction non nulle de $L^2(\mathbb{R})$ et $TF(\psi)$ sa transformée de Fourier. On dit que ψ est admissible si :

$$0 < \int_{-\infty}^{+\infty} \frac{|TF(\psi(x))|^2}{|x|} dx < +\infty \quad (2.10)$$

III.4.2. Localisation :

Une ondelette dont la fonction $\psi(x)$ de $L^2(\mathbb{R})$ est locale, si elle est à décroissances rapide sur les deux bords de son domaine de définition. La localisation signifie que l'énergie d'une ondelette est contenue dans un intervalle fini. Idéalement, l'ondelette est une fonction nulle en dehors d'un intervalle fini : c'est-à-dire une fonction à support compact.

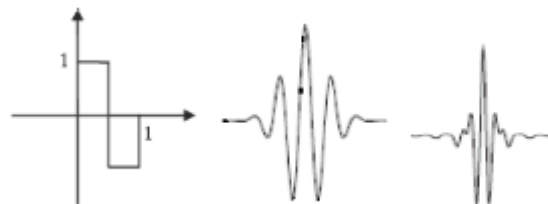
III.4.3. L'oscillation :

C'est le moment d'ordre 0, où la moyenne de la fonction $\psi(x)$ de $L^2(\mathbb{R})$ est nulle, et par conséquent, $\psi(x)$ doit avoir un caractère ondulatoire, qui change de signe au moins une fois. Cette propriété figure dans l'expression (2.8).

III.4.4. La translation et la dilatation :

L'ondelette mère doit satisfaire les propriétés de translation et de dilatation pour quelle puisse générer d'autres ondelettes (Figure 2.2).

Nous présentons ci-dessous quelques ondelettes unidimensionnelles :



Ondelette de Meyer

Ondelette de Haar

Ondelette de Morlet



Ondelette Bêta

Ondelette Chapeau mexicain

Figure III.2: Quelques exemples d'ondelettes 1D.

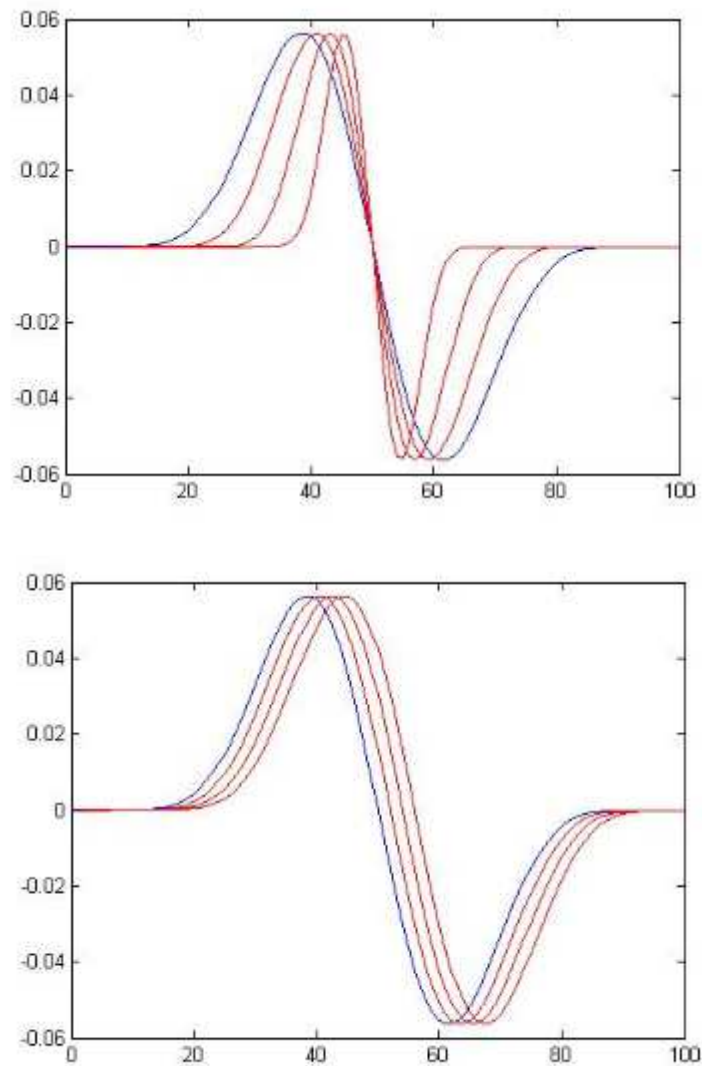


Figure III.3 : Exemple d'une ondelette dilatée et translatée.

III.5. La transformée en ondelettes :

La transformée en ondelettes [45] est similaire à la transformée de Fourier (et encore plus à la transformée de Fourier locale) avec une fonction de mérite complètement différente. La différence principale est la suivante : la transformée de Fourier décompose le signal en sinus et en cosinus, c'est-à-dire en fonctions localisées dans l'espace de Fourier ; contrairement à la transformée en ondelettes qui utilise des fonctions localisées à la fois dans l'espace réel et dans l'espace de Fourier. De manière générale, la transformée en ondelettes peut être exprimée avec l'équation suivante :

$$F(a, b) = \int_{-\infty}^{\infty} f(x) \psi_{(a,b)}^*(x) dx$$

Où le symbole $*$ désigne le conjugué complexe et ψ est une fonction donnée. Cette fonction peut être choisie arbitrairement à condition qu'elle obéisse à certaines règles.

Comme on peut le voir, la transformée en ondelettes est en fait un ensemble infini de diverses transformées, dépendant de la fonction de mérite utilisée pour la calculer. C'est la raison pour laquelle nous pouvons entendre parler de la « transformée en ondelettes » dans des contextes et applications très divers. Il existe aussi de nombreuses manières de classer les types de transformées en ondelettes. Nous ne présentons ici que la division basée sur l'orthogonalité des ondelettes. Nous pouvons utiliser les *ondelettes orthogonales* pour le développement en ondelettes discret et les *ondelettes non-orthogonales* pour le développement en ondelettes continu. Ces deux transformées possèdent les propriétés suivantes :

III.5.1. La transformation en ondelettes continues :

La transformée en ondelettes continue (CWT, Continuous Wavelet Transform) est une implémentation de la transformée en ondelettes utilisant des échelles arbitraires ainsi que des ondelettes pratiquement arbitraires. Les ondelettes utilisées ne sont pas orthogonales et les données obtenues par cette transformée sont hautement corrélées. Nous pouvons aussi utiliser cette transformée pour les séries discrètes dans le temps, avec la limitation que les translations des plus petites ondelettes soient égales au pas d'échantillonnage des données. Cette transformée est parfois appelée transformée en ondelettes continue discrète dans le temps (DT-CWT, Discrete-Time Continuous Wavelet Transform), et il s'agit de la façon la plus répandue de calculer la CWT pour des applications réelles.

En principe la transformée en ondelettes continue fonctionne en utilisant directement la définition de la transformée en ondelettes, c'est-à-dire en calculant la convolution du signal par l'ondelette mise à l'échelle. Nous obtenons de cette manière pour chaque échelle un ensemble de longueur N identique à celle du signal. En utilisant M échelles choisies arbitrairement nous obtenons une matrice $N \times M$ représentant directement le plan temps-fréquence. L'algorithme utilisé pour ce calcul peut être basé sur une convolution directe ou par une convolution réalisée par une multiplication dans l'espace de Fourier (aussi appelée transformée en ondelettes rapide).

Les propriétés de La transformée en ondelettes continue sont qu'elle retourne quant à elle un vecteur de dimension supérieure d'un à celle des données d'entrée. Pour des données 1D nous obtenons une image du plan temps-fréquence. On peut ainsi aisément visualiser l'évolution fréquentielle pendant la durée du signal et comparer son spectre avec ceux d'autres signaux. Comme on utilise ici un ensemble d'ondelettes non-orthogonales, les données sont hautement corrélées, on a donc dans ce cas une redondance élevée. Ceci permet de voir le résultat sous une forme plus « humaine ».

III.5.2. La transformation en ondelettes discrètes :

La transformée en ondelettes discrète (DWT, Discrete Wavelet Transform) est une implémentation utilisant un ensemble discret d'échelles et de translations d'ondelettes obéissant à certaines règles. En d'autres termes, cette transformée décompose le signal en un ensemble d'ondelettes mutuellement orthogonales, ce qui constitue la différence principale avec la transformée en ondelettes continue, ou son implémentation en séries discrètes dans le temps parfois appelée transformée en ondelettes continue discrète dans le temps (DT-CWT, discrete-time continuous wavelet transform).

L'ondelette peut être construite à partir d'une fonction d'échelle décrivant les propriétés d'échelle du signal. La restriction d'orthogonalité avec les translations discrètes implique certaines conditions mathématiques.

Les propriétés de La transformée en ondelettes discrète sont qu'elle retourne un vecteur de données de même longueur que les données d'entrée. Généralement la plupart des valeurs de ce vecteur sont pratiquement nulles. Cela vient du fait qu'elle décompose en un ensemble d'ondelettes (fonctions) orthogonales par translation et par homothétie. On décompose ainsi le signal en un nombre égal ou inférieur de coefficients du spectre d'ondelettes que le nombre de points de données du signal. Un tel spectre d'ondelettes est très bon pour le traitement du signal et la compression, par exemple, car nous n'obtenons ici aucune information redondante.

III.6. Propriétés des ondelettes:

III.6.1. Sélectivité en fréquence :

Dans la transformée de Fourier, la fonction utilisée pour analyser le signal étudié est une fonction sinusoïdale de fréquence précise, et quand on la multiplie par le signal, le coefficient obtenu ne se réfère qu'à cette fréquence.

En revanche, une ondelette est constituée de plusieurs fréquences. Les coefficients d'ondelettes se réfèrent à ce mélange de fréquences. Plus la gamme de fréquence de l'ondelette est étroite, plus l'ondelette est sélective en fréquence.

III.6.2. Similarité :

Toutes les ondelettes qui appartiennent à la même famille doivent être similaires, c'est-à-dire se déduire les unes des autres par combinaison linéaire de translations et de dilatations.

III.6.3. Symétrie:

On souhaite parfois que l'ondelette présente des propriétés de symétrie temporelle afin d'éviter le déphasage dans la transformée en ondelettes.

III.6.4. Orthogonalité :

Cette propriété est à l'origine de la popularité des ondelettes qui offrent des bases d'ondelettes orthogonales et non redondantes. Cela conduit à une décomposition unique.

III.6.5. Régularité :

Une ondelette doit être suffisamment régulière car c'est la principale contribution des ondelettes dans le domaine du codage. Elle agit sur la qualité de la reconstruction du signal.

Une ondelette est dite régulière si elle est très lisse et on peut l'approximer localement par un polynôme. L'ordre de régularité d'une ondelette est égal au nombre de ses moments nuls.

III.6.6. Nombre de moments nuls:

Pour certaines applications, les ondelettes doivent également avoir un certain nombre de moments nuls, afin d'éliminer la partie polynomiale du signal et être ainsi plus sensible aux fluctuations les moins régulières.

III.6.7. Facteur d'échelle minimal:

Théoriquement le facteur d'échelle, a , qui est strictement positif, peut varier jusqu'à $+\infty$.

En pratique, Il convient de se fixer un nombre de points de discrétisation minimum, N_{min} , de telle sorte que les valeurs discrètes de l'ondelette soient représentatives de sa forme continue.

Soit a_{min} le facteur d'échelle minimum, alors : $a_{min} = N_{min} / N$

Avec N_{min} : nombre d'échantillons minimal de $\psi_a(t)$

N : nombre d'échantillons de l'ondelette mère $\psi(t)$.

III.6.8. Relation entre fréquence et échelle:

Si f_0 est la fréquence centrale de l'ondelette mère $\psi(t)$, les autres ondelettes $\psi_{a,b}(t)$ oscillent à la fréquence $f = f_0/a$.

D'où l'identification : $a = f_0/f$.

III.7. Présentation des ondelettes multidimensionnelles :

Dans le cadre de la modélisation, il est fréquent d'avoir affaire à des processus multi variables, il est donc utile d'introduire la notion d'ondelette multidimensionnelle.

On peut définir une ondelette multidimensionnelle comme le produit d'ondelettes unidimensionnelles : on dit alors que les ondelettes sont séparables [44]. Dans ce cas, l'expression d'une ondelette multidimensionnelle est :

$$\Psi_j(x) = \prod_{k=1}^{N_1} \psi(Z_{jk}) \quad \text{avec : } Z_{jk} = \frac{x_k \pm m_{jk}}{d_{jk}} \quad (2.11)$$

Où x_k est la $k^{\text{ième}}$ composante du vecteur d'entrée X , et Z_{jk} la composante centrée par m_{jk} et dilatée d'un facteur d_{jk} . Il a été montré que ces ondelettes multidimensionnelles sont des frames à structures obliques de $L^2(\mathbb{R}^{N_1} \times \mathbb{R}^{N_1})$.

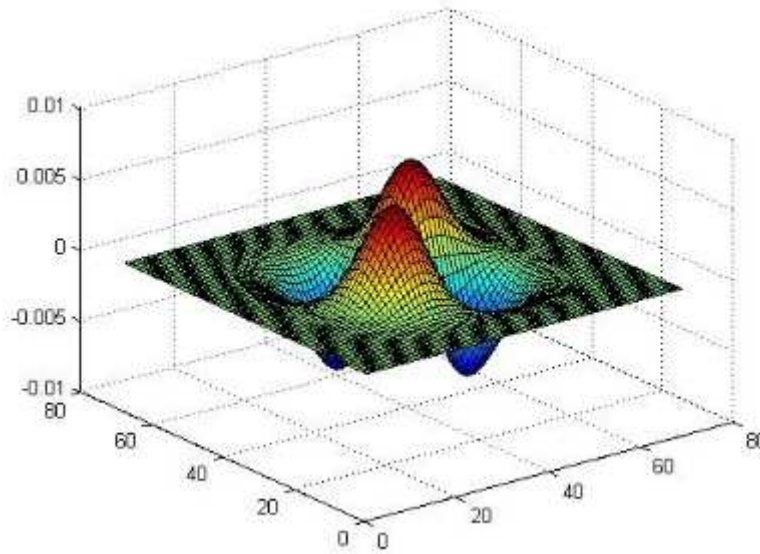


Figure III.4: Exemple d'une ondelette 2D.

III.8. Famille d'ondelettes :

Avant de détailler quelques familles d'ondelettes usuelles, nous dressons dans le tableau suivant (Tableau III.1) la liste de quelques-unes de ces familles, avec les abréviations associées.

Nom des familles d'ondelettes	Abréviations
Ondelette de Haar	<i>Haar</i>
Ondelettes de Daubechies	<i>Db</i>
Ondelettes Symlets	<i>Sym</i>
Ondelettes Coiflets	<i>Coif</i>
Ondelettes biorthogonales	<i>Bior</i>
Ondelette de Demystified	<i>dmey</i>
Ondelettes gaussiennes	<i>Gaus</i>
Ondelettes gaussiennes complexes	<i>Cgau</i>
Chapeau mexicain	<i>Mexh</i>
Ondelette de Morlet	<i>Morl</i>
Ondelette de Morlet complexe	<i>Cmor</i>
Ondelettes de Shannon complexes	<i>Shan</i>

Tableau III.1: Familles d'ondelettes.

Les familles d'ondelettes peuvent être caractérisées par quatre propriétés principales : existence de filtres associés, orthogonalité ou bi orthogonalité, support compact ou non, ondelettes réelles ou complexes. Le tableau (Tableau III. 2) résume ces diverses propriétés.

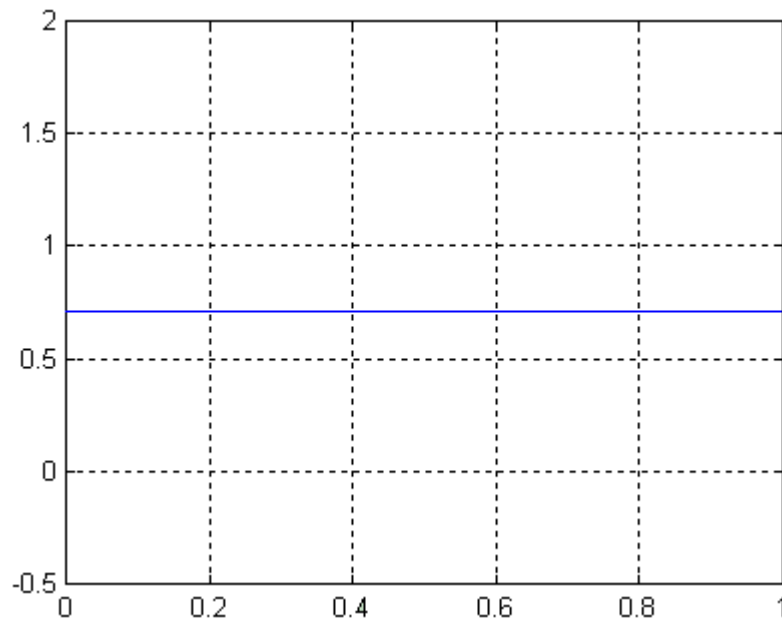
Ondelettes à filtres			Ondelettes sans filtres	
A support compact		A support non compact	Réelles	Réelles Complexe
Orthogonales	Biorthogonales	Orthogonales	gaus, mexh, morl	cgau, shan, cmor
Db, haar, sym, coif	Bior	dmey		

Tableau III.2 : Les propriétés principales des ondelettes.

Les ondelettes à filtre sont associées à des analyses multi résolution orthogonales ou bi orthogonales ; la transformée discrète et les calculs rapides en utilisant l'algorithme de Mallat [47] sont alors possibles. Les ondelettes sans filtre, en revanche, sont utiles pour la transformée en ondelettes continues.

En général, les ondelettes à support compact n'ont pas de forme analytique (c'est-à-dire : on sait comment calculer la fonction, mais on ne peut pas l'exprimer avec une formule mathématique).

III.8.1. Ondelette de Haar :

Figure III.5 : Filtre h_0 de Haar.

La transformée de Haar a été introduite en 1910, et est de loin la plus ancienne transformée en ondelettes. Elle est basée sur la démonstration de Haar que les fonctions $h(j,k;x)=2^{j/2}H(2^jx-k)$ telle que :

$H(x)=1$ pour x dans $]0,1/2[$

$H(x)=-1$ pour x dans $]1/2,1[$

$H(x)=0$ ailleurs,

Forment un ensemble orthogonal complet, i.e., une base pour l'espace $L^2(\mathbb{R})$.

L'ondelette de Haar est simple à étudier et à mettre en œuvre. Malheureusement les résultats de la transformée de Haar sont peu satisfaisants.

III.8.2. Ondelettes de Daubechies:

Cette famille d'ondelettes (dbN) à un paramètre, due à I. Daubechies [48], est la première permettant de manipuler des ondelettes orthogonales à support compact de régularité arbitraire, on dira que N est l'ordre de l'ondelette dbN .

Cette famille contient l'ondelette de Haar ($db1$), qui est la plus simple et certainement la plus ancienne des ondelettes. Elle est discontinue, ressemble à un échelon.

La fonction d'ondelette de Haar est définie par (Figure III.6) :

$y(x) = 1$ si $x \in [0, 0.5[$, $y(x) = -1$ si $x \in [0.5, 1[$ et 0 sinon.

La fonction d'échelle associée est la fonction échelon :

$j(x) = 1$ si $x \in [0, 1]$ et 0 sinon.

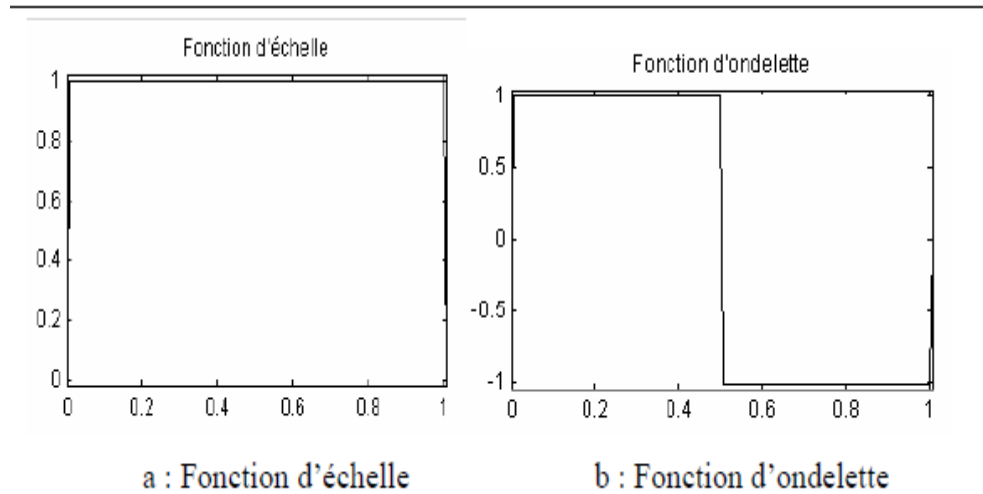


Figure III.6: La fonction d'échelle et la fonction d'ondelette de haar.

Hormis $db1$, les ondelettes de cette famille n'ont pas une formule analytique. Ces ondelettes pour les ordres de 2 à 10 ($db2$, $db3$, ..., $db10$) sont présentées dans la figure (Figure III.7).

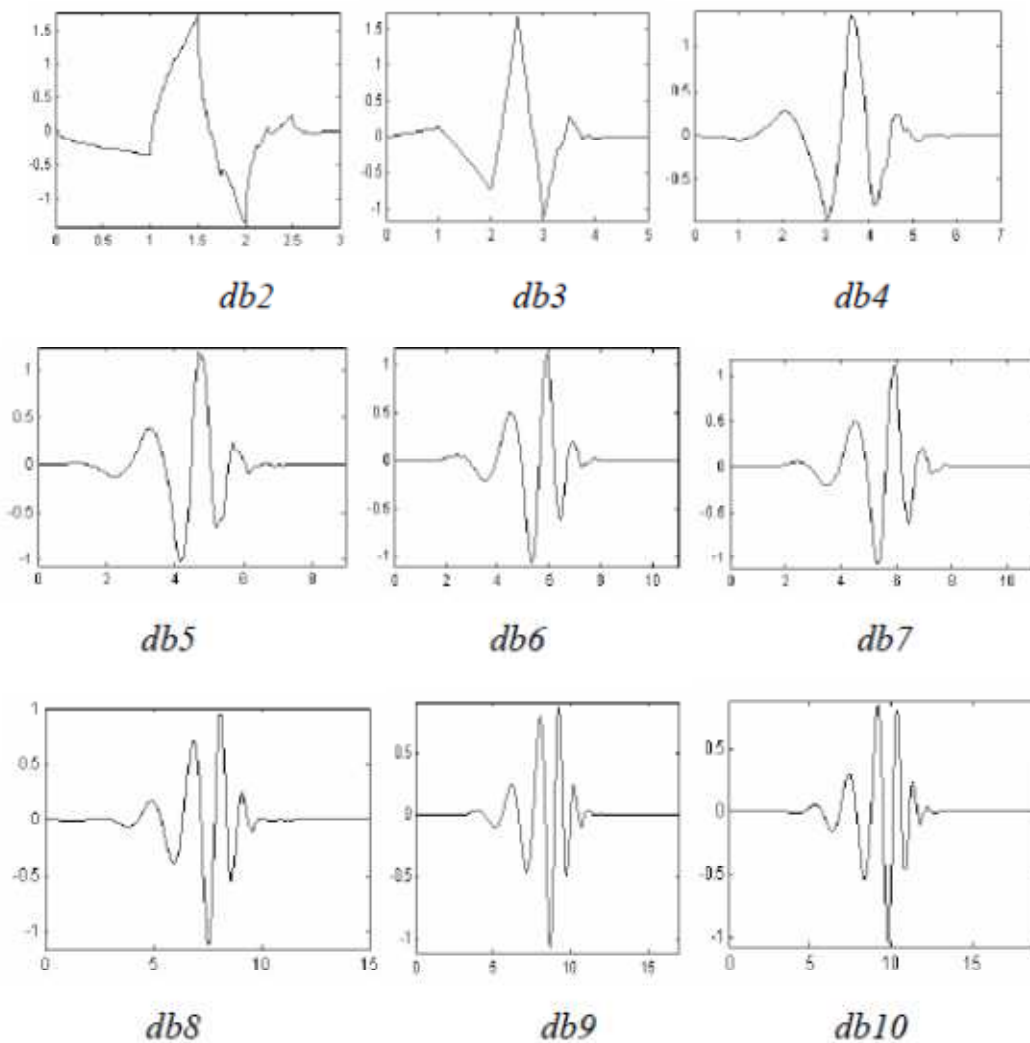
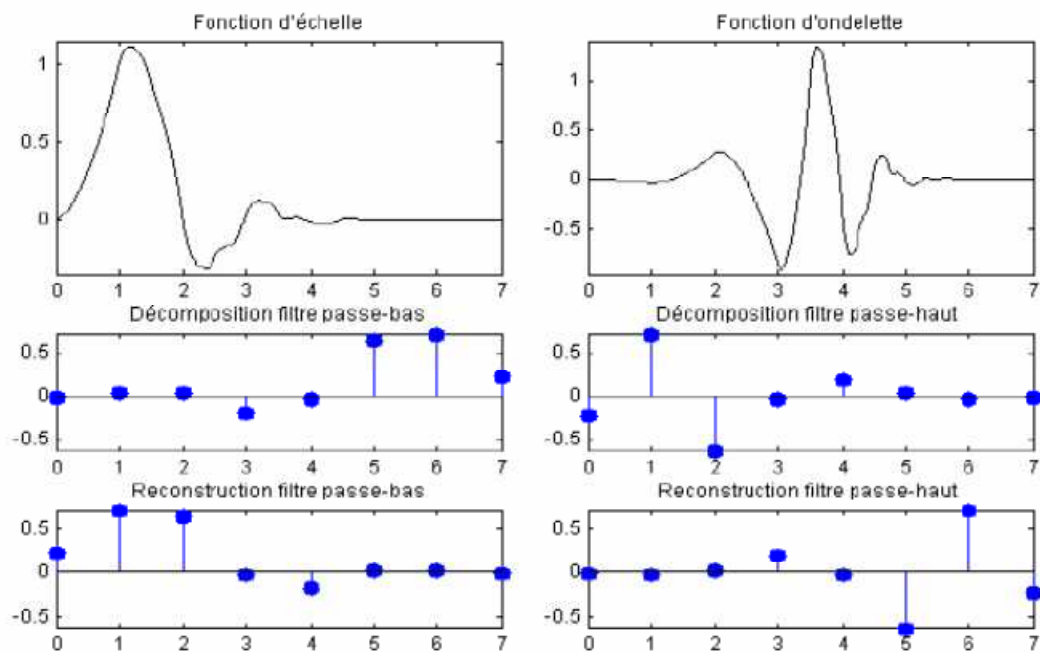
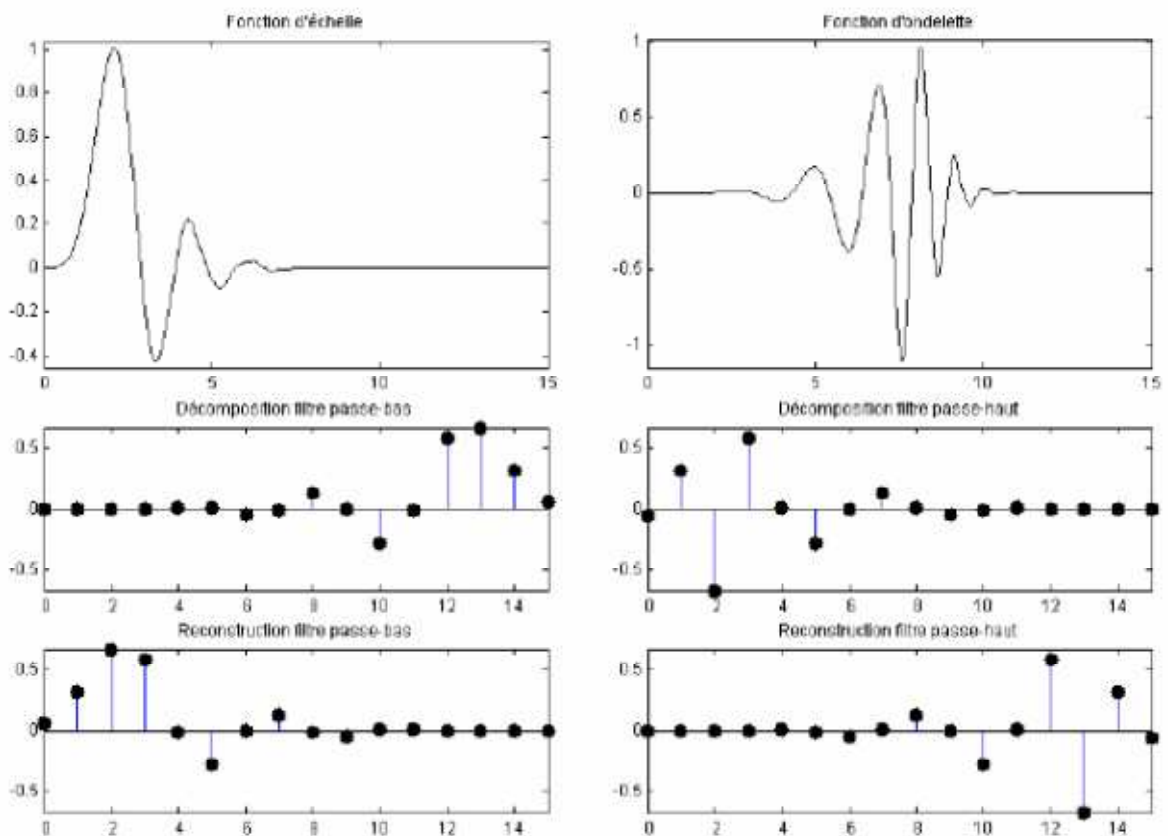


Figure III.7 : Les ondelettes de Daubechies.

Cette famille d'ondelettes possède les propriétés suivantes :

- Le support des ψ et de j sont de longueur $2N-1$. Le nombre de moments nuls de ψ est N ;
- Les ondelettes dbN sont asymétriques, en particulier pour les faibles valeurs de N , sauf l'ondelette de Haar ;
- La régularité augmente avec l'ordre ;
- L'analyse est orthogonale.

Pour les deux types d'ondelettes $db4$ et $db8$, on trouve dans les figure (Figure. III.8 et Figure. III.9) en plus de l'ondelette, la fonction d'échelle et les quatre filtres associés (deux pour la décomposition, deux pour la reconstruction).

Figure III.8:Ondelettes de Daubechies (*db4*).Figure III.9:Ondelettes de Daubechies (*db8*).

III.8.3. Ondelettes de Symlets:

Les symlets ($symN$) constituent une famille d'ondelettes presque symétrique, proposée par I. Daubechies en modifiant la construction des dbN . A part la symétrie, les autres propriétés des deux familles sont similaires. Les symlets d'ordre 2 à 8 ($sym1$ est simplement l'ondelette de Haar) sont présentées dans la figure (Figure III.10) [48]. De plus, pour deux d'entre elles ($sym4$ et $sym8$), on trouve dans les figures (Figure. III.11 et Figure. III.12) en plus de l'ondelette, la fonction d'échelle et les quatre filtres associés (deux pour la décomposition, deux pour la reconstruction).

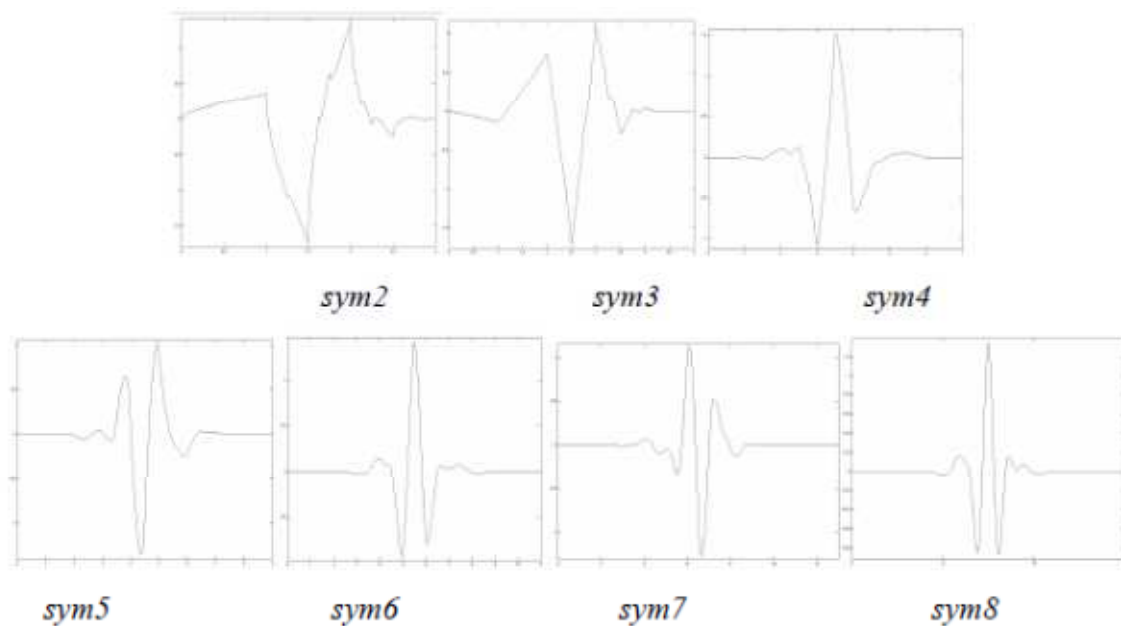


Figure III.10: Les ondelettes de symlets.

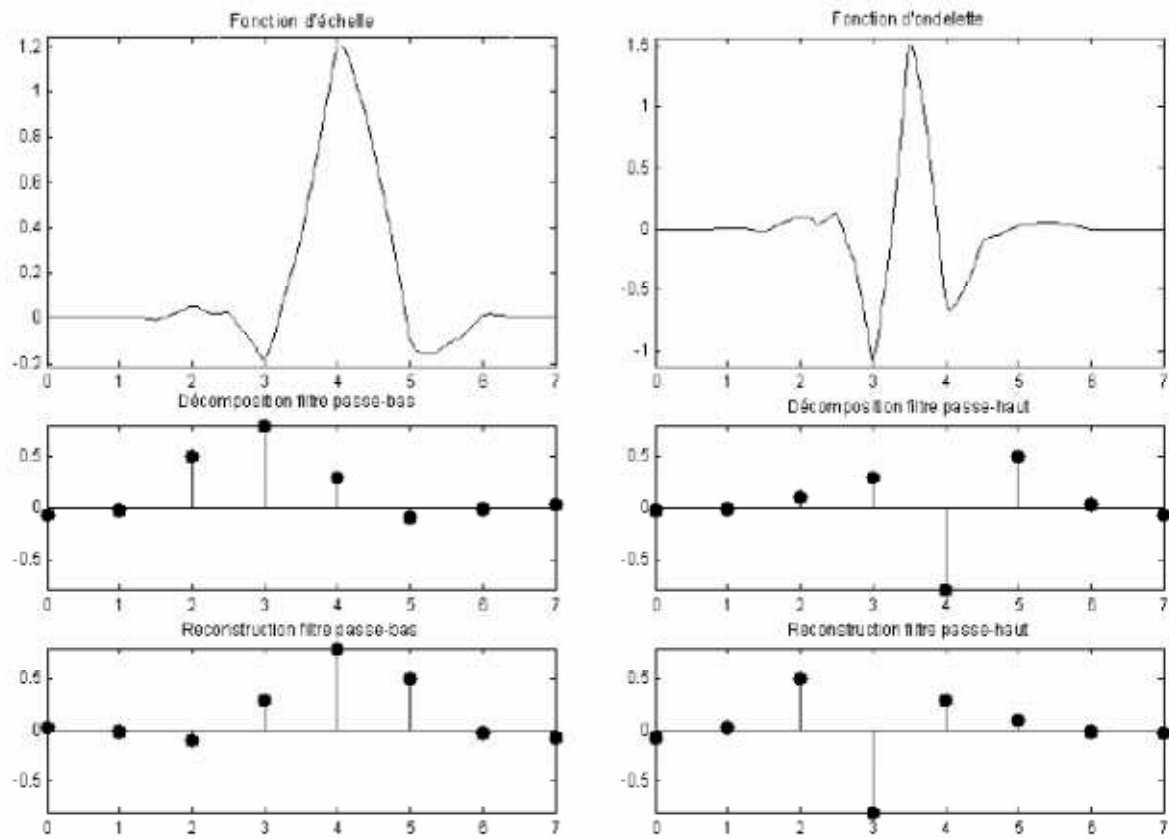


Figure III.11: Ondelettes de Symlets (*sym4*).

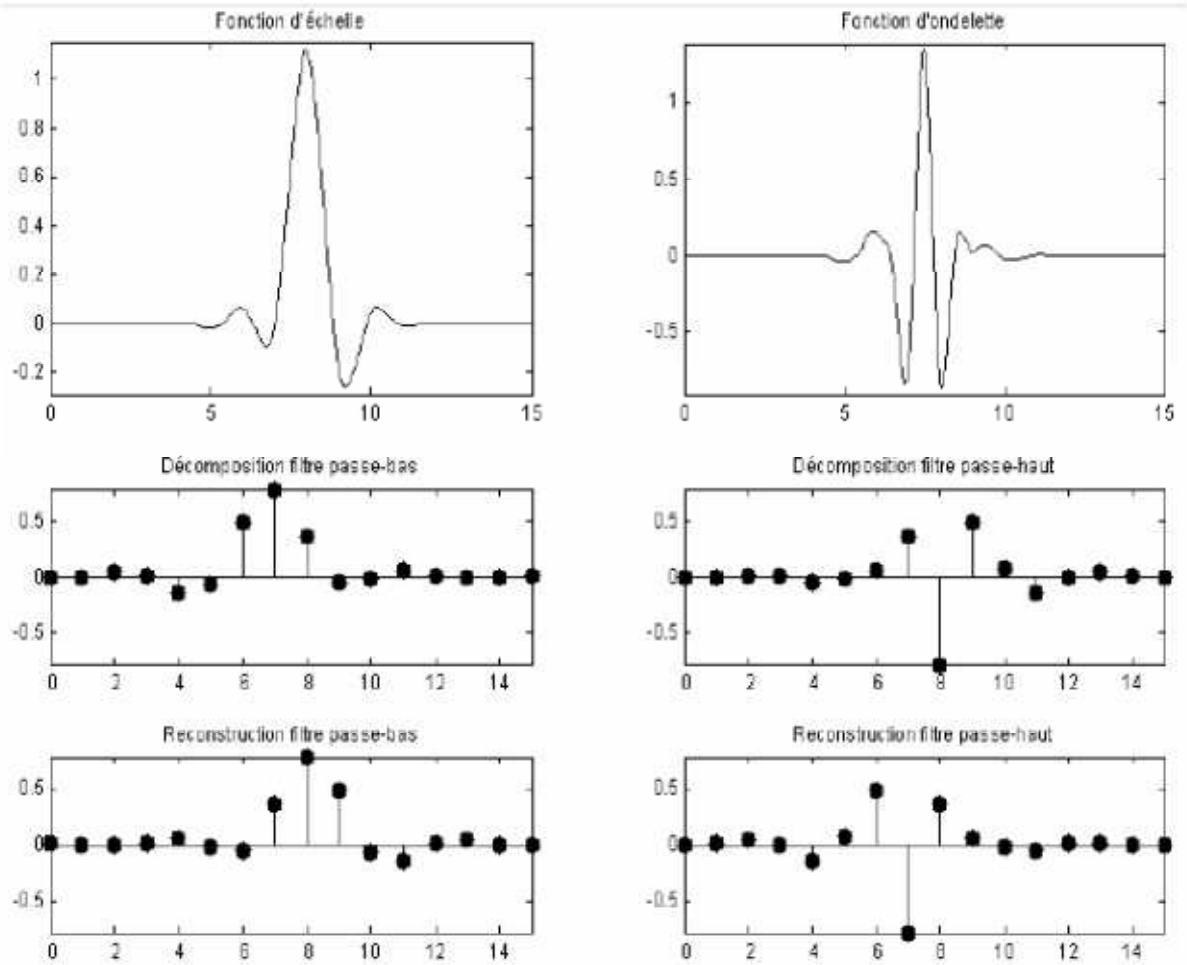


Figure III.12 : Ondelettes de Symlets (*sym8*).

III.8.4. Ondelettes de Coiflets:

Construite par I. Daubechies sur la demande de R. Coifman [48], les coiflets (*coifN*) constituent une famille d'ondelettes possédant une propriété inhabituelle. Non seulement, comme pour les deux familles précédentes, l'ondelette ϕ associée à *coif N* à $2N$ moments nuls. Les deux fonctions ϕ et φ ont un support de longueur $6N-1$. Les coiflets d'ordre 1 à 5 sont représentés à la figure (Figure. III.13).

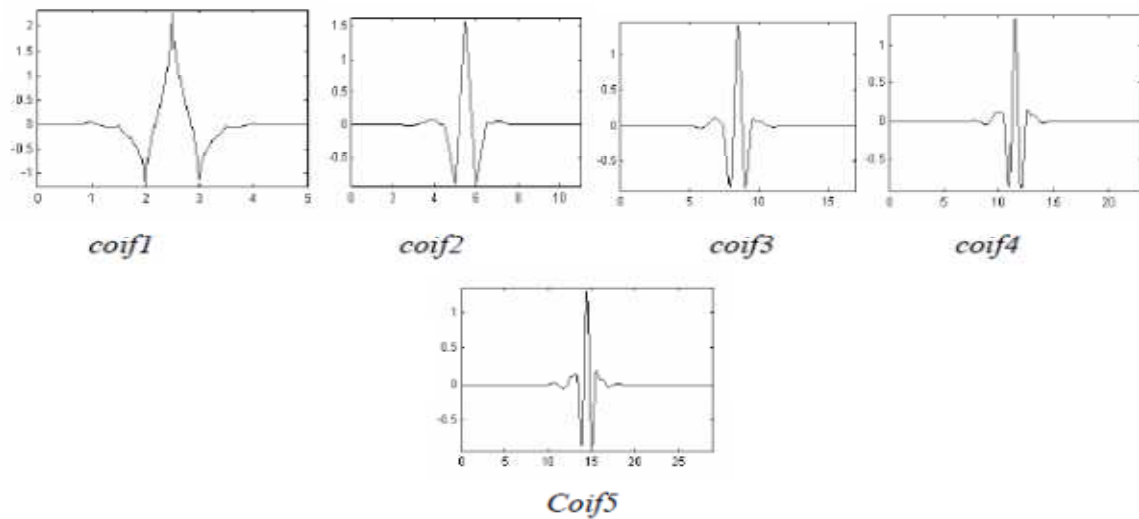


Figure III.13 : Les ondelettes de coiflets.

Pour deux d'entre elles (*coif3* et *coif5*), on trouve dans les figures (Figure. III.14 et Fig. III.15) l'ondelette, la fonction d'échelle et les quatre filtres associés.

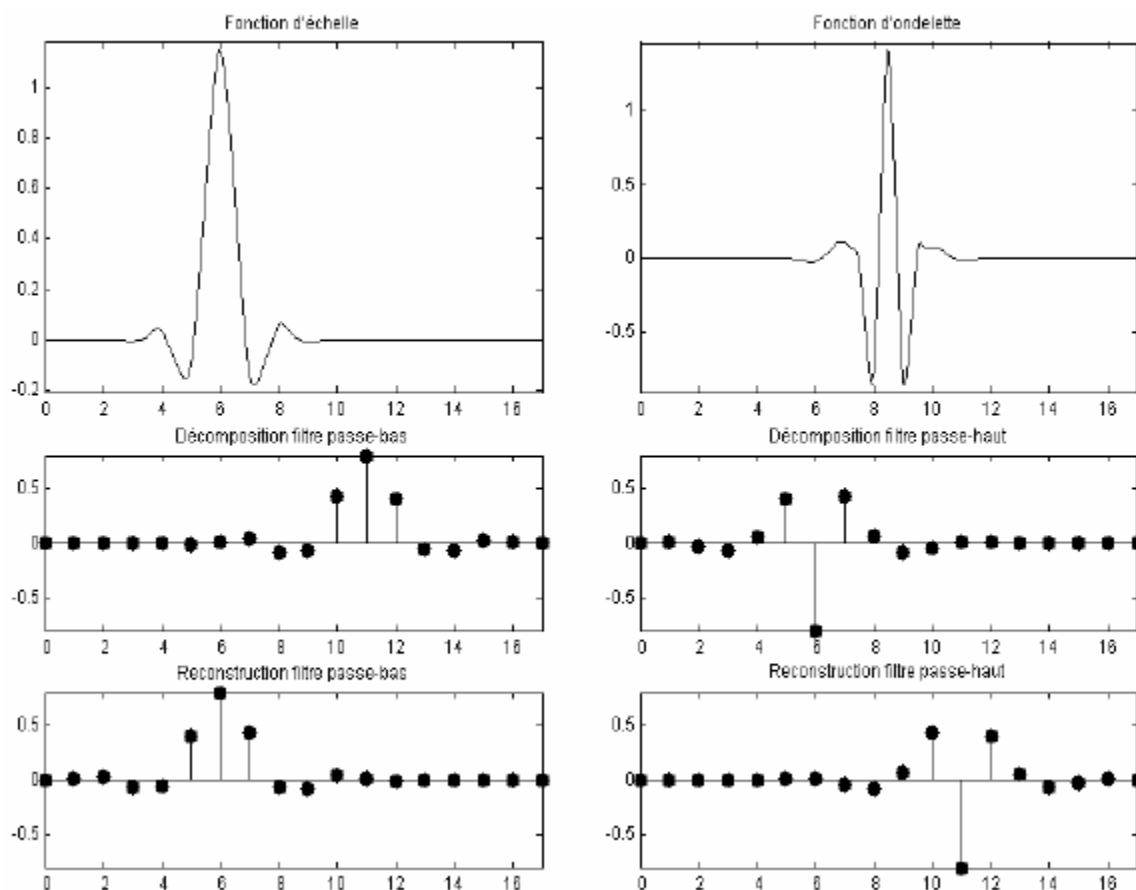


Figure III.14:Ondelettes de Coiflet (*coif3*).

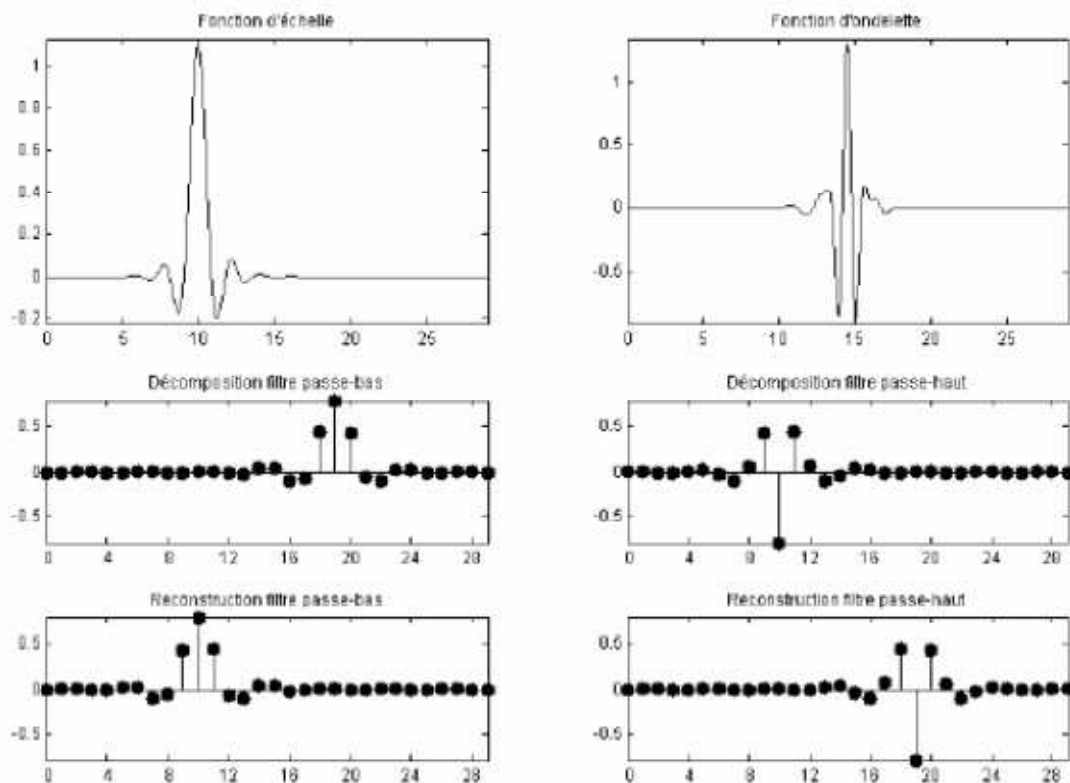


Figure III.15 : Ondelettes de Coiflet (coif5).

III.9. Les avantages de la transformée en ondelettes :

Le fait que la transformée utilise des fonctions bien localisées dans le plan temps-fréquence lui donne beaucoup d'avantages [44] :

- La résolution en fréquence de la transformée dépend du facteur de dilatation par le principe de Heisenberg, on peut donc choisir arbitrairement celle-ci suivant ce que l'on désire analyser.
- Pour des signaux physiques présentant des variations très rapides et des discontinuités, l'analyse en ondelettes est adaptée car l'ondelette va détecter ces variations et les analyser. Cette particularité rend l'analyse en ondelettes complémentaire à l'analyse de Fourier. En effet, avec l'analyse de Fourier, les discontinuités d'un signal ne sont pas facilement analysables.
- La localisation en temps est précieuse pour beaucoup d'applications.
- La transformée en ondelette peut représenter complètement et efficacement un signal quelconque avec peu de coefficients.

III.10. Conclusion :

Les ondelettes sont considérées comme une découverte importante en mathématiques appliqués. Dans plusieurs domaines d'applications où l'analyse de Fourier était habituellement utilisée, elles ont proposé une voie alternative souvent mieux adaptée à la nature des phénomènes étudiés.

L'étude approfondie qui a été menée dans ce chapitre a permis de mieux cerner les bases théoriques, les propriétés et les caractéristiques de la transformée en ondelettes, et mieux apprécier leurs avantages ainsi que leurs inconvénients dans l'analyse des signaux en général, et le traitement d'image en particulier.

Dans le chapitre suivant on parlera de la modélisation des paramètres et classification.

Chapitre IV :

MODELISATION DES PARAMETRES ET DECISION

IV.1. Introduction:

Après extraction des paramètres pertinents du visage et obtention des vecteurs DWT qui représentent le visage, on associe à chaque personne un modèle unique qui le caractérise à l'aide d'une fonction mathématique.

Ces modèles de caractéristiques discriminantes feront l'objet de reconnaissance des individus testés, et cela à l'aide d'un classificateur qui se base sur une méthode de classification par mesure de similarité avec les quatre distances respectivement, Euclidienne, Mahalanobis- Cosine, la norme Ctb et Cosine.

Nous présentons au cours de ce chapitre l'approche de modélisation par l'Analyse en composantes principales (PCA) et les distance utiliser pour la classification.

IV.2. Réduction de dimensionnalité :

Les techniques de réduction de dimensionnalité sont un ensemble de techniques mathématiques utilisées pour représenter des données disponibles dans un espace de faibles dimensions. Ces techniques issues de travaux en statistiques permettent d'obtenir une représentation réduite ou compressée des données originales tout en conservant les caractéristiques les plus importantes pour les traitements subséquents (Bengio et al, 2004, 2004b, 2006, Van der Maaten et al, 2001, 2009, Cai, 2009, Ghodsi, 2006, Saul, 2005).

La réduction de dimensionnalité permet d'obtenir une représentation d'un ensemble de données en tant qu'espace topologique de dimension p incorporé dans un espace de dimension m où $p < m$ (avec m la dimension des données originales et p la dimension des données réduites).

Les techniques de réduction de dimensionnalités peuvent être classifiées en utilisant trois caractéristiques (Journaux et al., 2006) :

- **Linéaire / non linéaire** : en fonction du type de transformation appliquée aux données (mapping).
- **Local / global** : basées sur les propriétés préservées par la transformation (dans la plupart des méthodes non linéaires, il y a un compromis entre la préservation des relations topologiques locales et la structure globale des données).
- **Euclidienne / géodésique** : sur la base de la fonction de distance utilisée pour estimer si deux données sont proches les unes des autres avant et après la transformation.

Dans la littérature scientifique, on peut retrouver d'autres types de classifications (Bengio et al, 2004, 2004b, 2006, Ghodsi, 2006) : convexes, non-convexes, spectrales, denses, éparses, etc.

En reconnaissance des visages, les techniques de réduction de dimensionnalité sont utilisées pour l'apprentissage des sous-espaces des visages et pour la reconnaissance des données extraites à partir d'images du visage. Dans le spectre infrarouge, la plupart des techniques utilisées sont des techniques linéaires.

La majorité des techniques de réduction de dimensionnalité est inspirée de la technique PCA. Ces dernières années, plusieurs auteurs (Yu et al, 2012, Bengio et al, 2004, 2004b, 2006, Ghodsi, 2006) ont démontré une relation directe entre diverses techniques non linéaires et la technique PCA. La majorité des techniques non linéaires sont une généralisation de la technique PCA où les données sont transformées de manière non linéaire avant leur projection dans un espace propre (Eigen space).

IV.2.1. Définition d'analyse en composantes principale :

La technique des Eigen faces [49] a été développée par (Turk et al, 1991). Elle est basée sur l'analyse en composantes principales (PCA). Cette analyse permet d'obtenir les vecteurs propres (correspondants aux plus grandes valeurs propres) qui formeront la base où sera représentée l'image du visage, d'où le nom de Eigen faces (Figure IV.1). Cette approche permet une réduction de dimensionnalité en projetant l'image du visage dans un espace de dimensions inférieures. Les coefficients de projection sont utilisés lors de la phase de reconnaissance.

L'approche des Eigen faces permet une réduction de dimensionnalité et une représentation sous-espace dans un prolongement topologique. Une représentation moyenne des images des visages est construite à partir de l'ensemble d'images utilisées lors de l'apprentissage. Cette image et l'ensemble d'apprentissage sont ensuite utilisés pour extraire les vecteurs propres représentatifs de l'espace des visages.

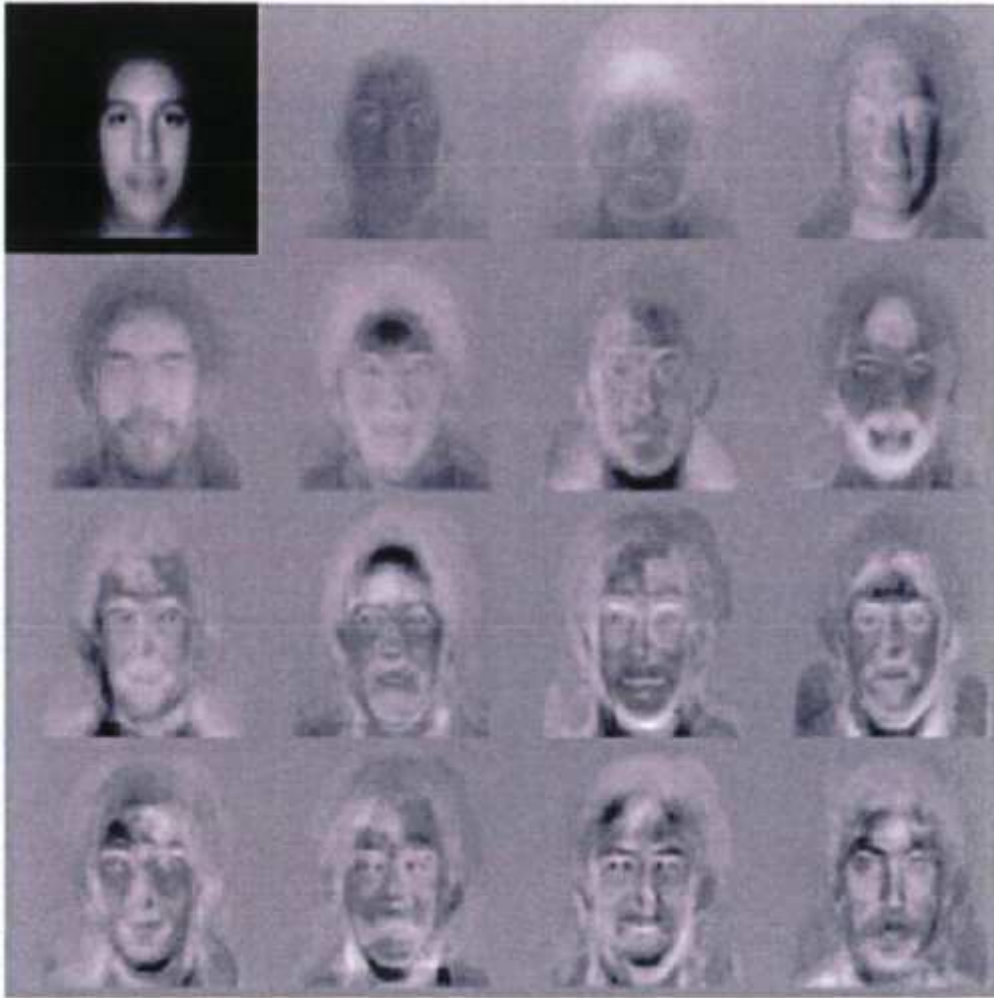


Figure IV.1 : Exemple d'Eigen faces (MIT 2012).

Supposons qu'on a un vecteur de dimensions m représentant l'image d'un visage, l'algorithme des Eigen faces permet d'en obtenir une décomposition en composantes principales. Il permet de retrouver le sous-espace ayant une direction de ses bases selon le maximum de variance de l'espace original. Soit F , une transformation linéaire (mapping) de l'espace original de dimensions m au sous-espace de dimensions n avec $n \ll m$.

Le nouveau vecteur est défini par : $v_i = F x_i$. Les colonnes de F sont les vecteurs propres obtenus en résolvant l'équation : $A \backslash vt = Q v_i$, avec Q étant la matrice de covariance. En supposant que l'ensemble des visages utilisés lors de l'apprentissage est une bonne représentation des diverses images de visages, alors les vecteurs sélectionnés sont une bonne représentation de tous les visages possibles (Turk et al, 1991, Socolinsky et al, 2001, Selinger et al, 2002). En sélectionnant les vecteurs propres correspondants aux valeurs propres les plus grandes, on construit un sous-espace de projection des images des visages de dimension réduite. Les étapes de l'algorithme des Eigenfaces sont présentées dans la suite :

IV.2.2. Modélisation par la méthode PCA :

La phase de modélisation se fait hors ligne et consiste à générer l'espace de projection des Eigenfaces à partir d'une base de données de vecteur caractéristiques du visage.

1. Soit un ensemble de M matrices de dimensions $N * N$: L_i avec $1 \leq i \leq M$.
2. Transformer les matrices L_i , de dimension $N * N$ en un vecteur Γ_i , de dimensions $N^2 * 1$ en superposant les colonnes de chaque image (figure IV.2).

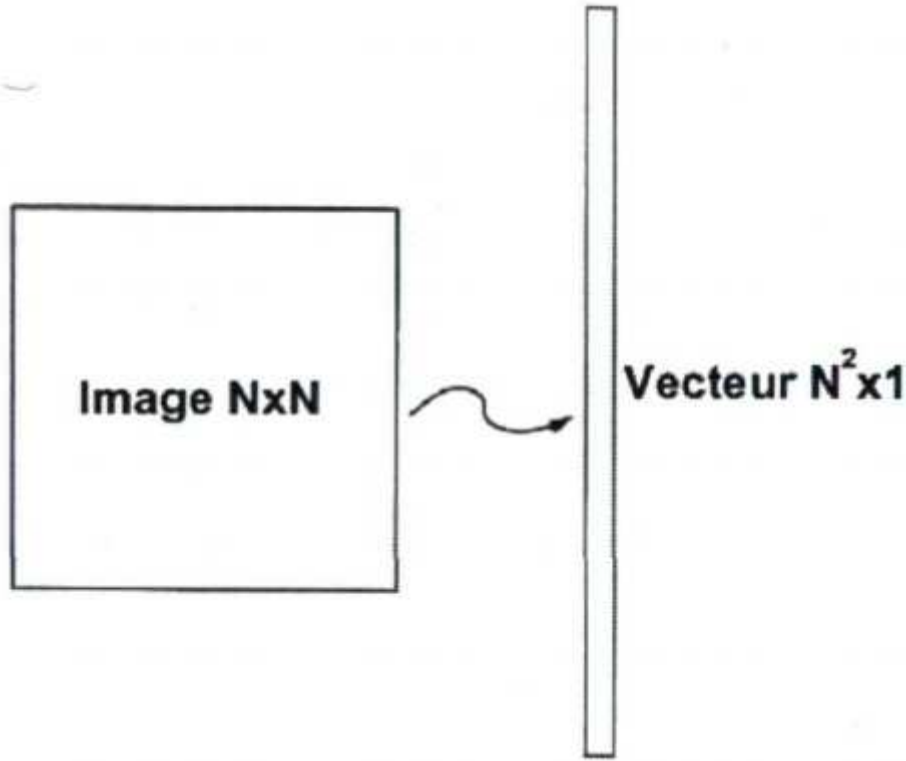


Figure IV.2 : Transformation de la matrice image $N * N$ en vecteur $N^2 * 1$.

3. Calculer le vecteur moyen des images du visage ψ par : $\psi = \frac{1}{M} \sum_{i=1}^M \Gamma_i$.
4. Soustraire le vecteur moyen des vecteurs représentant les images : $\phi_i = \Gamma_i - \psi$.
5. Calculer la matrice de covariance :

$$C = \frac{1}{M} \sum_{n=1}^M \phi_n \phi_n^T = AA^T \text{ (Matrice de dimension } N^2 * N^2 \text{). Ou } (A = [\phi_1 \phi_2 \dots \phi_M]).$$

6. Calculer les vecteurs propres U_i , de la matrice de covariance $C = AA^T$. La matrice AA^T est très grande $N^2 * N^2$, donc le calcul des vecteurs propres peut s'avérer très coûteux en temps de calcul. Turk et al (1991) ont proposé de résoudre un système de plus petite dimension : Calculer les vecteurs propres V_i , de la matrice $A^T A$ dont la dimension est de $M * M$.

AA^T et $A^T A$ ont les mêmes valeurs propres et leurs vecteurs propres sont reliés par l'équation suivante : $U_i = A * V_i$.

$A^T A$ à M valeurs propres correspondantes au M plus grandes valeurs propres de AA^T .

À cette étape, on calcule les M vecteurs propres U_i de AA^T correspondant aux M plus grandes valeurs propres, en utilisant l'équation : $U_i = A * V_i$ (Il est important de normaliser les vecteurs U_i , afin d'avoir $\|U_i\| = 1$).

7. Garder les K vecteurs propres correspondants aux K plus grandes valeurs propres (avec $K \leq M \ll N^2$).

IV.2.3. Représentation de l'image du visage dans l'espace des Eigen faces :

Les vecteurs propres calculés précédemment représentent les vecteurs de base de l'espace des Eigen faces où on projette les images du visage.

Une image du visage à laquelle on a soustrait la moyenne des visages peut être représentée par une combinaison linéaire des K vecteurs propres :

$$\phi_i = \Gamma i - \Psi = \sum_{j=1}^K W_j U_j. \quad \text{On a } W_j = U_j^T \phi_i.$$

Ainsi, chaque image du visage ϕ_i , peut être représentée dans la base des Eigen faces U_j par le vecteur:

$$\Omega_i = \begin{pmatrix} W_1^i \\ W_2^i \\ \vdots \\ W_K^i \end{pmatrix} \quad i = 1, 2, 3, \dots, M.$$

IV.2.4. Décision :

Dans le cas de l'identification, il s'agit d'examiner les modèles retenus par un agent humain et donc décider. En ce qui concerne l'authentification, la stratégie de décision nous permet de choisir entre les deux alternatives suivantes : l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ou elle ne correspond pas. Elle est basée sur un **seuil** prédéfini. L'estimation du seuil de la décision constitue la plus grande difficulté de ces techniques, et elle peut engendrer deux types d'erreurs, souvent prises comme mesures de performances pour ces techniques d'authentification: faux rejet (**FRR**) et fausse acceptation (**FAR**). Bien sûr, un système d'authentification idéal est celui qui donne $FAR=FRR=0$. Malheureusement, dans les conditions réelles, ceci est impossible. Par conséquent, un compromis doit être fait dans le choix du seuil, et ce dernier est très dépendant de l'application.

IV.2.5. Seuil :

Dans le problème de vérification d'identité, nous cherchons à définir, pour chaque personne, ou de manière globale un seuil. Ce seuil va déterminer le minimum de ressemblance entre deux images pour admettre qu'il s'agit de la même personne.

Ce minimum de ressemblance va s'exprimer comme une distance maximale entre les caractéristiques des deux images. Pour fixer ce seuil l'ensemble d'évaluation est utilisé. Deux distances sont calculées :

La distance intra classe (**distance_intra**) : La distance entre deux images de visage de même individu.

La distance extra classe (**distance_extra**) : La distance entre deux images de visage de deux individus différents.

Théoriquement on le calcule **Seuil** = $(\max(\text{distance_intra}) + \min(\text{distance_extra})) / 2$.

IV.3. Différentes distances utiliser pour la classification [50] :

Lorsqu'on souhaite comparer deux vecteurs de caractéristiques issus du module d'extraction de caractéristiques d'un système biométrique, on peut soit effectuer une mesure de similarité (ressemblance), soit une mesure de distance (divergence).

Dans le cadre de notre travail on s'est intéressé aux quatre distances suivantes: Euclidienne(L2), Cosinus de Mahalanobis (MahCosine), Cosine et la norme Ctb.

La première catégorie de distances est constituée de distances Euclidiennes et sont définies à partir de la distance de Minkowski d'ordre p dans un espace euclidien (déterminant la dimension de l'espace euclidien).

Considérons deux vecteurs $X = (x_1, x_2, \dots, x_n)$ et $Y = (y_1, y_2, \dots, y_n)$, la distance de Minkowski d'ordre p notée L_p est définie par :

$$L_p = \left(\sum_{i=1}^n (|x_i - y_i|)^p \right)^{1/p}$$

Nous allons présenter quelques mesures de distance dans l'espace original des images puis dans l'espace de Mahalanobis.

IV.3.1. Distances Euclidiennes:

Dans le cadre de notre travail on a utilisé seulement la distance L2.

1. Distance City Block (L1) :

Pour $p = 1$, on obtient la distance City-Block (ou distance de Manhattan) :

$$L_1(x, y) = \sum_{i=1}^n |x_i - y_i|$$

2. Distance Euclidienne (L2):

Pour $p = 2$, on obtient la distance euclidienne :

$$L_2(x, y) = \sqrt{\sum_{i=1}^n |x_i - y_i|^2}$$

Les objets peuvent alors apparaître de façons très différentes selon la mesure de distance choisie.

IV.3.2. Distance Cosine (cosinus):

La **similarité cosinus** (ou **mesure cosinus**) permet de calculer la similarité entre deux vecteurs à n dimensions en déterminant le cosinus de l'angle $\cos \theta$ entre eux.

Soit deux vecteurs A et B, l'angle $\cos \theta$ s'obtient : par le produit scalaire et la norme des vecteurs comme suit :

$$\cos \theta = \frac{A \cdot B}{\|A\| \cdot \|B\|}$$

Comme la valeur $\cos \theta$ est comprise dans l'intervalle $[-1, 1]$ la valeur -1 indiquera résolument opposés, 0 vecteurs indépendants (orthogonaux) et un des vecteurs similaires (de coefficient positif) les valeurs intermédiaires permettent d'évaluer le degré de similarité.

IV.3.3. Distances dans l'Espace de Mahalanobis :

1. De l'espace des images à l'espace de Mahalanobis :

Avant de pouvoir effectuer des mesures de distance dans l'espace de Mahalanobis, il est essentiel de bien comprendre comment l'on passe de l'espace des images Im à l'espace de Mahalanobis $\mathcal{EMah}$. En sortie de l'algorithme PCA, nous obtenons des vecteurs propres associés à des valeurs propres (représentant la variance selon chaque dimension). Ces vecteurs propres définissent une rotation vers un espace dont la covariance entre les différentes dimensions est nulle. L'espace de Mahalanobis est un espace où la variance selon chaque dimension est égale à 1. On l'obtient à partir de l'espace des images Im en divisant chaque vecteur propre par son écart-type correspondant.

Soit u et v deux vecteurs propres de Im , issus de l'algorithme PCA, et m et n deux vecteurs de $\mathcal{EMah}$. Soit λ_i les valeurs propres associées aux vecteurs u et v , et σ_i l'écart-type, alors on définit $\lambda_i = \sigma_i^2$. Les vecteurs u et v sont reliés aux vecteurs m et n à partir des relations suivantes :

$$m_i = \frac{u_i}{\sigma_i} = \frac{u_i}{\sqrt{\lambda_i}} \text{ et } n_i = \frac{v_i}{\sigma_i} = \frac{v_i}{\sqrt{\lambda_i}}$$

2. Mahalanobis L1 (MahL1):

Cette distance est exactement la même que la distance City-Block sauf que les vecteurs sont projetés dans l'espace de Mahalanobis. Ainsi, pour des vecteurs propres u et v de projections respectives m et n sur l'espace de Mahalanobis, la distance Mahalanobis L1 est définie par :

$$Mah_{L1}(u, v) = \sum_{i=1}^N |m_i - n_i|$$

3. Mahalanobis L2 (MahL2) :

Cette distance est identique à la distance euclidienne à part qu'elle est calculée dans l'espace de Mahalanobis. Ainsi, pour des vecteurs propres u et v de projections respectives m et n sur l'espace de Mahalanobis, la distance Mahalanobis L2 est définie par :

$$Mah_{L2}(u, v) = \sqrt{\sum_{i=1}^N |m_i - n_i|^2}$$

4. Cosinus de Mahalanobis (MahCosine):

Il s'agit tout simplement du cosinus de l'angle entre les vecteurs u et v , une fois qu'ils ont été projetés sur et normalisés par des estimateurs de la variance.

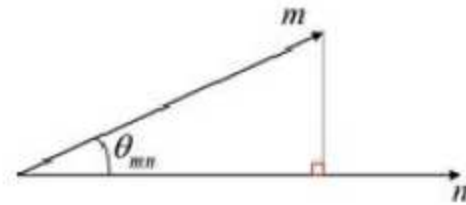


Figure IV.3 : Les deux vecteurs m et n dans l'espace de Mahalanobis.

Nous avons donc par définition :

$$S_{Mahcosine}(u, v) = \cos(\theta_{mn})$$

De plus, on peut écrire :

$$\cos(\theta_{mn}) = \frac{|m||n|\cos(\theta_{mn})}{|m||n|}$$

D'où la formule finale de la mesure de similarité *MahCosine*:

$$S_{Mahcosine}(u, v) = \frac{mn}{|m||n|}, D_{Mahcosine}(u, v) = -S_{Mahcosine}(u, v)$$

Où $DMahcosine(u, v)$ est la mesure de distance équivalente. On peut enfin noter qu'il s'agit principalement de la covariance entre les vecteurs dans l'espace de Mahalanobis.

IV.4. Conclusion :

Nous avons vu dans ce chapitre l'intérêt, le mode de fonctionnement de la méthode PCA pour la réduction de dimensions ou la modélisation, En deuxième lieu, nous nous sommes intéressées aux distances de classification. Nous verrons l'intérêt de ces dernières dans le chapitre Tests et Résultats. Pour le prochain chapitre on verra les différentes étapes pour la conception et réalisation de notre système.

Chapitre V :

CONCEPTION ET REALISATION

V.1. Introduction :

Ce Chapitre est consacré à l'étude analytique du fonctionnement du système, nous détaillerons l'implémentation structurelle ainsi que les différents concepts et approches informatiques utilisées pour la mise en œuvre de notre système. Nous débuterons par montrer les différents cas d'usage, en passant par les méthodes de mesure de performances, et enfin, la structure algorithmique et modulaire du système.

V.2. Conception :

Dans cette première partie du chapitre, nous présentons la composition d'un système de reconnaissance de visage en général, et celle de notre système en particulier, et cela en présentant les différentes approches adoptées, l'architecture des différents modules et classes constituant notre système et en montrant l'interaction entre ces derniers à travers plusieurs diagrammes.

V.2.1. Les acteurs du système :

1. L'Administrateur :

C'est la personne responsable de la gestion du système et de son bon fonctionnement, en effectuant plusieurs tâches :

- Gestion de la base de données.
- Enregistrement des nouveaux clients et suppression de ceux qui quittent le système.
- Maître à jour les informations des clients.
- Test et réglage des différents paramètres du système.

1. L'individu Test :

Est la personne qui soit demande une autorisation d'accès (authentification), ou qui va être identifiée.

V.2.2. Les diagrammes de cas d'utilisation du système :

Les cas d'utilisation vont nous permettre de préciser le contexte fonctionnel de notre système. Ci-dessous, nous montrerons les différentes façons d'utilisation du système proposé :

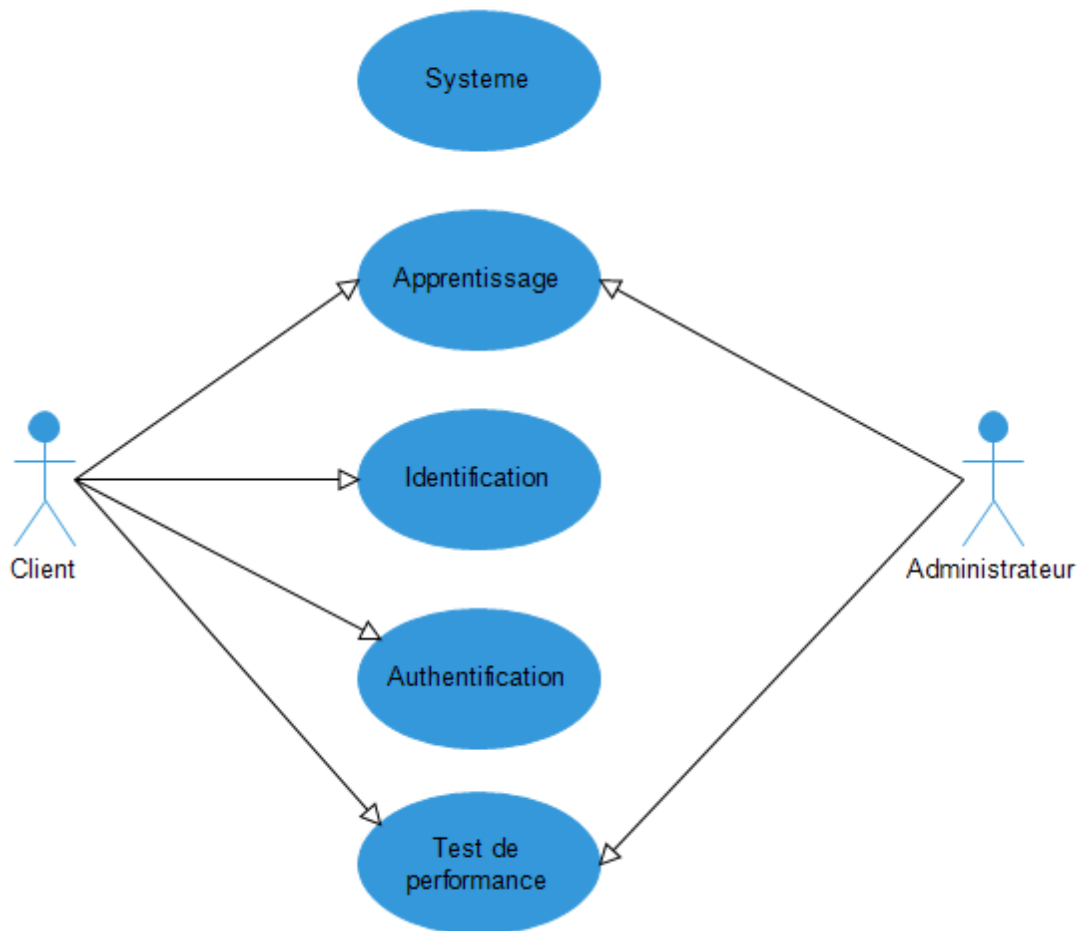


Figure V.1 :Diagramme de contexte du système.

1. Description du diagramme de contexte « Apprentissage » :

Titre : Enregistrement d'un nouveau client dans le système.

Résumé : Ce cas d'utilisation permet à l'administrateur de répondre aux demandes d'ajouts de nouveaux clients dans le système. Pour chacun, dix images du visage sont acquises, puis utilisées pour générer un modèle unique qui sera stocké avec les informations personnelles (nom du sujet) dans une base de données pour une utilisation ultérieure.

Acteur : le client, l'administrateur, webcam.

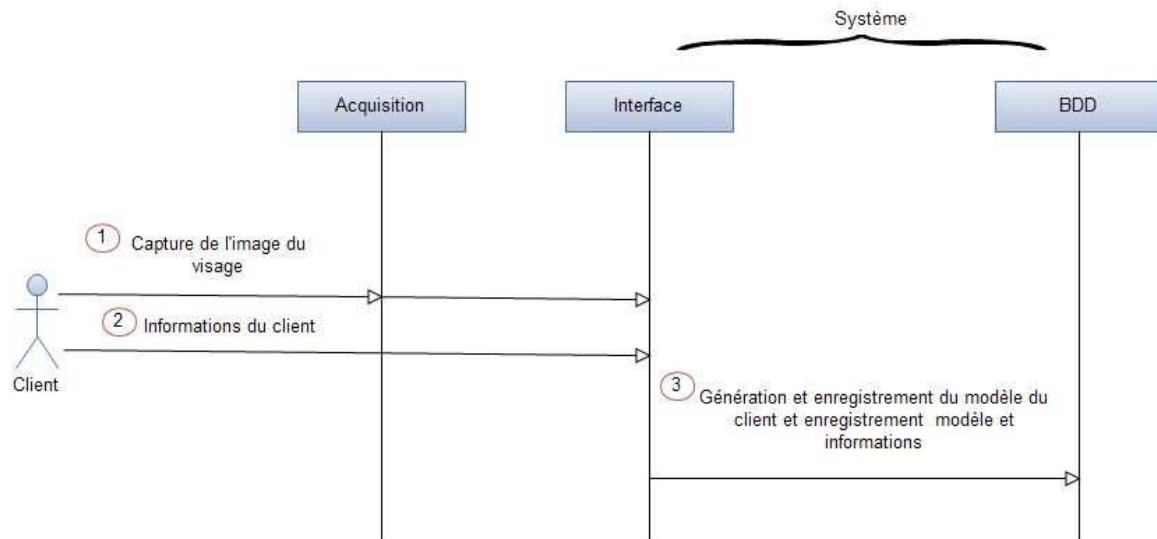


Figure V.2 :Description du cas d'apprentissage pour un nouveau client.

2. Description du cas d'utilisation « Identification » :

Titre : Identification d'un client.

Résumé : Quand l'utilisateur cherche à s'identifier, le système se charge de capter une image de lui. A partir de cette image et de l'ensemble de modèles stockés dans la base de données, le système définit l'identité de l'utilisateur.

Acteur : Client, webcam.

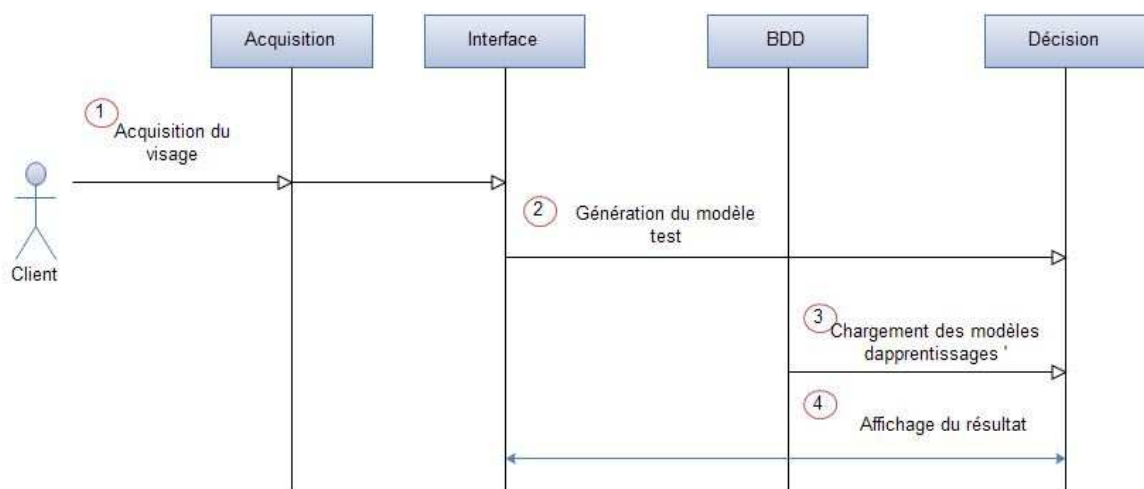


Figure V.3 :Description du cas d'apprentissage d'un client.

3. Description du cas d'utilisation « Authentification » :

Titre : Authentification d'un client.

Résumé : C'est le cas d'un individu qui proclame une identité pour une autorisation d'accès par exemple. Le système prend une image de son visage pour vérifier si elle correspond à l'identité proclamée ou pas.

Acteur : Client, webcam.

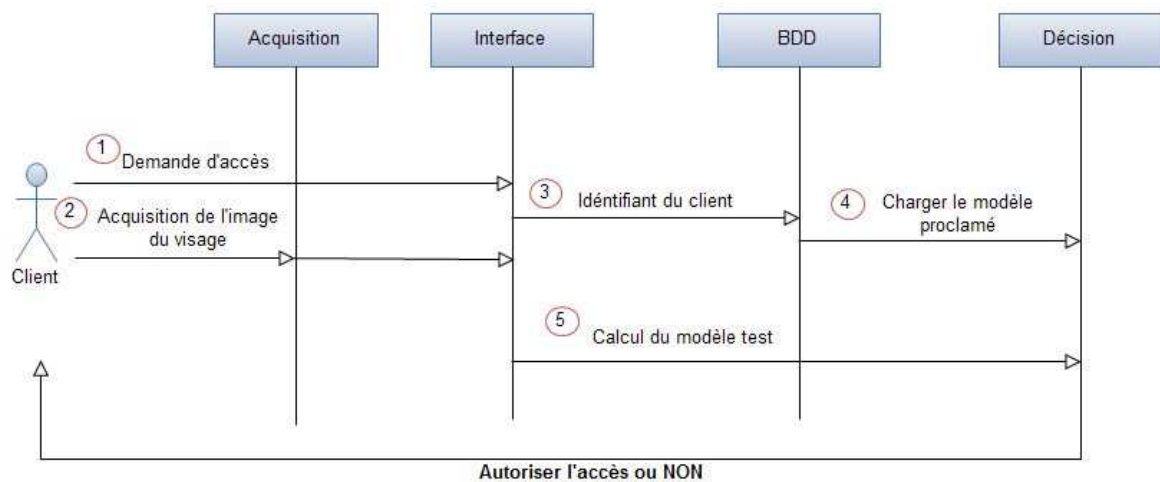


Figure V.4 : Description du cas d'authentification d'un client.

4. Description du cas d'utilisation « test des performances » :

Titre : Test des performances du système.

Résumé : Dans ce cas, l'Utilisateur fait des tests sur une base d'images donnée, en variant un ou plusieurs paramètres du système. Ceci, afin d'évaluer le système, mesurer les performances et calculer les paramètres optimaux adéquats pour cette base.

Acteur : Client, webcam.

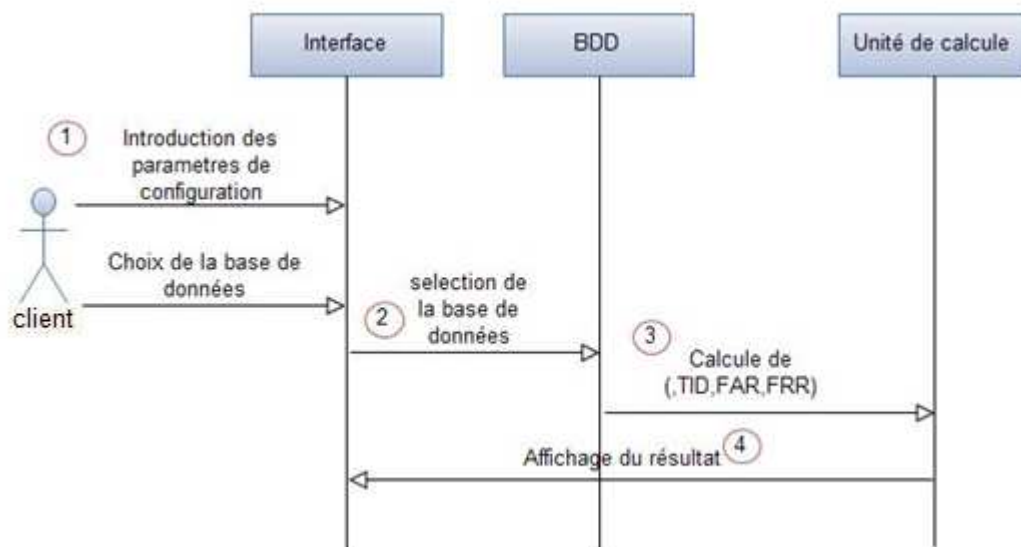


Figure V.5 : Description du cas d'authentification d'un client.

V.2.3. Architecture et fonctionnement du système :

Le système de reconnaissance de visage qu'on propose, se compose de deux unités principales (Figure IV.6) : apprentissage et reconnaissance.

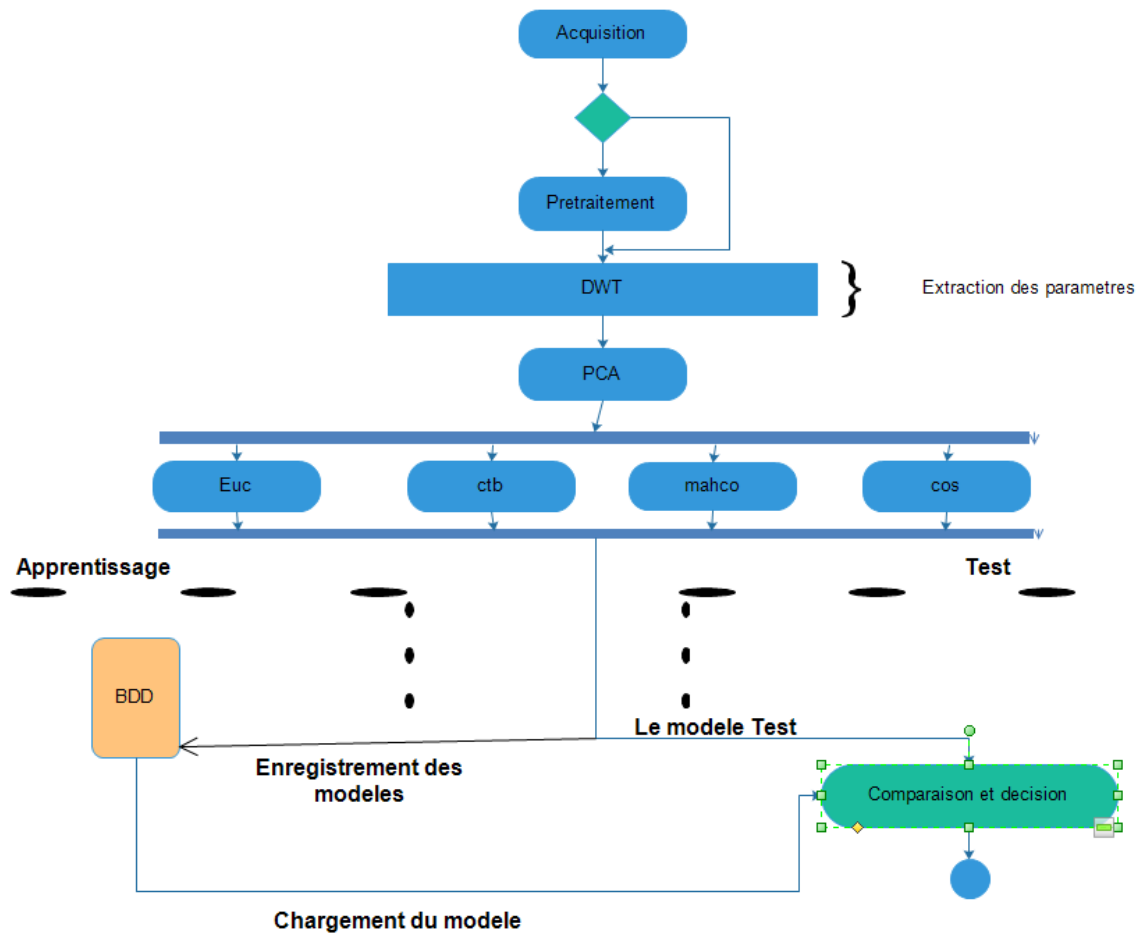


Figure V.6 :Diagramme d'activité du système.

Nous détaillerons ci-dessous les modules qui constituent chaque unité, ainsi que les algorithmes utilisés.

1. L'Apprentissage :

Fonctionnement du système en phase d'apprentissage :

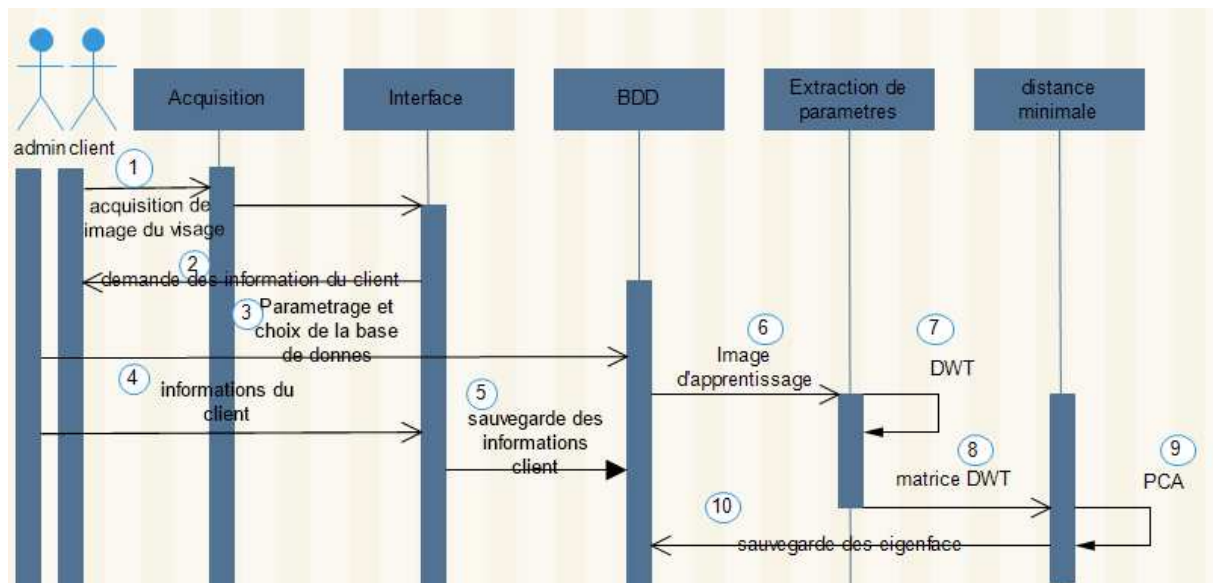


Figure V.7 :Diagramme de séquence Apprentissage.

Description du scénario d'apprentissage :

- Le client introduit au système un ensemble d'image de son visage.
- Le système demande au client d'introduire ses informations.
- L'administrateur choisi les paramètres du système et la base de données d'enregistrement.
- Le client introduit les informations demandées.
- Le système sauvegarde les informations entrées par L'utilisateur et l'ensemble de ses images dans la base de données.
- On prend n images de la base de données pour faire l'apprentissage.
- L'extraction des paramètres de l'ensemble des images d'apprentissage en utilisons l'approche DWT.
- Le résultat (Matrices DWT) s
- Projection sur un espace de vecteur propre avec la méthode PCA.
- Sauvegarde du modèle PCA.

2. Découpage modulaire :

Le processus d'apprentissage est illustré ci-dessous (Figure IV.8) et les différents modules qui le composent sont détaillés par la suite :

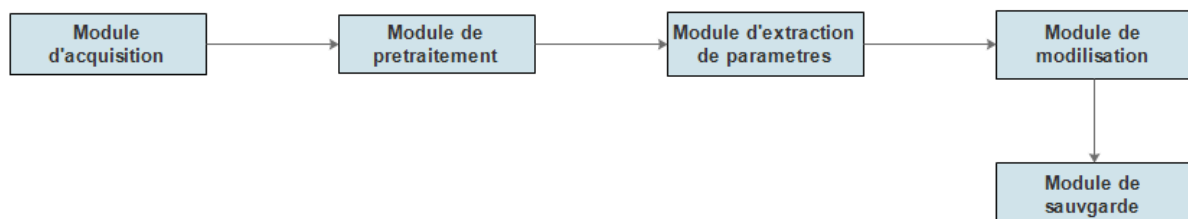


Figure V.8 :Représentation modulaire de la phase d'apprentissage.

3. Module d'acquisition :

L'acquisition de l'image de l'échantillon biométrique est la première étape du fonctionnement de tout système de reconnaissance biométrique. Elle consiste à extraire des informations du monde réel en utilisant des dispositifs appropriés à la modalité étudiée. Dans le cas de notre projet (reconnaissance du visage) cette phase suit le schéma suivant :



Figure V.9 :Processus d'acquisition.

➤ Localisation du visage

Elle se fait par la technique de détection des couleurs suivant trois étapes :

- Détection de l'ensemble des points ayant comme couleur celle de la peau.
- Calcul du centre de gravité de ces points.

Traçage d'un cadre qui englobe le visage ayant comme centre le point calculé auparavant.

La prise de l'image du visage se fait par une Webcam qui extrait la partie encadrée pour l'enregistrer et l'étudier plus tard.

4. Module de prétraitement :

Plusieurs facteurs peuvent diminuer la qualité de l'image lors de l'acquisition, notamment : la qualité du dispositif d'acquisition ou l'environnement d'acquisition. Voir figure IV.10.



Figure V.10 :Représentation de l'étape prétraitement.

5. Module d'extraction des paramètres :

Après prétraitements des images en niveaux de gris, qui représentent nos données, ce module permet d'extraire les caractéristiques pertinentes de chacune en appliquant l'approche DWT puis la projection de la matrice caractéristiques sur un espace de vecteur propre généré par la méthode PCA.

➤ **Algorithme DWT :**

Algorithme DWT

- 1) Découpage de l'image en quatre blocs de pixels à chaque itération (selon le Level « dans notre cas level 1 ») : les 3 derniers blocs concernent les détails de l'image (vertical, horizontal, diagonal), le premier bloc correspond à l'image détaillée.
- 2) Appliquer deux filtre (passe bas, passe haut) issue du choix d'ondelette à chaque bloc de pixel.
- 3) Construction de la matrice DWT à partir des coefficients (vecteur caractéristique) obtenu.

Remarque : la matrice DWT est formée par la concaténation de l'ensemble des vecteurs caractéristiques.

Figure V.11: Algorithme DWT.

6. Module de modélisation :

A partir des matrices DWT obtenues à l'aide du module d'extraction de paramètres, ce module qui est le plus important s'occupe de générer les modèles des personnes à partir d'un vecteur propre (Eigen face) en utilisant la méthode PCA.

Algorithme PCA

Entrées : chargement de la base d'apprentissage.

- 1) Calculer le vecteur moyen des images d'apprentissage du visage représenté par la matrice A .
- 2) Soustraire le vecteur moyen des vecteurs représentant l'image.
- 3) Calculer la matrice de covariance A^* .
- 4) Calculer les vecteurs propres V de la matrice $A * A^T$.
- 5) Les vecteurs propres calculés précédemment représentent les vecteurs de base de l'espace des Eigen faces ou on projette les images du visage.

Figure V.12: Algorithme PCA.

7. Module de sauvegarde :

Chaque client doit être enregistrée dans une base de données en sauvegardant ces informations personnelles et son modèle, pour être par la suite récupérer et utiliser en phase de reconnaissances.

V.2.4. Phase de reconnaissances (Test et décision) :

Après l'étape d'apprentissage qui se termine par l'enregistrement des clients dans la base de données, le système est mis en fonction selon les deux modes : Identification ou authentification (vérification).

1. Identification :

Fonctionnement du système en phase d'identification.

Un système de reconnaissance des visages qui fonctionne en mode identification est un système qui permet de chercher l'identité d'une personne parmi plusieurs sauvegardées au préalable (clients) comme montre la figure suivante :

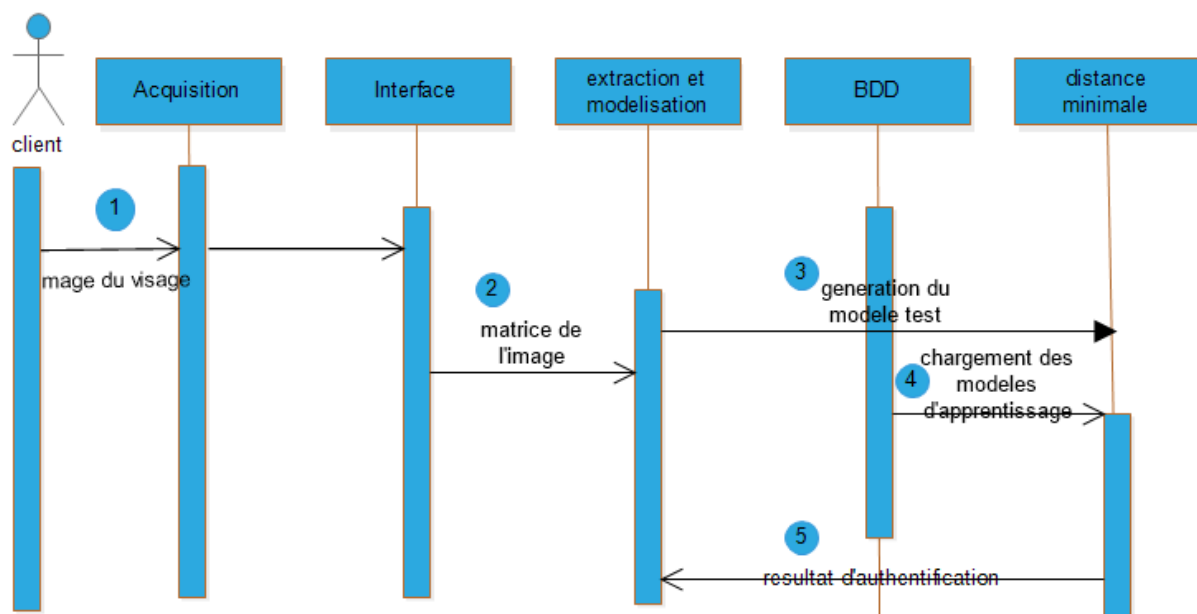


Figure V.13:Diagramme de séquence du cas Identification.

➤ Description du scénario d'identification :

- 1) Acquisition de l'image du visage de l'individu test.
- 2) Application des prétraitements nécessaires sur l'image acquise pour éliminer le bruit puis la transformer en une matrice de deux dimensions.

- 3) Extraction des paramètres pertinents de l'image test à l'aide de la DWT et la méthode PCA comme pour la phase d'apprentissage.
- 4) Calcul de la distance minimale de l'image test par rapport à tous les modèles des clients dans la base de données.
- 5) Le résultat de l'identification correspond au modèle ayant la plus petite distance avec l'image test.

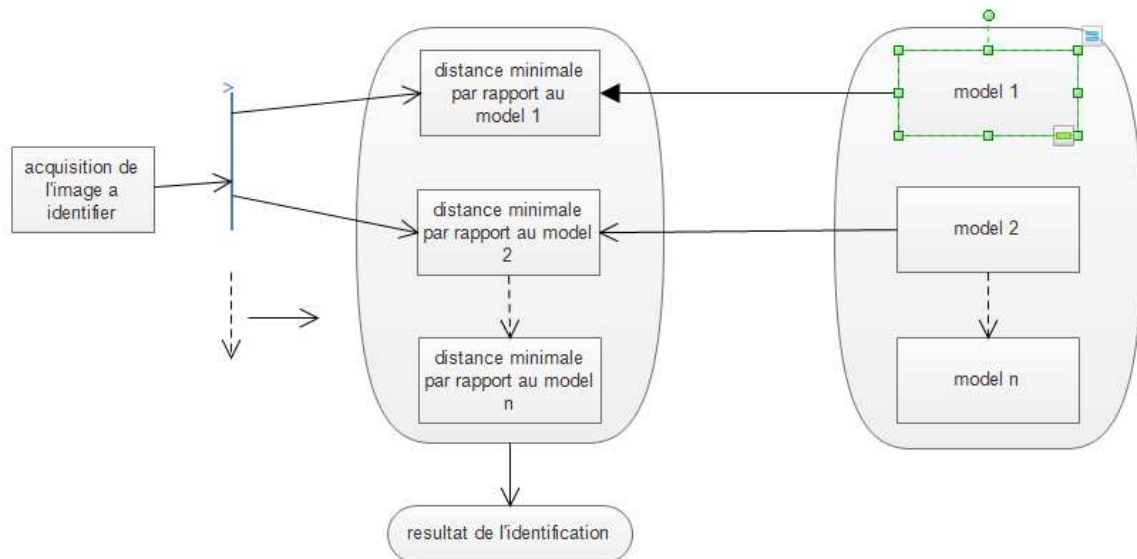


Figure V.14:Description du procédé d'identification.

2. Authentification :

Le principe de ce mode de reconnaissance est de vérifier si l'identité de la personne testée est la même que celle proclamée par cette dernière comme illustré dans la figure suivante :

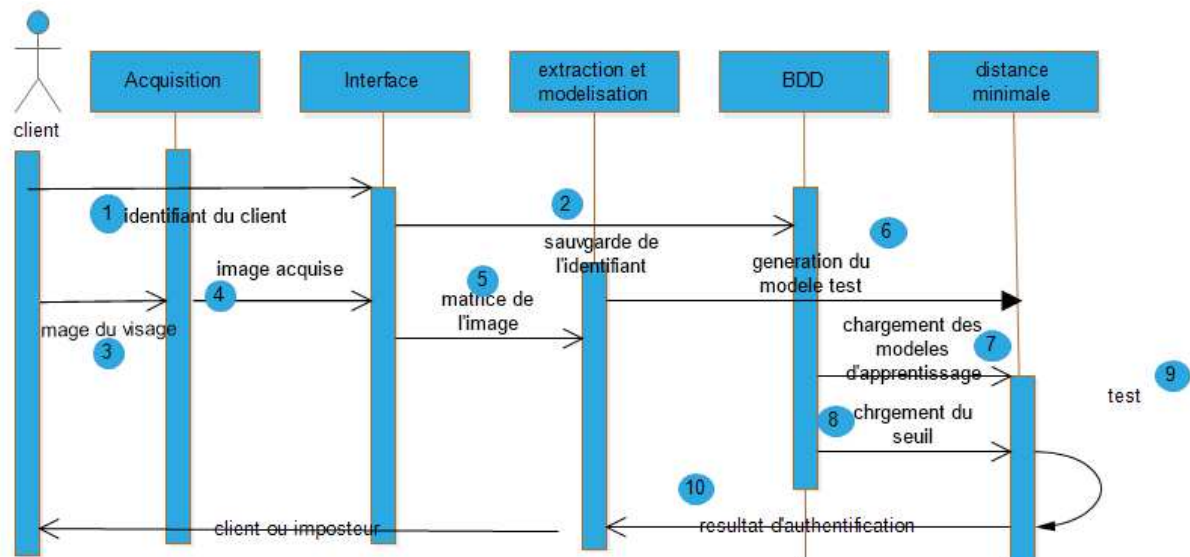


Figure V.15:Description du procédé d'authentification.

➤ **Description du scénario d'authentification :**

- 1) Le client introduit son identifiant.
- 2) La sauvegarde de l'identifiant dans la base de données.
- 3) Acquisition de l'image du visage du client.
- 4) Application des prétraitements sur l'image acquise, et sa transformation en matrice de deux dimensions.
- 5) Calcul du vecteur propre en appliquant la DWT et PCA à l'image obtenue après prétraitements.
- 6) Calcul de la distance minimale du vecteur propre par rapport au modèle proclamé.
- 7) Chargement du seuil.
- 8) Calculer le score_client et le score_imposteur:
 $\text{score_client} > \text{score_imposteur} \rightarrow \text{personne testée : client.}$
 $\text{score_client} \leq \text{score_imposteur} \rightarrow \text{personne testée : imposteur.}$

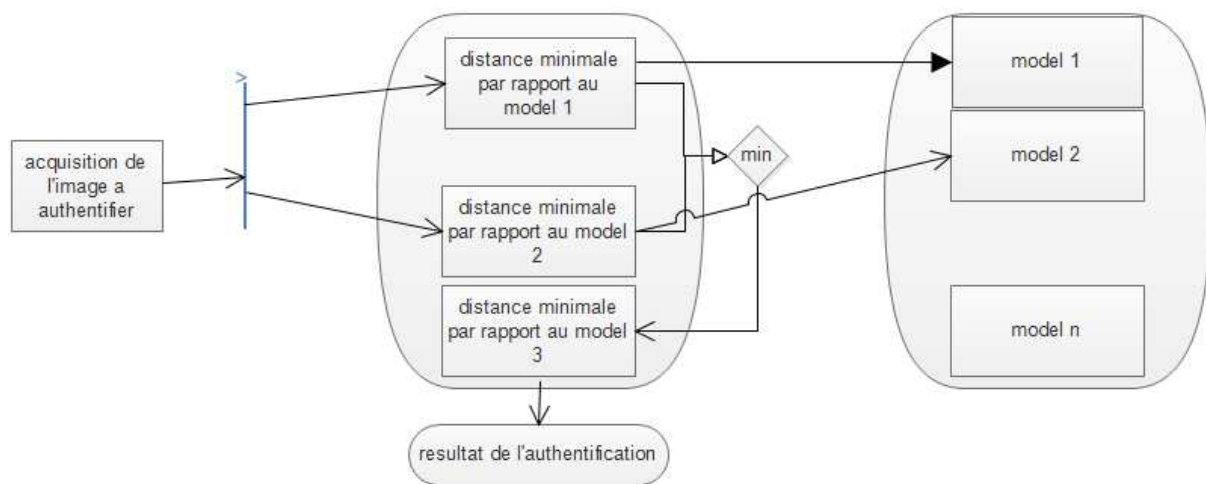


Figure IV.16 :Description du procédé d'authentification.

V.2.5. Calcul des performances du système :

L'objectif de cette opération est d'optimiser les performances du système en jugeant l'efficacité des méthodes sur lesquelles il se base. Cela se fait en estimant un ensemble d'indicateurs qui diffèrent selon le mode de reconnaissance :

1. Mode identification :

Mesurer les performances du système pour ce mode de reconnaissance consiste à calculer le taux d'identification (TID), qui représente la proportion du nombre de personnes identifiées sans erreurs. Le principe est le suivant : Pour toutes les personnes qui ont un modèle dans la base de données (client), l'administrateur effectue un test d'identification et compte le nombre de personnes bien identifiées. Puis, il divise ce dernier sur le nombre de personne testées et multiplie par 100.

$$\text{TID} = \frac{\text{nombre de tests ayant conduit à une identification correcte}}{\text{nombre totale de tests}} \times 100$$

Figure V.17 :Calcul du TID.

2. Mode authentification :

Mesurer les performances d'un système de reconnaissance des visages opérant en mode authentification se fait en trois étapes :

Le calcul de l'ensemble des scores clients et scores imposteurs et le seuil.

Seuil :

```
Seuil ← {}  
Seuil ← (max (distance_intra) + min (distance_extra)) / 2.
```

Figure V.18 :calcul du Seuil.

Scores clients:

```
Score_client ← {}  
Pour i=1 nb_presonne dans le système  
Min ← distance (proclamer (i,i))  
    Si Min ≤ Seuil  
        Score_client ← Score_client + 1  
Fin pour.
```

Figure V.19 :calcul du score client.

Scores imposteurs :

```
Score_imposteur ← {}  
Pour i=1 nb_presonne dans le système  
    Pour j=1, pas, nb_presonne dans le système (i <> j)  
        Min ← distance (proclamer (i,j))  
        Si Min > Seuil  
            Score_imposteur ← Score_imposteur + 1  
    Fin pour.  
Fin pour.
```

Figure V.20:calcul du score imposteur.

➤ Calcul des paramètres FRR, FAR :

Le FAR, FRR qui sont respectivement le taux de fausse acceptation, et le taux de faux rejets sont des paramètres utilisés pour mesurer les performances en mode authentification.

Le taux des fausses acceptations (FAR) est calculé à partir nombre de fausse acceptation sur le nombre de test extra classe multiplier par 100 qui représente le nombre de personnes qui ont proclamé des identités autre que les siennes, mais qu'ils ont été acceptés par le système (personne faussement acceptée). Le FAR est donné par l'algorithme suivant :

```
Fausse_acceptation ← {}  
Pour i=1 à nbr_Test_extra  
    si (dist_min_extra(i) ≤ Seuil)  
        Fausse_acceptation ← Fausse_acceptation + 1  
Fin pour  
FAR ← (Fausse_acceptation / nbr_Test_extra) * 100.
```

Figure V.21:calcul du FAR.

Le taux des faux rejets (FRR) est calculé à partir nombre de faux rejets sur le nombre de test intra classe multiplier par 100 qui représente le nombre de personnes qui ont été faussement rejeter, mais qu'ils doivent être accepter par le système (personne faussement rejeter). Le FRR est donné par l'algorithme suivant :

```
Faux_rejet ← {}  
Pour i=1 à nbr_Test_intra  
    si (dist_min_intra(i) > Seuil)  
        Faux_rejet ← Faux_rejet + 1  
Fin pour  
FAR ← (Faux_rejet / nbr_Test_intra) * 100.
```

Figure V.22:calcul du FRR.

3. Test de performances :

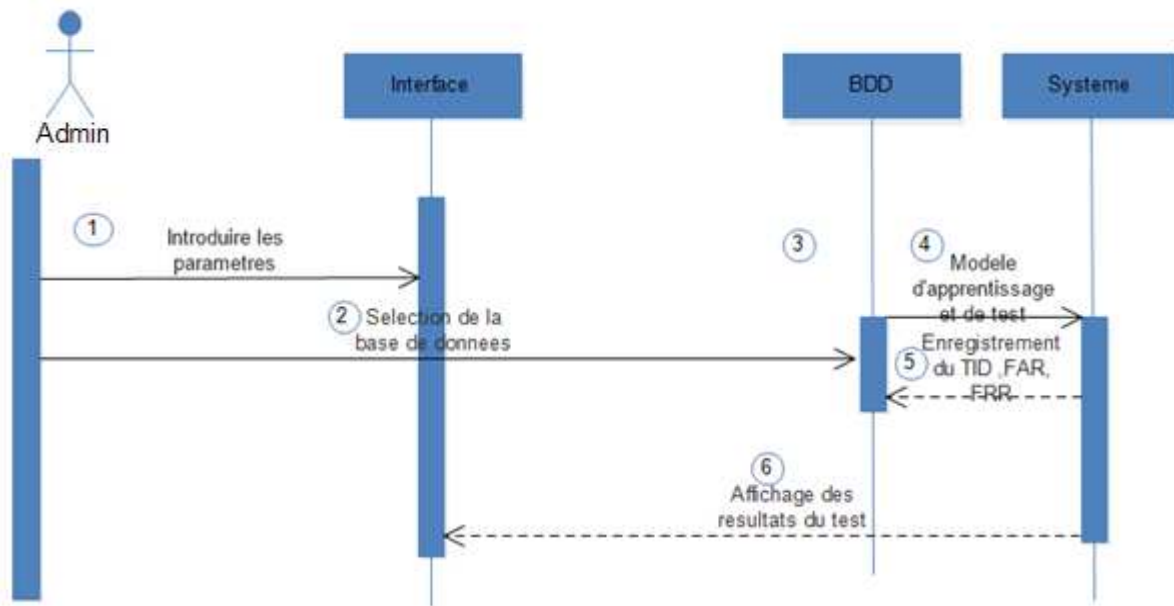


Figure V.23:Diagramme de séquence du cas test de performances.

- Description du scénario de calcul des performances :

- 1) L'utilisateur choisi la configuration.
- 2) La sélection de la base de données pour faire les tests.
- 3) La mesure des performances du système : le calcul du TID, FAR, FRR etSeuil pour la configuration choisie.
- 4) Chargement des modèles d'apprentissage et de teste déjà enregistrés.
- 5) Enregistrement du TID, FAR, FRR et Seuil.
- 6) Affichage des résultats.

V.2.6. Schéma conceptuel de la base de données :

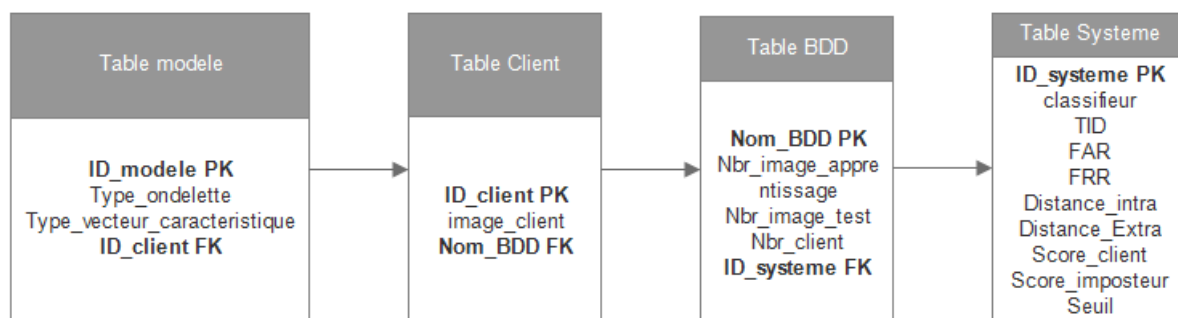


Figure V.24:Schéma conceptuel de la base de données.

V.3. Réalisation :

V.3.1. Introduction :

Après avoir présenté dans la partie précédente les différentes étapes de la conception de notre système, nous allons justifier nos choix techniques (outils utilisé et langages de programmation). Enfin nous allons présenter les différentes interfaces de notre application.

V.3.2. Outils de développement :

Le choix des outils de programmation se fait par plusieurs facteurs : La puissance, La disponibilité de plusieurs fonctionnalités, ...etc. Dans le cadre de notre projet, nous avons utilisé les outils suivants : Matlab 2015b.

1. Matlab :

MATLAB est une abréviation de Matrix LABoratory. Écrit à l'origine, en Fortran, par Cleve Moler à la fin des années 1970, optimisé pour le traitement des matrices, d'où son nom. MATLAB est un environnement puissant, complet en plus de sa disponibilité est assurée sur plusieurs plateformes : Sun, Bull, HP, IBM, compatibles PC (DOS, Unix ou Windows), Macintosh, iMac et Plusieurs machines parallèles.

Matlab est un environnement de calcul scientifique et de visualisation de données qui existe depuis plus de dix ans. Sa facilité d'apprentissage et d'utilisation (due à une syntaxe très claire) en ont fait un standard adapté pour les divers problèmes l'ingénierie. Parmi les raisons qui nous ont poussé à l'utiliser, on trouve :

- Ses très nombreuses fonctions prédéfinies et prêtes à l'emploi.
- Sa simplicité à l'implémentation et rapidité de calculs.
- Sa fiabilité et sa robustesse.

V.3.3. Structures de données et implémentation :

L'implémentation de notre système est composée de plusieurs bibliothèques de classes ; chacune contient plusieurs classes :

1. Acquisition :

Afin de capter des images d'individu à partir d'une webcam certaines méthodes sont nécessaires, Ci-dessous :

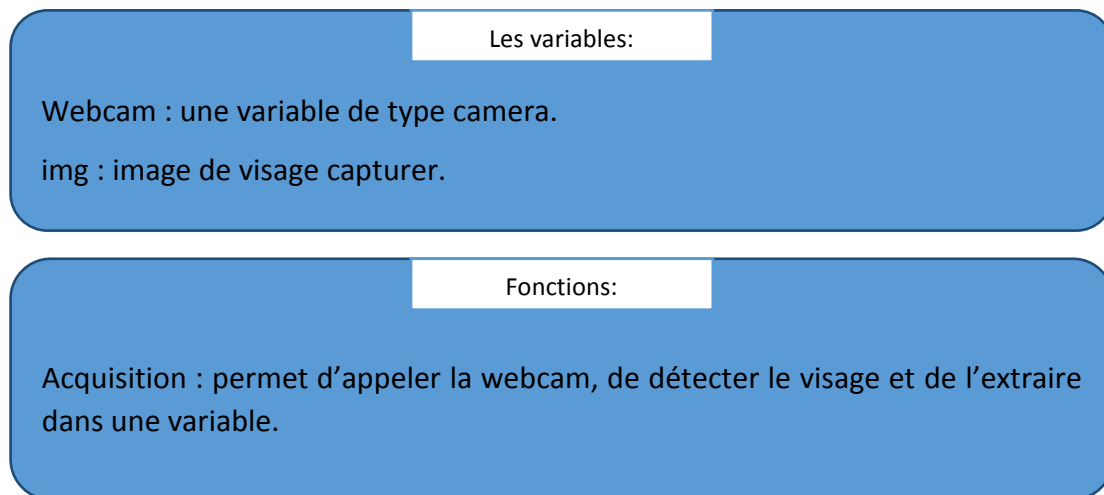


Figure V.25:variables et fonction de la partie acquisition.

2. Extraction de paramètre :

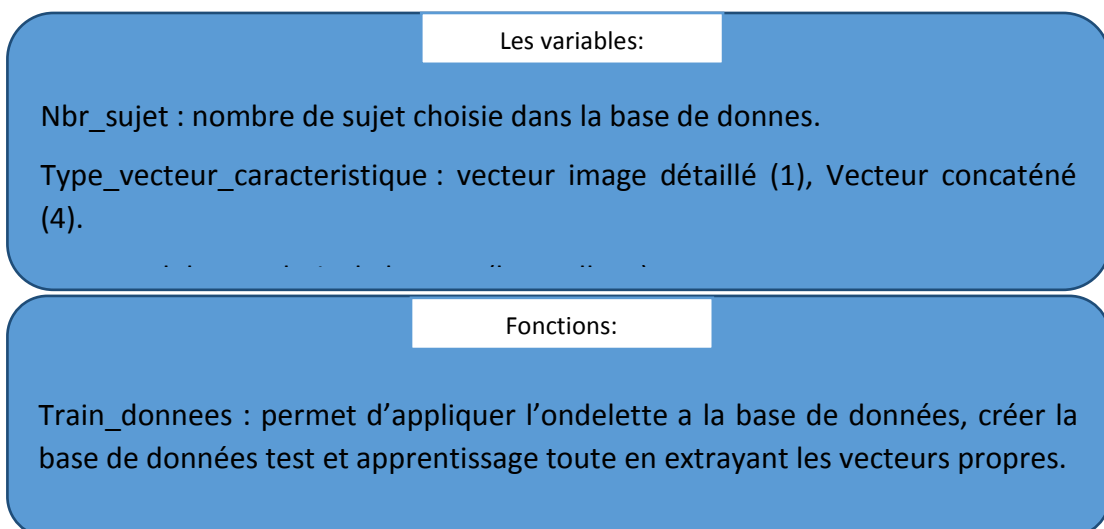
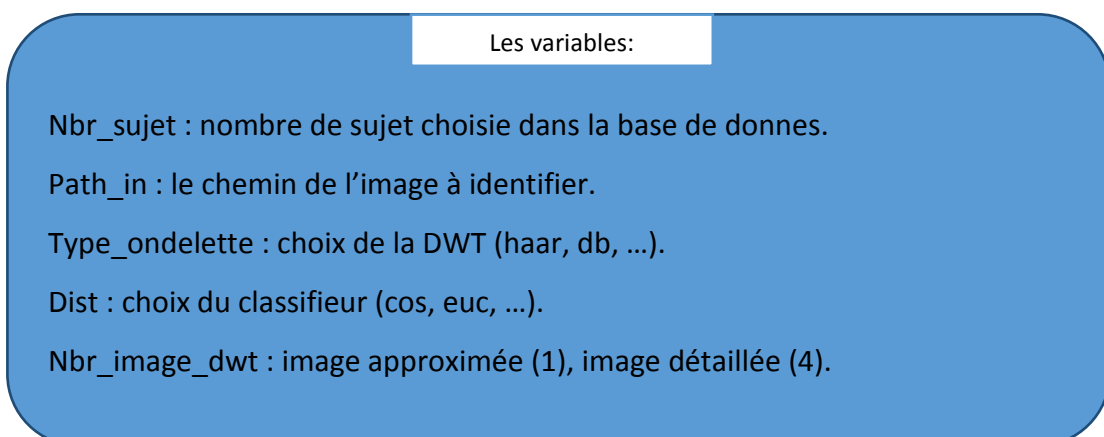


Figure V.26 :variables et fonction de la partie apprentissage.

3. Identification :



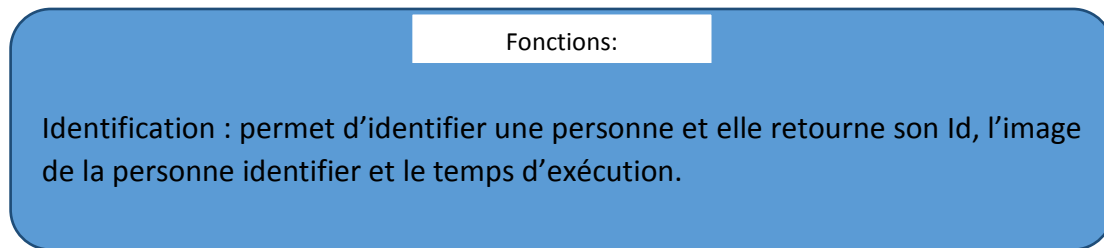


Figure V.27:variables et fonction de la partie identification.

4. Authentification :

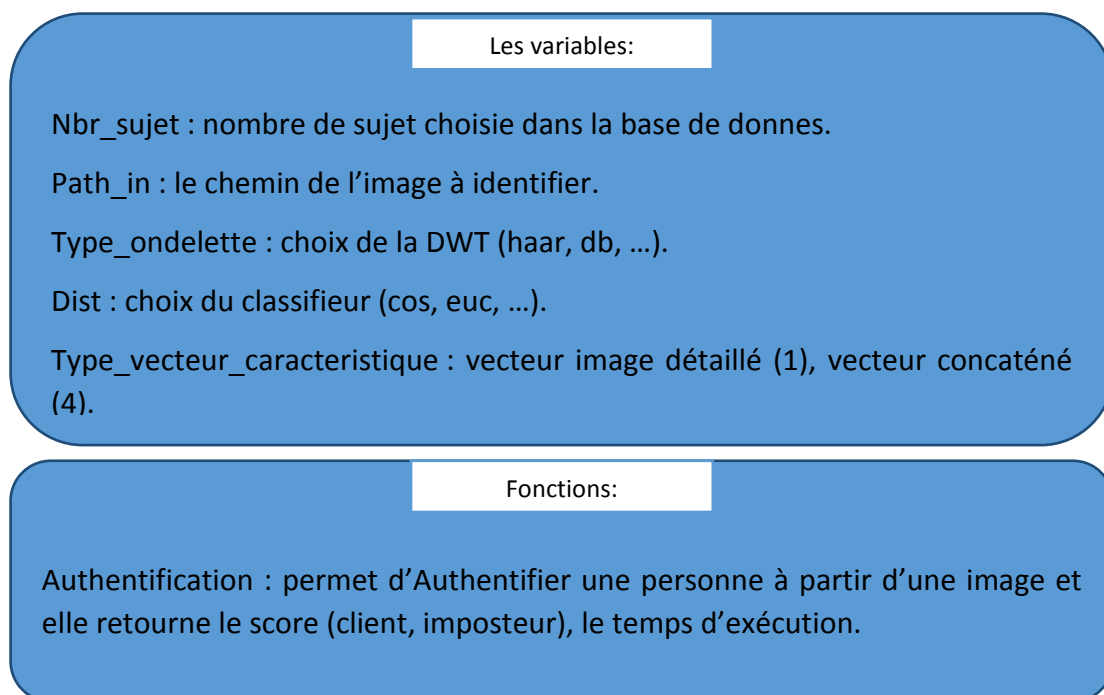


Figure V.28:variables et fonction de la partie authentification.

V.3.4. Présentation de l'application :

Dans cette partie, on présentera notre application, ainsi que ses différentes fonctionnalités et leur correspondance avec les modules illustrés dans les sections précédentes. Comme tout logiciel de reconnaissance de visages, le nôtre est composé des principaux modules suivants :

1. Interface apprentissage :

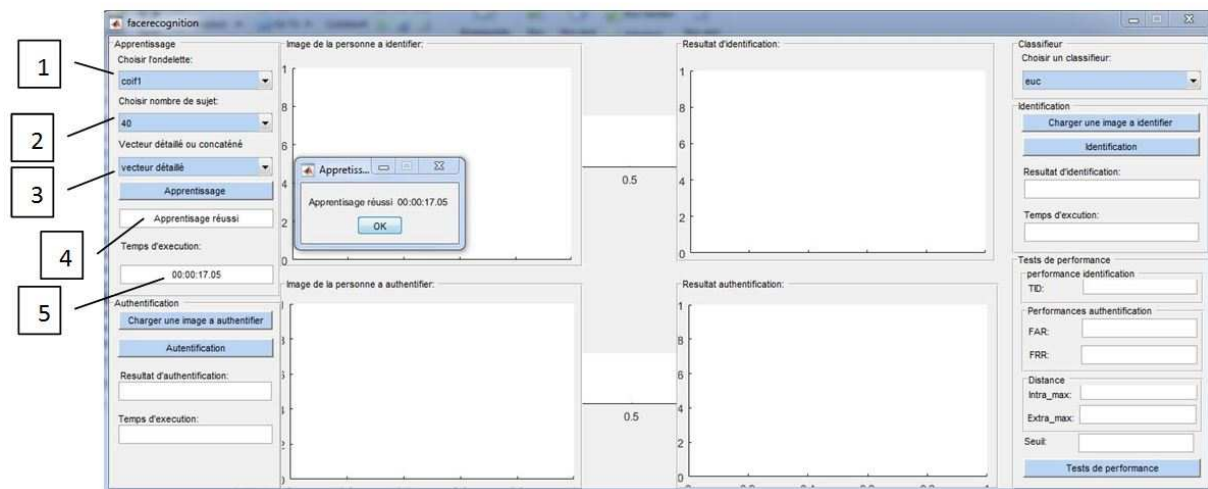


Figure V.29 : interface apprentissage.

1. Choix du type d'ondelette à appliquer (haar, db1, coif1, sym1, dym).
2. Choix nombre du sujet dans la base de données (1 à 40).
3. Choix du type du vecteur caractéristique (vecteur image détaillée, vecteur concaténé).
4. Résultat d'apprentissage.
5. Temps d'exécution de la phase apprentissage.

2. Tests de performance :

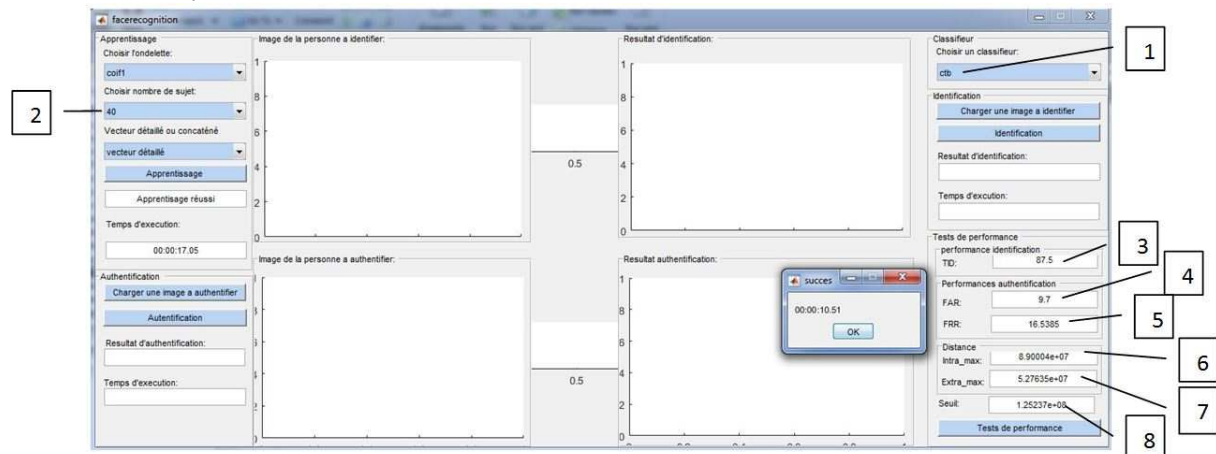


Figure V.30 : interface tests de performance.

1. Choix du classifieur.
2. Choix du nombre du sujet dans la base de données.
3. Taux d'identification (TID).
4. Taux de fausse acceptation (FAR).
5. Taux de faux rejet (FRR).
6. Distance intra classe (intra_max).
7. Distance extra classe (extra_max).
8. Seuil.

3. Interface identification :

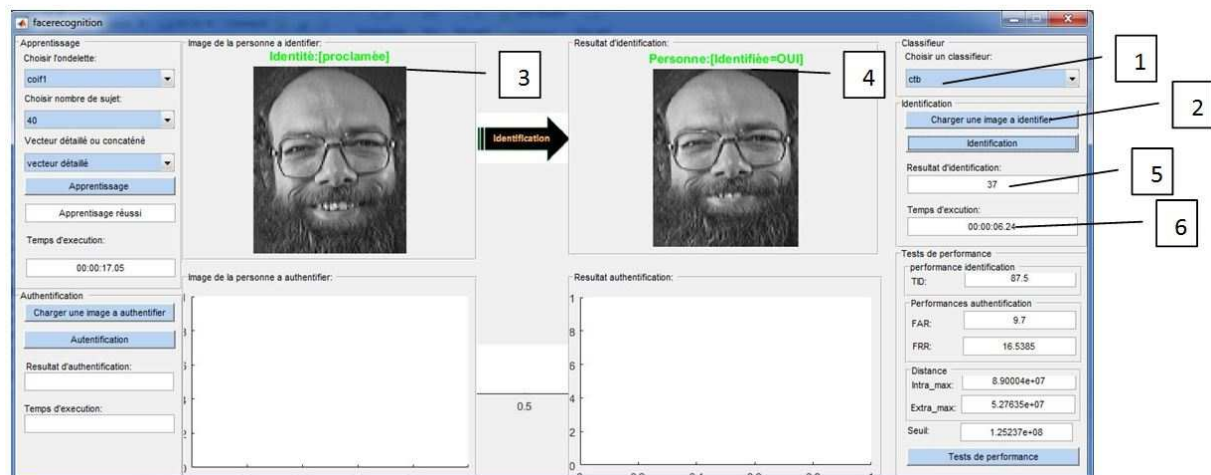


Figure V.31 : interface identification.

1. Choix du classifieur.
2. Chargement de l'image de la personne à identifier.
3. Image de la personne à identifier.
4. Image de la personne identifier
5. Résultat d'identification (identifiant client).
6. Temps d'exécution de la phase identification.

4. Interface authentification :



Figure V.32 : interface authentification.

1. Choix du classifieur.
2. Chargement de l'image de la personne à authentifier.
3. Image de la personne à authentifier.
4. Résultat d'authentification (client ou imposteur).
5. Temps d'exécution de la phase identification.

V.3.5. Conclusion :

Dans ce chapitre, nous avons illustré le schéma général de notre système de reconnaissance de visages et les détails des modules qui le composent, ainsi que les différents langages et outils utilisés pour assurer son bon fonctionnement.

Chapitre VI :

TESTS ET EVALUATION DES RESULTATS

VI.1. Introduction:

Dans ce chapitre, on exposera les résultats et tests effectués utilisant l'approche de classification dite : par mesure de similarité, ou nous avons utilisé quatre distances pour la classification à savoir (distance euclidienne, "Mahalcos", "Cosine" et la norme "Ctb"). Les tests effectués concernent les deux modes de reconnaissance à savoir l'identification et la vérification. Dans un premier temps, on exposera les tests effectués selon chaque mode, et pour chaque méthode de classification utilisée on va étudier l'influence du choix d'ondelette et le type de vecteur caractéristique (soit un vecteur image détaillée ou la concaténation des quatre vecteurs caractéristiques) utilisé dans l'étape extractions de paramètres, sur la performance du système. Ensuite, on fera une étude comparative de ces quatre approches de classification et on terminera par une conclusion des tests réalisés.

VI.2. La Base de données ORL :

Les données utilisées pour réaliser les tests sur notre système proviennent de la base **ORL**. Cette base de données est une référence pour les différents systèmes de reconnaissance automatique de visage dans le monde. Cela est dû au nombre important de contraintes qu'elle impose, et les différentes variations du visage qu'elle prend en compte, comme par exemple : la coiffure, la barbe, les lunettes, les changements d'expressions faciales, ...etc.

La base ORL (Olivetti Research Laboratory) a été conçue par AT&T laboratoires de l'université de Cambridge en Angleterre. Elle est constituée de 400 images (en niveau de gris de taille 92*112 pixels chacune) de l'ensemble de 40 individus, tel que chacun possède 10 poses 5 pour l'apprentissage et 5 pour le test.

- **Images apprentissages** : Les cinq premières images servent pour la phase d'apprentissage, ce qui nous fait un sous ensemble de 200 images dédiées à cette phase.
- **Images Tests**: Les cinq dernières images de chaque individu nous ont servies pour la réalisation des différents tests, ce qui nous fait un sous ensemble de 200 images dédiées à la phase test dans ses deux modes.

Les tests ont été réalisés sur un ordinateur personnel PC DELL i5-4200U CPU @ 1.6 GHz 2.3 GHz et une RAM de 6,00 G.



Figure VI.1 : Exemple de visages de la base ORL.

VI.3. Protocole d'évaluation:

Le système a été soumis à une série de tests en ses deux modes (identification et vérification) avec différents paramètres de configuration suivant les deux approches respectivement d'extraction de paramètres DWT et de modélisation par méthode ACP et ceci avec les quatre distances classification à savoir : (par distance euclidienne, mahalcov, cosinus et la norme l_1) dans le but de faire une étude comparative des différentes configurations et les performances qui en résultent. Ces tests ont été réalisés suivant le protocole suivant:

- **Générations des Modèles DWT:** On a utilisé comme indiqué précédemment les 5 premières images de chaque personne pour générer leurs modèles suivant l'algorithme DWT (avec le choix d'ondelette à appliquer et le type de vecteur caractéristique) défini dans le chapitre III, il en résulte au final 200 modèles représentatifs de ces personnes.
- **Réduction d'espace des modèles DWT par la méthode ACP:** on prend tous les Modèles DWT on les projette dans l'espace ACP pour réduire leurs tailles et ainsi, extraire les vecteurs visages (Eigen faces) pour chaque personne, qui seront ensuite des modèles à enregistrer dans la base de données pour la reconnaissance.
- **Configuration des paramètres du système:**

1. Paramètres fixes:

Le level (le niveau de décomposition) pour la DWT : un level (niveau)

Taille des "Eigen faces" : 199 comparantes caractéristique.

Nombre d'image d'apprentissage : 5 images pour chaque personne

2. Paramètres variables :

Ondelette à utiliser pour la DWT: "Haar", "sym", "db", "dmey", "coief".

Type de vecteur caractéristique : vecteur image détaillée, vecteur concaténé

Méthodes de classification : euclidienne, mahcos, cosine, la norme ctb.

Seuil de décision : variable pour chaque configuration.

Suivant différentes combinaisons des configurations de paramètres décrits plus haut, les résultats de ces tests sont détaillées comme suit:

VI.4. Résultats des Tests:

Dans ce qui suit, on exposera les différents tests effectués sur la base de données ORL.

Dans les deux modes identification et authentification (vérification).

VI.4.1. Mode identification (vecteurs caractéristiques concaténés) :

Effet du choix d'ondelette et la méthode de classification sur le TID:

	Euclidienne	Mahcos	Cosine	Ctb
Haar	52.00	53.00	53.00	73.5
Daubechies	52.00	53.00	53.00	73.5
Symlets	52.00	53.00	53.00	73.5
Coiflets	41.50	44.50	44.50	68.00
Demystified	63.50	56.50	56.50	78.50

Tableau VI.1 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance (Vecteur concaténé).

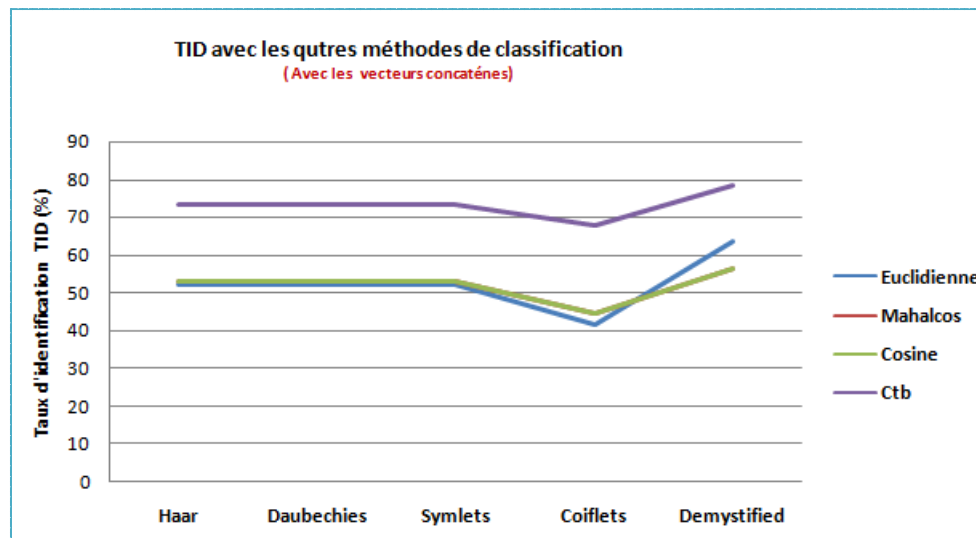


Figure VI.2 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance (Vecteur concaténé).

A travers ces courbes, on s'aperçoit que l'on atteint les meilleures performances en terme de taux d'identification (TID) avec la méthode de classification par mesure de similarité utilisant la distance de la norme Ctb par rapport aux autres méthodes, et cela quel que soit l'ondelette utilisée notamment l'ondelette orthogonale de "demystified" ou on a trouvé le TID le plus élevé (78.5%). Il est aussi à noter que avec les deux méthodes Cosine et Mahalcos on a trouvé les mêmes performances ce qui est expliqué par la superposition de la courbe Cosine sur celle de Mahalcos. En termes d'ondelette on a constaté que l'ondelette de "Haar", "Daubechies" et "Symlets" donnent les mêmes résultats (peu satisfaisant), une légère baisse des performances pour "Coiflets" et un excellent résultat pour l'ondelette de "Demystified" ceci peut être dû à sa grande capacité d'élimination de bruit dans l'étape d'extraction de paramètres.

VI.4.2. Mode authentification (vérification):

- Effet du choix d'ondelette et la méthode de classification sur le FAR:

	Euclidienne	Mahalcos	Cosine	Ctb
Haar	29.358	35.769	35.769	38.589
Daubechies	29.358	35.769	35.769	38.589
Symlets	29.358	35.769	35.769	38.589
Coiflets	47.564	38.461	38.461	36.794
Demystified	28.846	31.794	31.794	27.692

Tableau VI.2 : Variation du taux fausse acceptation FAR (%) en fonction de type d'ondelette et la distance (Vecteur concaténé).

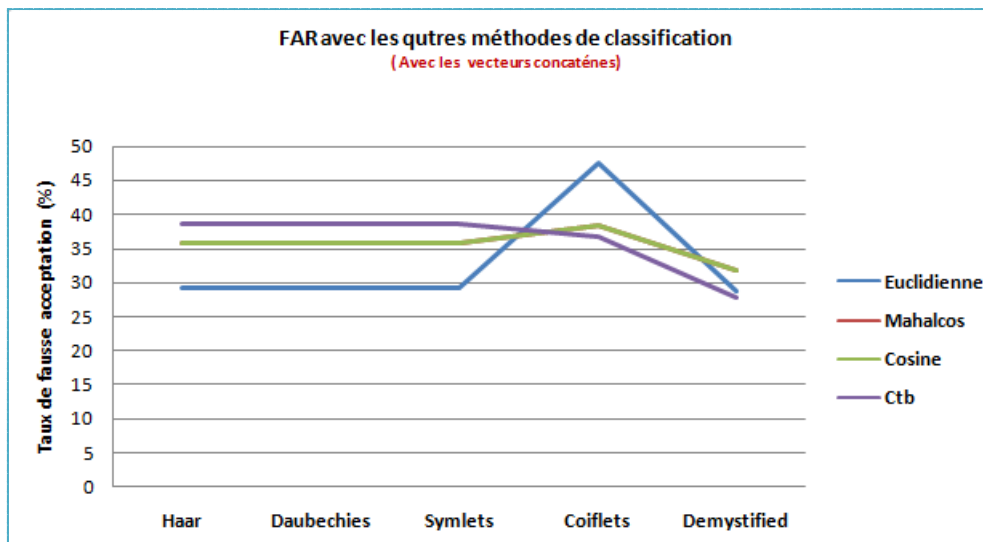


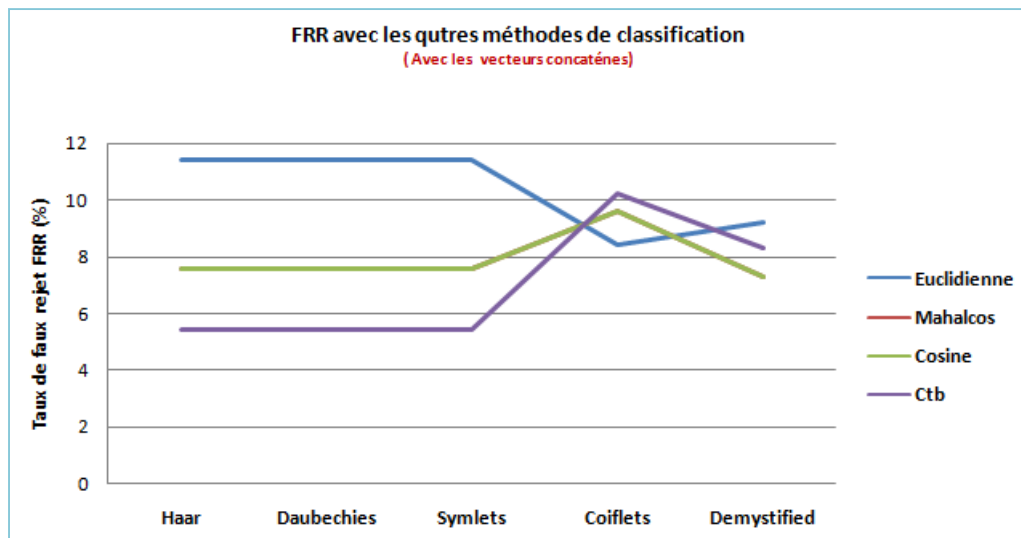
Figure VI.3 : Variation du taux de fausse acceptation FAR (%) en fonction de type d'ondelette et la distance (Vecteur concaténé).

A travers les résultats des tests voir (tableau VI.2) et la figure ci-dessus on remarque qu'on atteint le Taux de fausse acceptation (FAR) le plus bas avec la méthode de classification par la distance de la norme Ctb avec l'ondelette de "Demystified", d'où elle confirme aussi ses performances en mode authentification, il est important à savoir que, dans un système biométrique de reconnaissance plus le FAR est proche de zéro plus les performances sont bonnes et vice versa.

- Effet du choix d'ondelette et la méthode de classification sur le FRR:

	Euclidienne	Mahalcos	Cosine	Ctb
Haar	11.40	7.60	7.60	5.40
Daubechies	11.40	7.60	7.60	5.40
Symlets	11.40	7.60	7.60	5.40
Coiflets	8.40	9.60	9.60	10.20
Demystified	9.20	7.30	7.30	8.30

Tableau VI.3 : Variation du taux de faux rejet FRR (%) en fonction de type d'ondelette et la distance (Vecteur concaténé).



FigureVI.4 : Variation du taux de faux rejet FAR (%) en fonction de type d'ondelette et la distance (Vecteur concaténé).

A travers les résultats des tests voir (tableau VI.3) et la figure ci-dessus on remarque qu'on atteint le Taux de faux rejet (FRR) le plus bas avec la méthode de classification par la distance de la norme Ctb mais , cette fois ci avec les trois ondelettes respectivement "Haar" ,"Daubechies" et "Symelts" , et mêmes si "Demystified" donne de moins bonnes performances en terme de FRR par rapport aux ondelettes "Haar", "Daubechies" et "Symelts" il vaut mieux la choisir parce que avec cette ondelette on a obtenu de meilleure performances en FAR, cependant dans un système biométrique de reconnaissance , on préfère souvent un FAR plus bas qu'un FRR , en d'autre terme il vaut mieux rejeter un client qu'accepter un imposteur .

Il est important à savoir que dans un système biométrique de reconnaissance plus le FRR est proche de zéro plus les performances sont bonnes et vice versa.

VI.4.3. Mode identification (vecteur image détaillé) :

- Effet du choix d'ondelette et la méthode de classification sur le TID:

	Euclidienne	Mahalcos	Cosine	Ctb
Haar	78.00	78.00	78.00	82.50
Daubechies	78.00	78.00	78.00	82.50
Symlets	78.00	78.00	78.00	82.50
Coiflets	81.50	81.50	81.50	87.50
Demystified	77.50	79.50	79.50	85.50

Tableau VI.4 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance (Vecteur image détaillé).

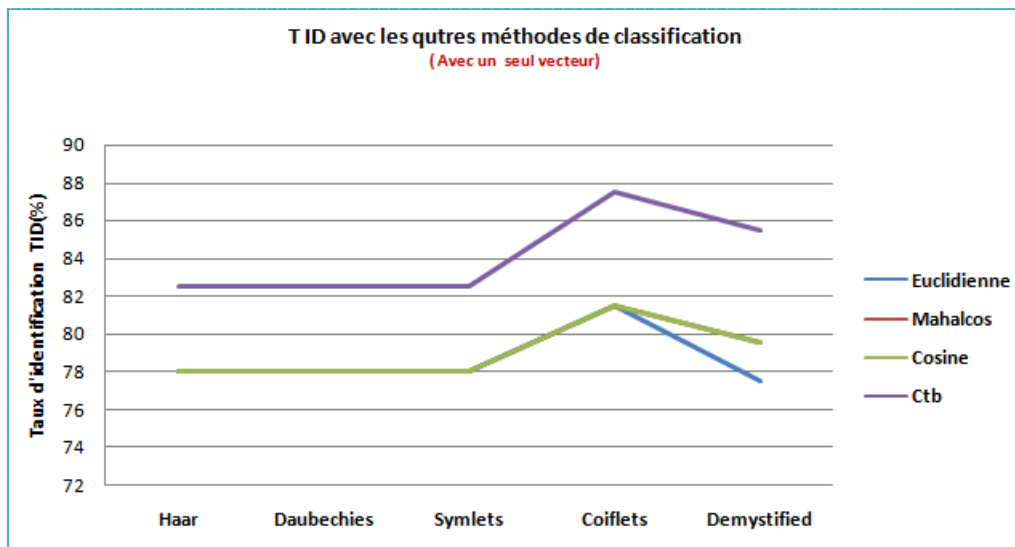


Figure VI.5 : Variation du taux d'identification TID (%) en fonction de type d'ondelette et la distance (Vecteur image détaillé).

On constate à travers ces courbes l'effet très positif engendré par l'utilisation d'un seul vecteur caractéristique (vecteur détaillé), où on atteint de très bonnes performances avec un TID égale à 87.5%, représentant le meilleur taux atteint des tests. Également ce taux a été obtenu avec la distance de la norme Ctb, mais cette fois ci avec l'ondelette de "Coiflets" et non plus avec l'ondelette de "Demystified", comme on a vu avec l'utilisation de vecteur caractéristique (vecteur concaténé) "Coiflets" elle a été au cinquième rang en terme de performances en mode identification bien que, avec l'utilisation de vecteur détaillé on a constaté une augmentation positive voire d'un TID de 41.5% à 81.5% avec "Coiflets" et la distance euclidienne. Pour les quatre distances de classification, aussi on remarque des augmentations très significative de performances par rapport à celles obtenus avec le vecteur concaténé, (voir tableau VI.1 et tableau VI.4).

VI.4.4. Mode authentification (vérification):

• Effet du choix d'ondelette et la méthode de classification sur le FAR:

	Euclidienne	Mahalcos	Cosine	Ctb
Haar	24.743	36.538	36.538	10.897
Daubechies	24.743	36.538	36.538	10.897
Symlets	24.743	36.538	36.538	10.897
Coiflets	21.666	33.846	33.846	16.538
Demystified	26.794	38.205	38.205	20.384

Tableau VI.5 : Variation du taux de fausse acceptation FAR (%) en fonction de type d'ondelette et la distance (Vecteur image détaillé).

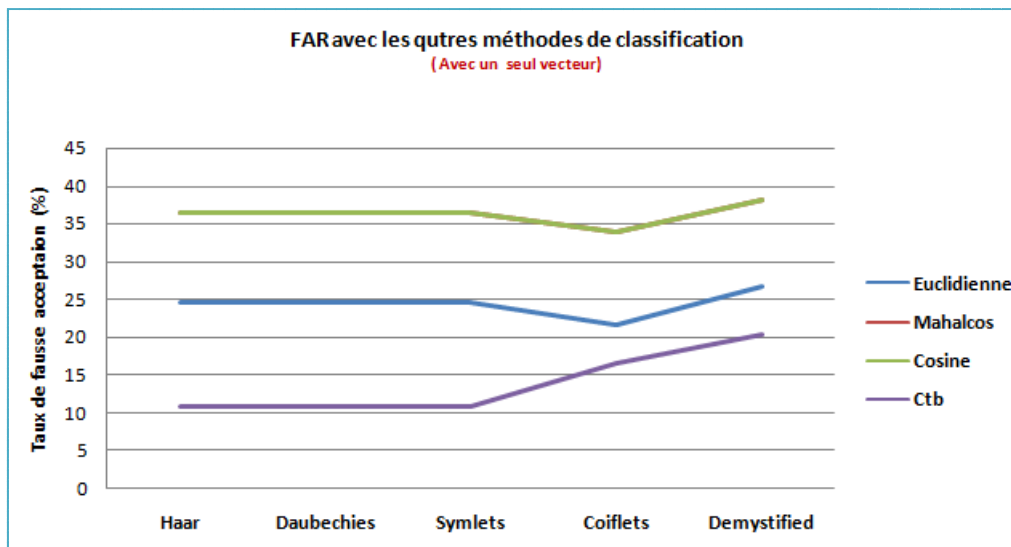


Figure VI.6 : Variation du taux de fausse acceptation FAR (%) en fonction de type d'ondelette et la distance (Vecteur image détaillé).

A travers les résultats des tests voir (tableau VI.4) et la figure ci-dessus on remarque qu'on atteint le Taux de fausse acceptation (FAR) le plus bas avec la méthode de classification par la distance de la norme Ctb avec les trois ondelettes respectivement "Haar", "Daubechies" et "Symlets", d'où il est préférable de les utilisées en mode authentification, il est à savoir que dans un système biométrique de reconnaissance plus le FAR est proche de zéro plus les performances est bonnes et vice versa.

- **Effet du choix d'ondelette et la méthode de classification sur le FRR:**

	Euclidienne	Mahalcos	Cosine	Ctb
Haar	7.70	5.10	5.10	13.80
Daubechies	7.70	5.10	5.10	13.80
Symlets	7.70	5.10	5.10	13.80
Coiflets	7.70	4.40	4.40	9.70
Demystified	6.10	3.80	3.80	7.50

Tableau VI.6: Variation du taux de faux rejet FRR (%) en fonction de type d'ondelette et la distance (Vecteur image détaillé).

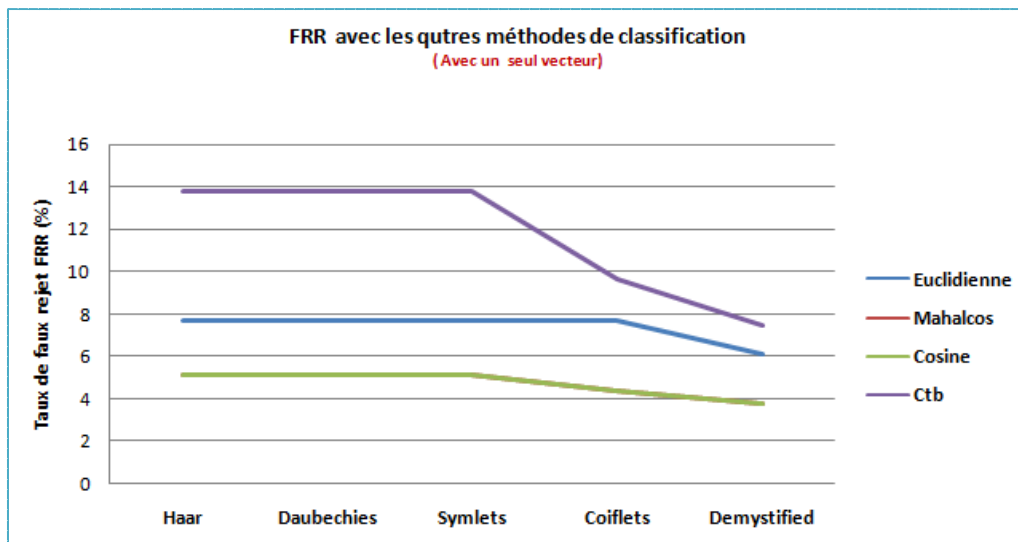


Figure VI.7 : Variation du taux de faux rejet FRR (%) en fonction de type d'ondelette et la distance (Vecteur image détaillé).

A travers les résultats des tests voir (tableau VI.6) et la figure ci-dessus on remarque qu'on atteint le Taux de faux rejet (FRR) le plus bas de ces tests avec la méthode de classification par les distances "Cosine" et "mahalcos" avec l'ondelette de "Demystified", même si cette fois ci la distance de la norme Ctb n'a pas donner les meilleures performances en faux rejet, elle reste quand même, la meilleure en mode authentification, vue les performance obtenus en fausse acceptation (FAR). Cependant dans un système biométrique de reconnaissance, on préfère un FAR plus bas qu'un FRR, en d'autres termes il vaut mieux rejeter un client qu'accepter un imposteur.

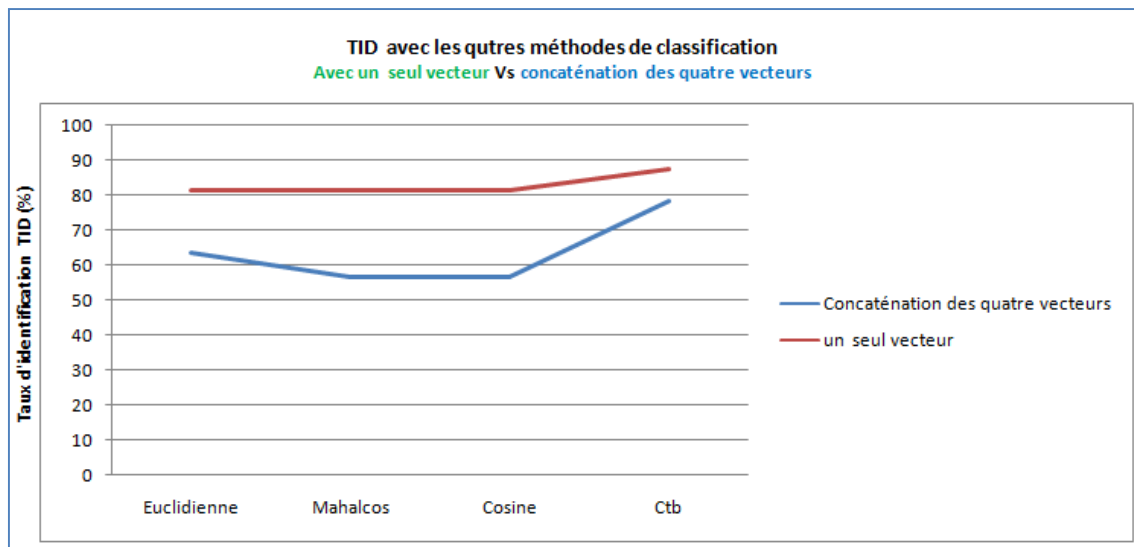
Il est à savoir que dans un système biométrique de reconnaissance plus le FRR est proche de zéro plus les performances sont bonnes et vice versa.

VI.5. Comparaison entre l'utilisation de vecteur image détaillé et le vecteur concaténé:

Dans le but de comparer les deux cas nous avons dressé des tableaux récapitulatifs des meilleurs taux de chaque cas, ceci est donné par le tableau ci-après:

	Euclidienne	Mahalcos	Cosine	Ctb
Un seul vecteur	63.50	56.50	56.50	78.50
Concaténation des quatre vecteurs	81.50	81.50	81.50	87.50

Tableau VI.7 : vecteur image détaillé Vs vecteur concaténé TID(%)



FigureVI.8 : vecteur image détaillé Vs vecteur concaténé TID(%)

Ces courbes nous montrent que les performances avec l'utilisation de vecteur concaténé sont meilleures que celles d'utilisation de vecteur concaténé et l'écart de performances augmente en faveur des distances "Cosine" et "mahalcos".

VI.6. Comparaison entre les quatre distances de classification :

Dans le but de comparer les quatre distances de classification nous avons dressé un tableau récapitulatif des meilleurs taux d'identification dans les deux cas c.-à-d. (vecteur image détaillé ou vecteur concaténé) et cela pour chaque distance, ceci est donné par le tableau suivant:

Euclidienne	Mahalcos	Cosine	Ctb
63.50	56.50	56.50	78.50
81.50	81.50	81.50	87.50

Tableau VI.8 : comparaison des quatre distances de classification en TID (%).

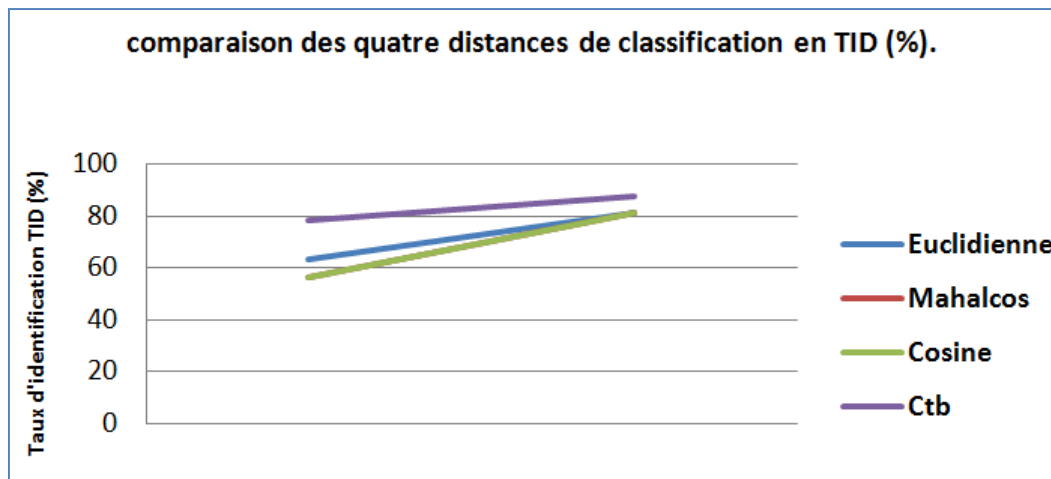


Figure VI.9 : comparaison des quatre distances de classification en TID (%).

A travers ces courbes on remarque bien, que la distance de la norme Ctb donne de meilleures performances en mode identification avec un TID très satisfaisant de 87.5 %, en deuxième rang les trois autres distances Euclidienne, Cosine et Mahalcos avec un TID de 81.5%.

VI.7. Temps d'exécution:

L'approche de classification par mesure de similarité utilisant la distance de la norme Ctb est particulièrement robuste et on a vu à travers les différents tests effectués qu'elle donne d'excellents résultats que ce soit en mode identification ou vérification. Cependant il reste confirmé en terme du temps d'exécution et le comparant ainsi aux temps obtenus avec les trois autres distances à savoir, Cosine, Mahalcos et Euclide.

Entre autres ce temps-là augmente en augmentant le nombre de personnes dans la base. Voici donc à titre indicatif quelques mesures de temps d'exécutions pour les quatre distances de classification en mode identification et authentification avec l'utilisation de l'ondelette de "Coifelets " et le vecteur détaillé qui ont donné des bons résultats.

Euclidienne	Cosine	Mahalcos	Ctb
4.18 s	4.70 s	6.38 s	3.68 s

Tableau VI.9 : temps d'exécutions en mode identification et authentification en (seconds).

Les temps d'exécution des quatre distances ne dépassent pas sept seconds en identification plus authentification.

VI.8. CONCLUSION :

A travers ces tests effectués dans les deux modes (Identification et vérification), on peut résumer l'effet du choix d'ondelettes à appliquer, la distance de classification et le type de vecteur caractéristique, comme suit:

En utilisant le vecteur détaillé, les performances augmentent d'une manière significative et ceci quel que soit l'ondelette à appliquer et la distance de classification à utiliser ceci peut être due à l'utilisation seulement de l'information pertinente c.-à-d. en se focalisant juste sur les détails de l'image issu de l'application de la DWT.

En utilisant le vecteur concaténé le système n'a pas atteint des très bonnes performances dans les deux modes identification et authentification, ceci due peut-être à l'utilisation de composantes caractéristique en plus (détail vertical, détail horizontal et détail diagonal), c'est-à-dire de l'information inutile qui joue le rôle de parasite ou bien de bruit dans la classification.

En terme, d'ondelette " Demystified" est la mieux adapté dans le cas du vecteur image détaillé, elle nous donne de bonnes performances en identification et authentification, l'ondelette de " Coiflets" est la mieux adapté dans le cas de la concaténation, avec une faveur pour cette dernière car, avec l'application de celle-ci on a atteint les meilleures performances des tests réalisés, quant aux trois autres ondelettes, " Haar", " Daubechies" et "symlets", les performances sont peu satisfaisantes, et elles sont égales durant tous les tests réalisés.

Enfin, pour les distances de classification la distance de la norme Ctb est meilleure pour la classification, avec elle on a atteint les meilleures performances en identification et en authentification, voire un TID de 87.5% qui est un résultat très satisfaisant en prenant en compte les limites de la classification par mesure de similarité.

Conclusion et Perspectives :

Ce travail s'inscrit dans le domaine de la reconnaissance automatique des visages. Celui-ci consiste à vérifier l'identité d'une personne à partir de son image. Utilisés principalement pour des raisons de sécurité et/ou confidentialité, les systèmes de reconnaissance automatique des visages sont souvent développés dans les applications de télésurveillance et l'accès à des endroits sécurisés. On peut également l'associer à d'autres modalités (ex : vérification de signatures, la voix, des empreintes digitales et de la forme de la main) dans des systèmes de vérification et d'authentification multimodale de l'identité. Du point de vue applicatif, les systèmes de reconnaissance de visages ont atteint une maturité permettant une intégration dans les applications commerciales. Aussi, l'amélioration des performances permet d'envisager le déploiement d'applications visant à réduire de façon significative la fraude dans différents contextes où la sécurité est impérative. Notre projet de fin d'étude s'inscrit dans ce contexte.

En effet, nous avons conçu et réalisé un système de reconnaissance de visages dans ses deux modes (identification et vérification) basé sur l'approche DWT-PCA pour l'extraction et la modélisation de paramètres, la méthode de classification dite par mesure de similarité associée à quatre distances (Euclidienne, "Mahalanobis", "Cosine" et la "norme C_tb"), dont nous avons constaté la puissance, la robustesse et la simplicité.

Dans chaque système de reconnaissance, le critère de mesure permettant le choix de telle ou telle approche concerne les performances incarnées par le taux d'identification correcte en mode identification et le taux de fausse acceptation (FAR) et le taux de faux rejet (FRR) en mode vérification. A cet effet, les tests effectués sur la base de données ORL nous ont permis de constater que la modélisation par l'approche DWT-PCA donne de bons résultats que ce soit par utilisation de la méthode de classification par mesure de similarité associée aux quatre distances notamment celle de la norme C_tb.

Cependant, l'approche DWT-PCA permet de palier aux problèmes de dimensionnement dans le sens que si la dimension des données est élevée, elle permet de réduire leur dimension d'une manière considérable, aussi pour les problèmes d'éclairement, de pose et d'expression faciale.

Ainsi, et comme perspective d'améliorations, l'utilisation de méthodes basées sur la modélisation probabiliste de mélange de gaussiennes GMM. En effet, les GMM dont la pertinence a été prouvée, constituent même l'état de l'art actuel des systèmes de reconnaissance du locuteur présente l'avantage de modéliser avec habileté une large gamme de distributions complexes dont la densité de probabilité n'étant pas connue d'avance.

Aussi, étant donné que notre système est totalement opérationnel, nous pouvons envisager une association avec une autre modalité, en l'occurrence la voix afin d'avoir un système bimodal plus complet et répondant aux exigences actuelles dans le domaine de la sécurité.

De plus, les activités de recherche dans le domaine sont en perpétuelle évolution. Ces dernières portent sur la consolidation des approches existantes, l'amélioration des

techniques de modélisation et d'estimation statistiques ainsi que le renforcement de l'efficacité des stratégies de décision.

Références bibliographiques :

- [2] A. Jain, L. Hong, S. Pankanti, « Biometrics: Promising Frontiers for Emerging Identification Market », Communications of the ACM, Feb 2000, p. 91-98.
- [3] C. Fredouille, J. Mariethoz, C. Jaboulet, J. Hennebert, J.-F. Bonastre, C. Mokbel, F. Bimbot, « Behavior of a Bayesian Adaptation Method for Incremental Enrollment in Speaker Verification », International Conference on Acoustics, Speech, and Signal Processing, p. 1197-1200, Istanbul, Turquie, 5-9 Juin 2000.
- [4] L. Heck, N. Mirghafori, « On-Line Unsupervised Adaptation in Speaker Verification », International Conference on Spoken Language Processing, Vol. 2, p. 454-457, Pékin, Chine, 16-20 Octobre 2000.
- [5] P. Phillips, A. Martin, C. Wilson, M. Przybocki, « An Introduction to Evaluating Biometric Systems », Computer, Vol. 33, n°2, p. 56-63, Février 2000.
- [6] P. Phillips, H. Hyeonjoon, S. Rizvi, P. Rauss, « The FERET Evaluation Methodology for Face-Recognition Algorithms », IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, n°10, Octobre 2000.
- [7] S. Liu, M. Silverman, « A Practical Guide to Biometric Security Technology », IEEE Computer Society, IT Pro-Security, Janvier-Février 2001.
- [8] P. Verlinde, « Une Contribution à la Vérification Multimodale de l'Identité en Utilisant la Fusion de Décision », École Nationale Supérieure des Télécommunications, Paris, France, Septembre 1999.
- [9] L. Hong, A. Jain, S. Pankanti, « Can Multibiometrics Improve Performance ? », Proceedings AutoID'99, Summit, NJ, p.59-64, Oct 1999.
- [10] J. Kittler, M. Hatef, R. Duin, J. Matas, « On Combining Classifiers », IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 20, n°3, p. 226-239, 1998.
- [11] CNN World News. Schiphol Backs Eye Scan Security. Available at <http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/>, March 27, 2002.
- [12] J. Daugman. Recognizing Persons by Their Iris Patterns. In A. K. Jain, R. Bolle, and S. Pankanti, editors, Biometrics: Personal Identification in a Networked Society, pp. 103-121, Kluwer Academic Publishers, 1999.
- [14] « The Price of Biometrics », USA Today, 26 Janvier 1999 <http://www.usatoday.com/life/cyber/tech/ctc448.htm>.
- [15] « A Review of Dynamic Handwritten Signature Verification », James Cook University, Computer Science Department, Technical Article, 1997.
- [17] Airports Council International, <http://www.airports.org>.
- [18] « Identifiez-Vous au Doigt et à l'Oeil », Courrier Cadres, n°1412, 20 Septembre 2001.

- [19] « Biometrics Comes To Life », Banking Journal, Janvier 1997
http://www.banking.com/aba/cover_0197.htm.
- [20] Z. Korotkaya. Biometric person authentication : Odor, 2003.
- [21] M. Hashiyada. Development of biometric dna ink for authentication security. Tohoku Journal of Experimental Medicine, pages 109–117, 2004.
- [22] K. Phua, J. Chen, T. H. Dat, and L. Shue. Heart sound as a biometric. Pattern Recognition, 41 :906–919, 2008.
- [23] : Adrien LEMAITRE & Corentin BUET -ISTIA- E12 2011-2012.
- [24] : https://www.priv.gc.ca/information/research-recherche/2013/fr_201303_f.asp.
- [26] : https://fr.wikipedia.org/wiki/Système_de_reconnaissance_faciale.
- [27] : Kalghoum ANWAR, Institut supérieur d'informatique et de gestion de Kairouan en Tunisie, "Gestion des présences via la technologie de reconnaissance faciale ,2011.
- [28] : SOUHILA GUERFI ABABSA , Université Evry Val d'Essonne, France, Thèse de doctorat intitulé : Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D , 2008.
- [29] : Nicolas MORIZET, École Doctorale d'Informatique,Télécommunications et Électronique de Paris, France ,Thèse de doctorat intitulé : Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris, 2009.
- [30] : M. A. Turk and A. P. Pentland, Face Recognition using Eigenfaces, Proc. IEEE, 1991, 586-591.
- [31] : Nicolas MORIZET, Thomas EA, Florence ROSSANT, Frédéric AMIEL et AMARA. "Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie" P1-11. Institut Supérieur d'Electronique de Paris (ISEP), département d'Electronique, 2006.
- [32] : Michael David Kelly. Visual identification of people by computer. PhD thesis, Stanford, CA, USA, 1971.
- [33] : KANADE, T. 1973. Computer recognition of human faces. Birkhauser, Basel, Switzerland, and Stuttgart, Germany.

[34] : Mohamed ADJOUT et Abdelhak BENAÏSSA, «Fusion de la DCT-PCA et la DCT-LDA Appliquée à la reconnaissance de visages ».Institut National de formation en Informatique (I.N.I), Alger, 2007.

[35] : Toufik AMELLAL, Kamel BENAKLI, « Système de reconnaissance de visage basé sur les GMM ». Institut National de formation en Informatique (I.N.I), Alger, 2007.

[36] : Martinez, A. 2002. Recognizing imprecisely localized, partially occluded and expression variant faces from a single sample per class. IEEE Trans. Patt. Anal. Mach. Intell. 24, 748-763.

[37] : Y. Adini, Y. Moses, S. Ullman, Face recognition : The problem of compensating for changes in illumination direction. IEEE Trans. Patt. Anal. Mach. Intell. 19, 721–732, 1997.

[38] : D. Blackburn, M. Bone, P. J Phillips. “Face recognition vendor test 2000”. Tech. rep. <http://www.frvt.org>, 2001.

[39] : R. Gross, J. Shi, J. Cohn. Quo Vadis Face Recognition ?. Third Workshop on Empirical Evaluation Methods in Computer Vision, December, 2001.

[40]: Pierre Buyssens, Marinette Revenu. Fusion des modalités Visible et Infrarouge pour la Reconnaissance Faciale. RFIA, Jan 2010, Caen, France. 8 p., 2010.

[41]: Hassen Drira, Rim Slama, Boulbaba Ben Amor, Mohamed Daoudi, Anuj Srivastava. Une nouvelle approche de reconnaissance de visages 3D partiellement occultées. RFIA 2012 (Reconnaissance des Formes et Intelligence Artificielle), Jan 2012, Lyon, France. pp.978-2-9539515-2-3, 2012.

[43] Y. Oussar. Réseaux d'ondelettes et réseaux de neurones pour la modélisation statique et dynamique de processus. Thèse de doctorat de l'université Pierre et Marie Curie. Paris, France. Juillet 1998.

[44] D. Jonathan, B. Michael et F. Sébastien. Les Ondelettes. Université Libre de Bruxelles. Printemps des Sciences. Bruxelles. Belgique.

[45] A. Bultheel: Bull. Belg. Math. Soc. (1995) 2.

[46] Y. Meyer. Ondelettes et opérateurs I - Ondelettes. Hermann, Paris, 1990.

[47] Mallat, S. A wavelet tour of signal processing, Academic Press, second edition, 1998.

[48] DAUBECHIES, I. « The wavelet transforms time-frequency localization and signal analysis». IEEE Trans. On information theory, Vol. 36, N° 5, pp. 961-1005, September 1990.

[49] Moulay Abdelatif Akhloufi `RECONNAISSANCE DES VISAGES PAR IMAGERIE MULTISPECTRALE Du visible à l'infrarouge lointain` université Laval Québec.

[50] boudjellal.S `détection et identification de personne par méthode biométrique` UMMTO.

Webographie :

[1] <https://www.securiteinfo.com/conseils/biometrie.shtml>

[13] Recognition Systems Inc., <http://www.recogsys.com>.

[16] Visionics, <http://www.visionics.com>.

[25]<https://www.biometrie-online.net/technologies/voix/voix-abreviations/14>.
Technologies.

[42] <http://my-definitions.com/fr/definition/ondelette>.

- <https://www.mathworks.com/matlabcentral/fileexchange/?requestedDomain=www.mathworks.com>