



Faculté de Génie Electrique et d'Informatique
Département d'informatique

MEMOIRE

DE FIN D'ETUDE

En vue de l'obtention d'un diplôme de Master Académique en Informatique.

Option : Réseaux Mobilité et Systèmes Embarqués.

Présenté par :

ICHALLALENE Katia

AMARA Fatma

Thème

Développement d'un système biométrique pour la reconnaissance de visages basé sur l'approche LBP, ses variantes et un réseau neuronal

Encadreur : Mme FERHAOUI-CHERIFI Chafia

Président : Mr M .REMDANI

Examinatrice : Melle Y. YESLI

Promotion 2018-2019

Remerciement

*Nous tenons à témoigner notre reconnaissance à DIEU tout puissant,
qui nous a donné la force pour survivre, ainsi que l'audace pour
dépasser toutes les difficultés durant toute cette année.*

*Nous tenons avant tout à exprimer notre reconnaissance à notre
Promotrice*

Mme CHERIFI pour avoir accepté de nous encadrer dans cette étude.

*On la remercie pour son implication, son soutien et ses
encouragements tout au long de ce travail.*

*A tous les enseignants de l'UMMTO qui ont contribué à notre
formation.*

*Nos plus vifs remerciements vont aussi aux membres du jury pour
avoir accepté d'honorer par leur jugement notre travail.*

*Dans l'impossibilité de citer tous les noms, nos sincères
remerciements vont à tous ceux et celles,*

qui de près ou de loin,

*ont permis par leurs conseils et leurs compétences à la réalisation de
ce mémoire, en particulier nos chères familles et nos amis.*

Dédicaces

A mes très chers parents pour leurs encouragements et leurs soutien

A mes chers frères SAID et JUBA

A ma chère sœur AMEL

A tous mes amis (es), particulièrement ma binôme KATIA

*A tous ceux qui ont participé de près ou de loin dans la réalisation de
ce travail,*

Je dédie ce modeste travail

Fatma

Dédicaces

A mes très chers parents pour leurs encouragements et leurs soutien

A mon cher frère HALIM

A mes chères sœurs RYMA et AMIRA

A mon fiancé

A tous mes amis (es), particulièrement ma binôme FATMA

*A tous ceux qui ont participés de près ou de loin dans la réalisation de
ce travail,*

Je dédie ce modeste travail

Katia

Table des matières

Table des matières	5
Table des figures	11
Liste des tableaux	15
Introduction générale	1
	3
I Biométrie et Reconnaissance de Visages.	5
1 Biometrie : Concepts, application, et enjeu	7
1.1 Introduction	7
1.2 Biométrie	7
1.2.1 Définition	7
1.2.2 Un bref historique de la biométrie :	8
1.3 Les systèmes Biométriques	9
1.3.1 Définition d'un système biométrique :	9
1.3.2 Modules d'un système biométrique	9
1.3.3 Architecture d'un système biométrique	9
1.3.3.1 Module d'apprentissage (enrôlement) :	10
1.3.3.2 Module de reconnaissance :	11
1.3.3.3 Module d'adaptation :	12
1.3.4 Mesure de la performance d'un système biométrique	13
1.4 Modalités biométriques :	16
1.4.1 Les modalités morphologiques :	16
1.4.1.1 Les empreintes digitales :	16

1.4.1.2	La géométrie de la main :	17
1.4.1.3	L'iris :	18
1.4.1.4	La rétine :	19
1.4.1.5	Le visage :	20
1.4.2	Les modalités comportementale :	21
1.4.2.1	La reconnaissance vocale :	22
1.4.2.2	La signature :	22
1.4.2.3	La dynamique de frappe au clavier :	23
1.4.2.4	Analyse de la démarche :	24
1.4.3	Les modalités biologiques :	25
1.4.3.1	L'ADN :	25
1.4.3.2	Veines de la main :	26
1.4.3.3	Odeur corporelle :	27
1.4.3.4	d. La reconnaissance de la thermographie :	27
1.4.4	Les multimodalités :	28
1.5	Caractéristiques des modalités biométriques	28
1.6	Domaine d'application de la biométrie	30
1.6.1	Les applications commerciales :	30
1.6.2	Les applications gouvernementales :	30
1.6.3	Les applications judiciaires :	30
1.7	Les avantages et les limites de la biométrie	31
1.7.1	Les avantages de la biométrie	31
1.7.2	Les limites de la biométrie	32
1.8	Le marché de la biométrie :	33
1.8.1	Présentation du marché :	33
1.8.2	La part du marché par technologie :	35
1.9	Conclusion	35
2	Reconnaissance Automatique Du Visage	37
2.1	Introduction	37
2.2	Pourquoi le visage ?	37
2.3	Systèmes de reconnaissance faciale	38
2.3.1	Le monde physique	39
2.3.2	Acquisition	39
2.3.3	Détection de visage	39
2.3.4	Les prétraitements	39
2.3.5	Extraction des paramètres	39
2.3.6	L'apprentissage	40
2.3.7	La classification (Modélisation)	40
2.3.8	La décision	40

2.4	Principales difficultés de la reconnaissance de visages	40
2.4.1	Changement d'illumination	41
2.4.2	Variation de pose	41
2.4.3	Expression faciale	42
2.4.4	Présence de composants structurels	42
2.5	Etat de l'art des méthodes de reconnaissance de visage	42
2.5.1	Techniques 2D de la reconnaissance de visage	43
2.5.1.1	Les méthodes globales	43
2.5.1.2	Les méthodes locales	47
2.5.1.3	Les méthodes hybrides	51
2.6	Conclusion	52

53

II Extraction des caractéristiques et classification 55

3 Extraction de caractéristiques et classification 57

3.1	introduction	57
3.2	Pourquoi le motif binaire locale(LBP)	57
3.3	Définition de la texture	58
3.4	Définition de LBP	59
3.5	LBP circulaire	60
3.6	LBP uniformes	61
3.7	Histogramme LBP	62
3.8	Reconnaissance de visage avec LBP	63
3.9	variantes de l'opérateur LBP :	64
3.9.1	Complete local binary pattern (CLBP)	65
3.9.1.1	Extraction des caractéristiques avec la CLBP . . .	66
3.9.2	LBP Allongée (ELBP)	66
3.9.3	Ligne des motifs binaires locales (LLBP)	67
3.9.4	Applications de LBP et de ses variantes	68
3.9.4.1	La détection et le suivi d'objets	68
3.9.4.2	La biométrie :	68
3.9.5	Classification	68
3.9.5.1	La distance	69
3.10	Conclusion	70

4 État de l'art sur les reseaux de neurones 71

4.1	Introduction	71
-----	------------------------	----

4.2	Pourquoi les réseaux de neurones ?	71
4.3	Le neurone	72
4.3.1	Le neurone biologique	72
4.3.2	Le neurone artificiel	73
4.3.2.1	Structure	73
4.3.2.2	Comportement	73
4.4	Réseau de neurones	75
4.5	Topologie des réseaux de neurones	76
4.5.1	Réseau multicouche	76
4.5.2	Réseau à connexions locales	77
4.5.3	Réseau à connexions récurrentes (dynamiques)	77
4.5.4	Réseau à connexion complète	78
4.6	Type de réseaux de neurones	78
4.6.1	Réseaux de neurones non bouclés	79
4.6.1.1	. Réseau de neurone monocouche (Perceptron) . . .	80
4.6.1.2	Perceptron Multicouches	81
4.6.1.3	Les Réseaux de Neurones à Fonctions à Base Ra- diale	82
4.6.2	Les réseaux de neurones bouclés	83
4.6.2.1	Réseau de Hopfield(HNN)	84
4.6.2.2	La carte auto-organisatrice de Kohonen (SOM) . .	84
4.6.2.3	Les réseaux compétitifs	85
4.6.2.4	Les Réseaux ART	86
4.7	Apprentissage des réseaux de neurones	86
4.7.1	Types d'apprentissage	87
4.7.1.1	Apprentissage supervisé (supervised Learning) . .	87
4.7.1.2	Apprentissage non supervisé (unsupervised Learning)	87
4.7.1.3	Apprentissage par renforcement (Apprentissage semi supervisé)	87
4.7.1.4	Apprentissage mixte (hybride)	88
4.7.2	Les règles d'apprentissage	88
4.7.2.1	Règle de Hebb	88
4.7.2.2	Apprentissage par compétition	89
4.7.2.3	Règle de Correction d'erreur	90
4.7.2.4	Apprentissage de Boltzman	90
4.8	Les avantages et les inconvénients des réseaux de neurone	90
4.8.1	Les avantages des réseaux de neurones	90
4.8.2	Les points faibles des réseaux de neurones	91
4.9	Domaines d'applications	92
4.10	Réseaux de neurones et classification d'images	93

4.11	Conclusion	94
5	Conception et Réalisation	95
5.1	Introduction	95
5.2	Mise en situation	95
5.3	Conception du système	95
5.3.1	Les acteurs du système	96
5.3.2	Le diagramme de cas d'utilisation global :	96
5.3.3	Description textuelle des cas d'utilisation	97
5.3.3.1	Déscription du cas d'utilisation « Apprentissage »	97
5.3.3.2	Déscription du cas d'utilisation « identification »	98
5.3.3.3	Déscription du cas d'utilisation « authentification »	98
5.3.3.4	Déscription du cas d'utilisation « Performane Iden- tification »	99
5.3.3.5	Déscription du cas d'utilisation «performance vé- rification »	99
5.3.4	Diagrammes de séquence (cas d'utilisation détaillés) :	99
5.3.4.1	Cas d'utilisation : Apprentissage	100
5.3.4.2	Cas d'utilisation : Identification	101
5.3.4.3	Cas d'utilisation : Authentification	102
5.3.4.4	Cas d'utilisation : Performance identification	103
5.3.4.5	Cas d'utilisation : Performance vérification	104
5.3.5	Architecture et fonctionnement du système	105
5.3.5.1	L'Apprentissage	105
5.3.5.2	Module prétraitement :	106
5.3.5.3	Module extraction des paramètres :	106
5.3.5.4	Module de sauvegarde :	108
5.3.5.5	Phase de reconnaissance et la prise de décision	109
5.3.6	Calcul des performances du système	112
5.4	Implémentation et Réalisation	113
5.4.1	Outils de test et développement	114
5.4.1.1	MATLAB	114
5.4.2	L'implémentation de notre système :	115
5.4.2.1	Présentation de l'application	115
5.5	Conclusion	120
6	Test et évaluation des résultats	121
6.1	Introduction	121
6.2	La base de données ORL	121

6.3	Evaluation du système	124
6.3.1	Évaluation de la première approche en utilisant le classifieur basé sur les métriques de distances	125
6.3.1.1	Mode identification	125
6.3.1.2	Mode authentification	128
6.3.2	Évaluation de la deuxième approche en utilisant la classifi- cation par réseau de neurone	132
6.3.2.1	Variation du paramètre « fonction d'activation » .	133
6.3.2.2	Variation du paramètre « fonction d'entraînement »	134
6.3.2.3	Variation du nombre de neurones dans la couche cachée avec LBP uniforme :	134
6.3.2.4	Variation du taux d'apprentissage avec LBP uni- forme :	135
6.3.2.5	Variation du nombre d'itérations avec LBP uniforme	136
6.3.3	Amélioration des résultats obtenus en terme d'authentification	137
6.3.3.1	Variation du nombre de neurones dans la couche cachée :	137
6.3.3.2	Variation du taux d'apprentissage avec LBP uni- forme :	138
6.3.3.3	variation du nombre d'itérations avec LBP uniforme	139
6.3.4	Amélioration des performances de notre système en utilisant la division en 16 blocs(28*23)	140
6.3.4.1	Variation du nombre de neurones dans la couche cachée avec LBP uniforme :	140
6.3.5	Comparaison des résultats :	143
6.3.6	Conclusion	143
	Conclusion générale et perspectives	145
	Bibliographie	147

Table des figures

1.3.1	Architecture d'un système biométrique	10
1.3.2	Enrôlement d'une personne dans un système biométrique[N.Morizet 09]	10
1.3.3	Identification d'un individu dans un système biométrique [N.Morizet 09]	11
1.3.4	Authentification d'un individu dans un système biométrique[N.Morizet 09]	12
1.3.5	courbe de distribution des scores imposteurs et authentique et les taux d'erreurs (FAR et FRR), pour un seuil de donné	13
1.3.6	courbe ROC	14
1.3.7	Exemple de courbe CMC	15
1.4.1	Une empreinte digitale[zakaria 14]	17
1.4.2	Appareil d'acquisition de la géométrie de la main	18
1.4.3	L'iris [zakaria 14]	19
1.4.4	la rétine[Fouad 18]	20
1.4.5	Reconnaissance du visage	21
1.4.6	Spectre d'un signal de voix[Douib 16]	22
1.4.7	La signature[Amina 16]	23
1.4.8	La dynamique de frappe au clavier[Céline 13]	24
1.4.9	La démarche	25
1.4.10	l'ADN	25
1.4.11	Veines de la main	26
1.4.12	La thermographie faciale	28
1.8.1	Perspectives des revenus du marché mondial de la biométrie [Stephen 14]	34
1.8.2	Parts de marché des différentes méthodes biométrique	35
2.3.1	Le processus de reconnaissance de visage[Serge 10].	38
2.4.1	Exemple de variation d'éclairage[Bettahar Abdessettar 14]	41
2.4.2	Exemple de variation de pose[Bouchra 13].	41
2.4.3	Exemple de variation d'expressions.	42
2.5.1	Classification des algorithmes principaux utilisés en reconnaissance faciale[Nicolas 01]	43
2.5.2	le principe des méthodes globales.	44
2.5.3	Caractéristiques autour desquelles est réalisée une ACP	46

2.5.4	les projections ACP et LDA d'un ensemble de données.	47
2.5.5	Les 5 états d'un HMM (de haut en bas) [R.Djourani 06].	49
2.5.6	Représentation de neurone formel	50
2.5.7	Une illustration de LBP basique	50
2.5.8	Exemples de d'opérateur LBP	51
2.5.9	Découpage de l'image originale en 7×7 , 5×5 et 3×3 régions [F. Perronnin 03]	51
3.2.1	stabilité de LBP au changement d'illumination [Serge 10]	58
3.4.1	Calcul et génération du code LBP pour un pixel d'une image	59
3.5.1	Exemples de différents voisinages circulaires pour les LBP	60
3.6.1	Exemple d'un modélé uniforme et non uniforme	61
3.6.2	Les 58 différents motifs uniformes dans un voisinage (8,R)[Juslin 16]	62
3.8.1	Illustration de la procédure d'extraction de LBP[Bettahar Abdessettar 14].	64
3.8.2	Illustration du stage de reconnaissance.	64
3.9.1	Méthodologie de CLBP	66
3.9.2	Des exemples de ELBP avec différentes valeurs de A, B, et m[Mekkani 84]	67
3.9.3	opérateur LLBP avec une longueur de ligne de 9 pixels [Mekkani 84]	67
4.3.1	Schéma simplifié d'un neurone biologique.	72
4.3.2	Mise en correspondance neurone biologique/neurone artificiel[Claude 92b]	73
4.3.3	Modèle d'un neurone formel	74
4.3.4	Les modèles de fonctions d'activation	75
4.4.1	Forme générale d'un Réseaux de neurone	75
4.5.1	Réseau multicouche	77
4.5.2	Réseau à connexions locales[Yasmine 99]	77
4.5.3	Réseau à connexions récurrentes[Yasmine 99]	77
4.5.4	Réseau à connexion complète[Yasmine 99]	78
4.6.1	Topologie des réseaux de neurones[James G 17].	79
4.6.2	un réseau de neurone non bouclé [Zahir 14].	80
4.6.3	Perceptron Multi Couche PMC [Philippe]	80
4.6.4	Perceptron Multi Couche PMC [Philippe]	82
4.6.5	Architecture générique d'un RBF	83
4.6.6	Architecture de Hopfield	84
4.6.7	Topologie de Kohonen[Youcef 17]	85
4.6.8	Les réseaux à compétition	86
4.7.1	i le neurone amont, j le neurone aval et wij le poids de la connexion	88
4.7.2	La loi de Hebb	89
5.3.1	Diagramme de cas d'utilisation global	97
5.3.2	Diagramme de séquence cas d'utilisation « Apprentissage ».	100

5.3.3	Diagramme de séquence cas d'utilisation « Identification ».	101
5.3.4	Diagramme de séquence cas d'utilisation « Authentification ».	102
5.3.5	Diagramme de séquence cas d'utilisation « Performance identification ».	103
5.3.6	Diagramme de séquence cas d'utilisation « Vérification ».	104
5.3.7	Diagramme de fonctionnement du système	105
5.3.8	Représentation modulaire de la phase apprentissage	106
6.2.1	Base de données ORL[Ahmed 15]	122
6.2.2	Exemple de changements d'orientations du visage	122
6.2.3	Exemple de changements d'éclairage	122
6.2.4	Exemple de changements des expressions faciales	123
6.2.5	Exemple de port de lunettes	123
6.2.6	Exemple de changements de coiffure et de port de barbe	123

Liste des tableaux

1.1	Comparaison entre les techniques biométriques[Hanane 12].	29
1.2	Comparaison entre l'authentification biométrique et par mot de passe clé	32
3.1	Exemple d'histogramme LBP	63
5.1	Représentation de l'étape prétraitement	106
5.2	Module Extraction de paramètres	106
5.3	Calcul du code LBP uniforme pour un pixel	107
5.4	Calcul de l'histogramme LBP uniforme	108
5.5	Programme du réseau	110
5.6	Tableau capitulatif des paramètres du réseau neuronal utilisé . . .	111
5.7	Calcul du FRR	113
5.8	Calcul du FAR	113
5.9	Interface Apprentissage	115
5.10	Interface performance identification	116
5.11	Interface vérification	117
5.12	Interface identification	118
5.13	Interface authentification	119
5.14	Interface Prétraitement	120
6.1	Variation du taux d'identification TID (%) en fonction des va- riantes LBP uniforme et les distances pour un bloc	125
6.2	Variation du taux d'identification TID (%) en fonction des va- riantes LBP uniforme et les distances pour quatre blocs	126
6.3	Variation du taux d'identification TID (%) en fonction des va- riantes LBP uniforme et les distances pour seize bloc	127
6.4	Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage pour un bloc.	128
6.5	Variation du taux des faux rejets FRR (%) en fonction du rayon et voisinage pour un bloc.	128

6.6	Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage pour quatre blocs.	129
6.7	Variation du taux des faux rejets FRR (%) en fonction du rayon et voisinage pour quatre blocs.	130
6.8	Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage pour seize blocs.	131
6.9	Variation du taux des faux rejets FRR (%) en fonction du rayon et voisinage pour seize blocs.	131
6.10	Résultats du FAR, FRR et TID (%) en variant les fonction d'activation	133
6.11	Résultats du FAR, FRR et TID (%) en variant les fonction de transfert	134
6.12	Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre neurone	135
6.13	Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et taux d'apprentissage	136
6.14	Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre d'itération	137
6.15	Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre neurone	138
6.16	Variation du FAR, FRR et TID (%) en fonction de type LBP et taux d'apprentissage	139
6.17	Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre d'itération	140
6.18	Variation du FAR, FRR et TID (%) en fonction du nombre de neurones	141
6.19	Variation du FAR, FRR et TID (%) en fonction du nombre de neurones	142

Introduction générale

Le contrôle d'accès a toujours été un aspect essentiel pour la sécurité de notre société. Pour répondre à ces besoins les outils classiques tel que les mots de passes et les badges ne suffisent plus car l'utilisation d'un mot de passe nécessite sa mémorisation et le fait d'en avoir plusieurs rendent la tâche plus difficile, le noter engendre le risque de perte ou de vol. De même, l'utilisation de cartes magnétiques ou de badges n'échappe pas aux risques de vol par des imposteurs qui sont capable de falsifier leur identité. Afin d'accroître la fiabilité des systèmes de sécurité classique, la biométrie est une alternative de plus en plus employée.

La biométrie se focalise sur l'analyse de données liées à l'identité d'un individu par des méthodes mathématiques en se basant sur ses propres et uniques caractéristiques biologiques, comportementaux ou physiologiques. Elle est utilisée dans plusieurs domaines, tout en garantissant un niveau de sécurité élevé, elle pallie aux risques d'accès ou d'oubli des mots de passes.

Différentes techniques d'authentifications basées sur les caractéristiques physiques de l'utilisateur ont été développées par la recherche scientifique comme la reconnaissance faciale qui a progressé à pas de géant. Elle s'impose aujourd'hui comme la plus naturelle des mesures biométriques, elle présente un avantage d'être naturelle et facile à mettre en œuvre ; mais qui peut être sensible à certains éléments externes tel que l'éclairage, la qualité du capteur, la variation des pose les occultations et les expressions faciales.

Plusieurs méthodes de reconnaissance de visages ont été proposées durant ces trente dernières années, qui ont été classé en trois catégories : les approches globales comme ACP, les approches locales comme LBP, les approches hybrides.

Le modèle binaire local (LBP) est un descripteur non paramétrique qui résume efficacement les textures locales des images. Au cours de ces dernières années, il a suscité un intérêt croissant dans diverses domaines du traitement d'images et de la vision par ordinateur et a montré son efficacité dans de nombreuses applications, en particulier pour l'analyse d'images faciales, comprenant des tâches aussi différentes que la détection des visages, la reconnaissance des visages, l'analyse de l'expression faciale. Le but d'un système de reconnaissance de visages est de simuler le système de reconnaissance humain par la machine pour automatiser certaines applications

telles que : La télésurveillance, le contrôle d'accès à des sites, accès à des bâtiments sécurisés, etc.

C'est dans ce cadre que se place notre projet de fin d'études qui consiste à développer un système biométrique pour la reconnaissance faciale basé sur l'opérateur LBP et ses variantes en se basant sur deux types de classifieurs à savoir : les métriques de distance (euclidienne, ctb , mahcos, cosinus, sqr) et les réseaux neuronaux de type MLP, qui se veut être fiable et adaptée à un environnement présentant des variabilités de luminance, de pose, d'expression de visage et présence ou absence des composants structurels.

Il est nécessaire de travailler à tous les niveaux du système ; détection, prétraitement, extraction des caractéristiques et classification. Nous, on se base sur l'extraction des caractéristiques en utilisant l'approche LBP qui nous permettent d'extraire les données pertinentes d'une image grâce à son invariance aux influences des éléments externes, puis les classifier avec les normes de distance ou le réseau de neurone qui se sont montrés très efficaces dans le domaine de la reconnaissance statistique de forme.

Afin de décrire le travail effectué, cette recherche comporte les six principaux chapitres organisés comme suit :

Chapitre I : « BIOMETRIE : CONCEPTS, APPLICATION ET ENJEUX », décrit les modalités biométriques, le principe de fonctionnement des systèmes et les outils utilisés pour mesurer leurs performances ainsi que leurs avantages et limites.

Chapitre II : « SYSTEME DE RECONNAISSANCE AUTOMATIQUE DU VISAGE », décrit la place de la reconnaissance faciale parmi les autres modalités biométriques, également les principales composantes d'un système de reconnaissance faciale, notamment la détection, l'extraction de caractéristiques et la reconnaissance. Enfin, une analyse détaillée de différentes techniques développées au cours de ces dernières années dans la reconnaissance faciale.

Chapitre III : « APPLICATION DE LBP POUR L'EXTRACTION DES CARACTERISTIQUE ET CLASSIFICATION », décrit en particulier la méthode locale : LBP. Ces principes de fonctionnement ainsi que ses avantages apportés pour la communauté scientifique.

Chapitre IV : « ÉTAT DE L'ART SUR LES RÉSEAUX DE NEURONES », décrit la topologie, les types et les modes d'apprentissage des réseaux de neurones. Ainsi que leurs avantages, point faible et applications.

Chapitre V : « CONCEPTION ET RÉALISATION » présente la phase de conception et réalisation du système, les cas d'utilisation de notre système ainsi que toutes les méthodes utilisées pour le réaliser.

Chapitre VI : « TEST ET ÉVALUATION DES RÉSULTATS » donne les tests et les résultats obtenus après réalisation et exécution de notre système toutes en donnant une synthèse de notre travail.

Première partie

Biométrie et Reconnaissance de Visages.

Chapitre 1

Biometrie : Concepts, application, et enjeu

1.1 Introduction

Grace à la puissance de calcul grandissante des ordinateurs, les applications biométriques sont devenues de plus en plus nombreuses et efficaces. La biométrie s'invite progressivement dans notre vie quotidienne, elle fait partie des grands enjeux pour un monde plus sûr. Le marché des produits d'authentification et d'identification est en pleine croissance, dû à la nécessité croissante du besoin de sécurité de chacun, dans les domaines privés, professionnels ou publics.

La biométrie est de plus en plus utilisée pour les titres d'identité, dans les aéroports, les établissements pénitentiaires, l'accès à des locaux sécurisés, le vote électronique, la sécurité des paiements bancaires ou des transactions via Internet.

Dans ce chapitre, nous introduisons tout d'abord la définition de la biométrie et ses origines, nous décrivons le principe de fonctionnement d'un système biométrique ainsi que les outils d'évaluations utilisés pour mesurer leurs performances, nous donnons un bref aperçu des modalités biométriques les plus répandues.

1.2 Biométrie

1.2.1 Définition

Définition de la biométrie : Le terme "biométrie" provient des mots grecs, « bios » qui veut dire la vie et du mot « métrique » qui veut dire mesure[Francis 88]. La biométrie englobe les technologies utilisées pour mesurer et analyser les caractéristiques uniques d'une personne.

La biométrie peut être définie comme étant "la reconnaissance automatique

d'une personne en utilisant des traits distinctifs"[John D. 03]. Une autre définition de la biométrie est "toutes caractéristiques physiques ou traits personnels automatiquement mesurables, robustes et distinctives qui peuvent être utilisées pour identifier un individu ou pour vérifier l'identité prétendue d'un individu".

1.2.2 Un bref historique de la biométrie :

Les toutes premières formes d'utilisation de la biométrie remontent à bien plus longtemps que ce que la plupart des personnes croient. En effet, les historiens ont des traces d'échanges commerciaux babyloniens utilisant les empreintes digitales pour la transaction de biens, en office des signatures, ou encore vers le 7ème siècle en Chine antique pour les mêmes raisons. On observe par contre une période « d'inactivité », durant laquelle on ne dispose pas de nouvelles découvertes à propos de la biométrie [Estelle]. Ainsi, jusqu'au 17ème siècle, nous ne détenons aucune ressource à propos de l'histoire de la biométrie.

Alphonse Bertillon, est l'inventeur du premier système biométrique, appelé plus tard "système Bertillon ou Bertillonage" en 1882. Ce système était basé sur un ensemble de mesures anthropométriques comme la longueur de la main ou la distance entre les yeux. Peu pratique et insuffisamment fiable, l'empreinte digitale s'est ensuite imposée sur le système Bertillon à partir des années 1900. Ce système d'identification, aussi appelé "système Henry" dans les pays anglo-saxons pour Edward Henry, est basé sur l'unicité et la permanence de certaines figures cutanées (boucles, arches, tourbillons).

Depuis lors, de nombreux autres traits physiques ont été étudiés pour reconnaître les personnes. On peut noter les premiers travaux sur reconnaissance faciale en 1973 au Japon par Takeo Kanade ou également les travaux sur l'Iris de John Daugmann en 1994. Plusieurs chercheurs ont également proposé au début des années 2000 d'utiliser plusieurs traits biométriques afin de construire un système multimodal plus performant que les systèmes existants basés sur une seule modalité. En 2010 le plus ambitieux programme d'identité numérique au monde dénommé Aadhaar (une identité pour tous) basé sur plusieurs modalités [Antitza] a été lancé en Inde.

Actuellement la biométrie est largement utilisée lors des contrôles aux frontières, elle devient même un outil dans la vie de tous les jours pour accéder à des ressources de manière fiable et conviviale. C'est dans ce contexte que l'iPhone X en 2017 intègre un module de reconnaissance faciale.

1.3 Les systèmes Biométriques

1.3.1 Définition d'un système biométrique :

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en acquérant des données biométriques à partir d'un individu[Attalah 12], extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques à la signature dans la base de données.

Il sert à vérifier l'identité d'une personne à l'aide d'une ou plusieurs modalités qui lui sont propres (voix, iris, empreintes digitales, visage . . .). On peut dire qu'un système de contrôle biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à l'individu.

1.3.2 Modules d'un système biométrique

Un système biométrique typique peut être représenté par quatre modules principaux :

- **Le module de capture** : qui est responsable de l'acquisition des données biométriques d'un individu, cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité, etc.
- **Le module d'extraction de caractéristiques** : qui prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.
- **Le module de correspondance** : compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude entre les deux.
- **Le module de décision** : vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s).

1.3.3 Architecture d'un système biométrique

Il existe toujours au moins trois modules dans un système biométrique : le module d'apprentissage et celui de reconnaissance [S.lui 01], le troisième module 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 [C.Fredouille 06]. 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.

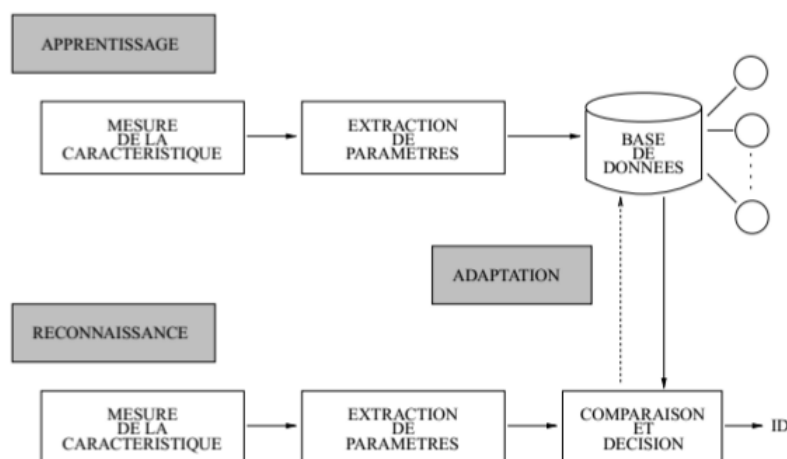


FIGURE 1.3.1 – Architecture d'un système biométrique

1.3.3.1 Module d'apprentissage (enrôlement) :

L'enrôlement est la première phase de tout système biométrique, il s'agit de l'étape pendant laquelle un utilisateur est enregistré dans le système pour la première fois et où une ou plusieurs modalités biométriques sont capturées et enregistrées dans une base de données [N.Morizet 09]. Cet enregistrement peut s'accompagner par l'ajout d'information biographique dans la base de données. Cette phase comporte deux principaux modules : module de capture et module d'extraction de caractéristiques.

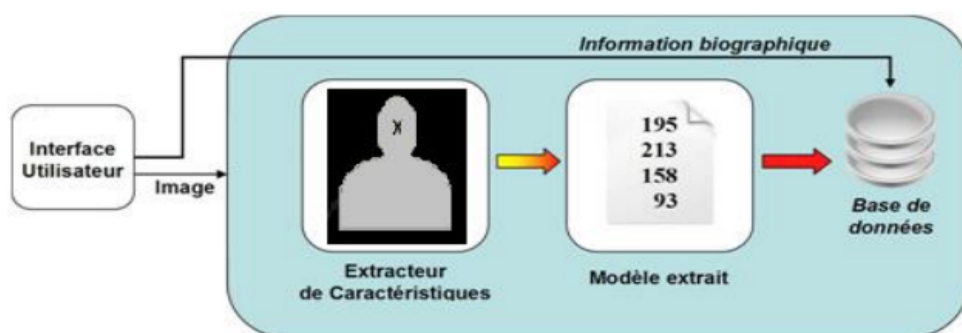


FIGURE 1.3.2 – Enrôlement d'une personne dans un système biométrique[N.Morizet 09]

1.3.3.2 Module de reconnaissance :

Une modalité biométrique de la personne qui désire être reconnue est captée par un dispositif d'acquisition. Les paramètres pertinents de l'individu en question seront par la suite extraits. L'étape suivante dépend du mode de reconnaissance, à savoir l'identification ou l'authentification.

1. Système opérant en mode identification :

Cette méthode consiste à sélectionner l'identité correcte d'une personne inconnue à partir d'une base de données d'identités enregistrées. Il est appelé processus de correspondance « un à plusieurs » (1...N), car le système doit effectuer une comparaison entre les données biométriques de la personne et tous les modèles biométriques stockés dans une base de données[Mohamed 07]. La sortie du système biométrique est constituée par l'identité de la personne dont le modèle possède le degré de similitude le plus élevé avec l'échantillon biométrique présenté en entrée. Typiquement, si la plus grande similarité entre l'échantillon et tous les modèles est inférieure à un seuil de sécurité minimum fixé, la personne est rejetée, ce qui implique que l'utilisateur n'était pas une des personnes enrôlées par le système. Dans le cas contraire, la personne est acceptée.

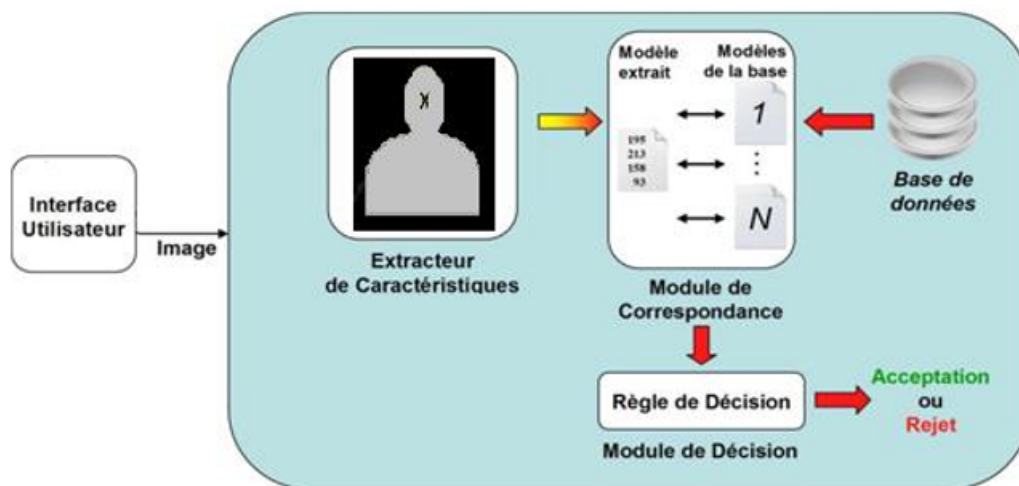


FIGURE 1.3.3 – Identification d'un individu dans un système biométrique [N.Morizet 09]

1. Système opérant en mode authentification :

Le mode de vérification ou authentification est une comparaison "un à un", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisies avec le modèle biométrique de cette personne stockée dans la base de données du système[Souhila 08]. Dans un tel mode, le système doit alors répondre

à la question suivante : « Suis-je réellement la personne que je suis en train de proclamer ? » . Actuellement la vérification est réalisée via un numéro d'identification personnel, un nom d'utilisateur, ou bien une carte à puce.

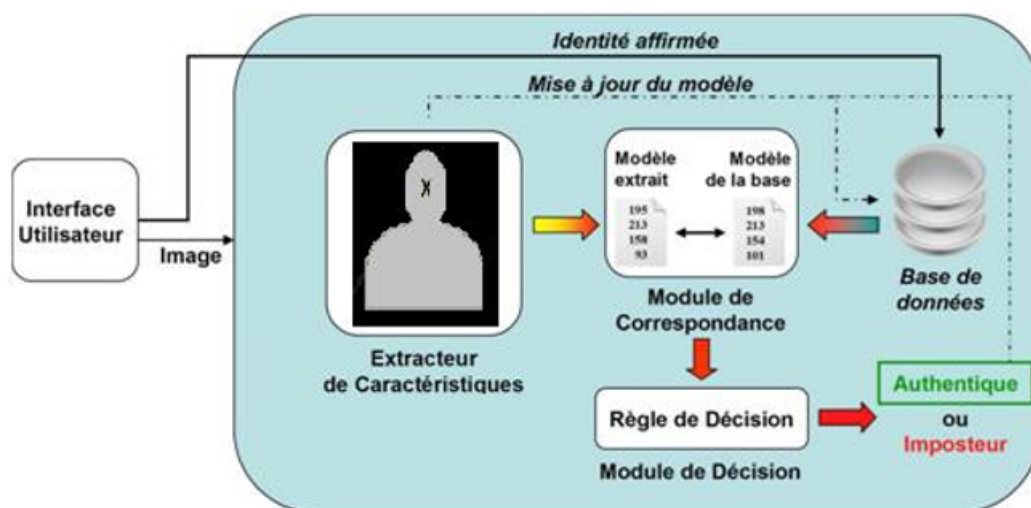


FIGURE 1.3.4 – Authentification d'un individu dans un système biométrique[N.Morizet 09]

1.3.3.3 Module d'adaptation :

Pendant la phase d'apprentissage, afin de limiter la gêne pour l'utilisateur y a que quelques instances d'un même attribut qui sont capturés par le système biométrique. Donc y a souvent certaines difficultés pour construire un modèle assez général capable de décrire toutes les variations de cet attribut. De plus, la variation des caractéristiques de cette biométrie ainsi que ses conditions d'acquisition sont toujours envisagées[C. Fredoville 00]. L'adaptation est donc nécessaire pour maintenir voire améliorer la performance d'un système utilisation après utilisation. L'adaptation peut se faire en deux modes : supervisé ou non-supervisée, mais en pratique le mode non-supervisée est de loin le plus convenable. 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[C. Fredoville 00]. L'adaptation est quasi indispensable pour les caractéristiques non permanentes comme la voix.

1.3.4 Mesure de la performance d'un système biométrique

En mode vérification, les performances d'un système biométrique sont données par la mesure de deux taux d'erreurs [Hizem] le FRR (False Rejet Rate ou Taux de Faux Rejet) et le FAR (False Acceptation Rate ou Taux de Fausse Acceptation).

— Le FRR ou le TFR : le taux de faux rejet ("False Reject Rate" ou FRR)
Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système [Pierre 11].

$$FRR = \frac{\text{nombre des clients rejetés}(FR)}{\text{nombre total de test clients}}$$

— Le FAR ou le TFA : le taux de fausse acceptation ("False Accept Rate" ou FAR)

Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système [Hizem].

$$FAR = \frac{\text{nombre des imposteurs acceptés}}{\text{nombre total de test imposteurs}}$$

Le EER : le taux d'égale erreur ("Equal Error Rate" ou EER). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où $FRR = FAR$, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.

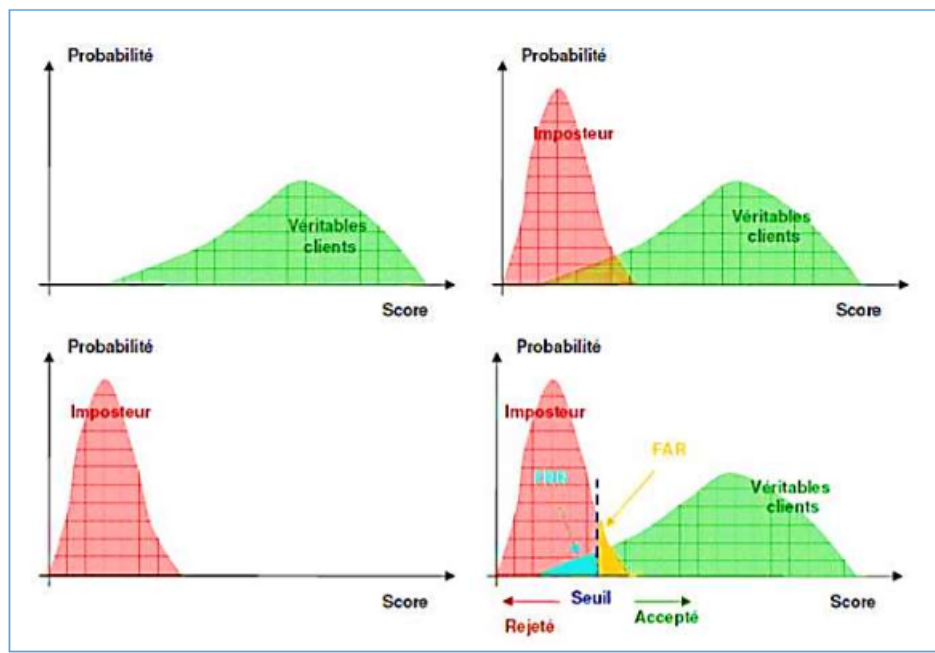


FIGURE 1.3.5 – courbe de distribution des scores imposteurs et authentique et les taux d'erreurs (FAR et FRR), pour un seuil de donné

Le problème de l'authentification peut être formalisé par [Souhila 08] :

Soient X_Q le vecteur de caractéristiques de la personne proclamée I , X_t le vecteur de caractéristiques de la personne I stockée dans la base de données, $S(X_Q, X_t)$ la fonction de similarité entre le vecteur X_Q et X_t . La fonction S donne le score de similarité entre les mesures biométriques de la personne de la base de données et la personne proclamée.

Le test de vérification est alors défini par la fonction (I, X_Q) , telle que :

$$\begin{cases} w1 & \text{si } S(X_Q, X_t) \geq \theta \\ w2 & \text{sinon} \end{cases}$$

Où $w1$ indique que la personne proclamée est vraie et $w2$ qu'elle n'est pas vraie.

L'utilisation de la courbe ROC (Receiver Operating Characteristic) est très fréquente pour l'évaluation de tels systèmes d'authentification [Pierre 11], elle représente la variation de taux FRR en fonction du taux de FAR. C'est une courbe strictement décroissante dont le taux d'égale erreur peut être facilement identifiable puisqu'il s'agit de l'intersection de cette courbe avec la droite d'équation $y = x$.

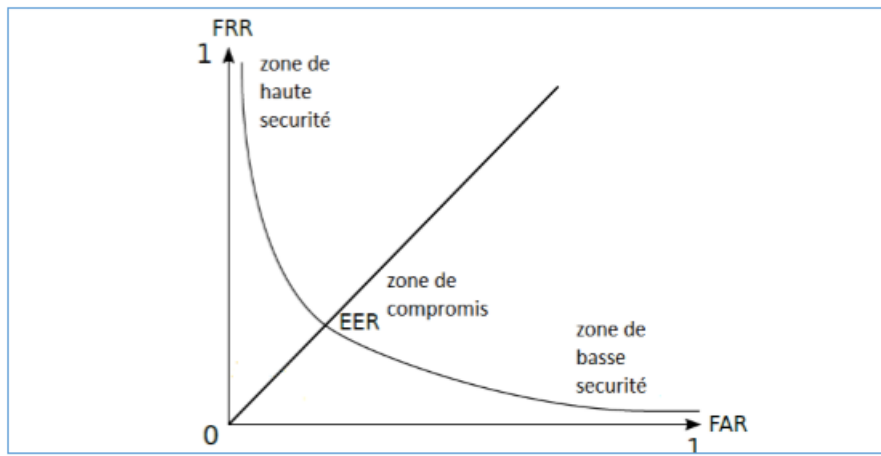


FIGURE 1.3.6 – courbe ROC

En mode Identification, les performances sont mesurées par le pourcentage des personnes bien reconnues par rapport aux nombres de tests, appelé le Taux d'Identification (TID) qui est définie par la formule suivante :

$$TID = \frac{\text{nombre de tests qui ont conduit à une bonne identification}}{\text{nombre total de tests}}$$

Le problème d'identification peut être formalisé par :

Soient X_Q le vecteur de caractéristiques, pour déterminer l'identité I_K , $k \in \{1, 2, \dots, N, N+1\}$ où $I_1, I_2, \dots, I_N$ sont les identités des personnes enrôlées dans le système, I_{N+1} une identité rejetée, on calcule la fonction (I, X_Q) définie par [Estelle] :

$$\begin{cases} I_k & \text{si } \max \{S(X_Q, X_{i,k}) \geq \theta\} \quad k = 0, \dots, N \\ I_{N+1} & \text{sinon} \end{cases}$$

Où $X_{i,k}$ est le vecteur de caractéristique correspond à l'identité I_k , le seuil.

Le teste d'identification se fait souvent en utilisant la courbe CMC (Cumulative Match Characteristics) qui représente le taux d'identification du système en fonction d'une variable que l'on appelle le rang [N.Morizet 09]. Le rang est une variable définie après que l'identification d'un individu est réalisée avec succès. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit le plus proche individu correspond à l'identité proclamée. On dit qu'un système reconnaît au rang 2 lorsqu'il choisit parmi deux images celle qui correspond le mieux à l'image d'entrée, et ainsi de suite.

La courbe CMC est une courbe strictement croissante, dont l'abscisse est compris entre $[0, n1]$ où $n1$ est le nombre d'identités dans la base, et l'ordonnée est comprise entre 0 et 100 [Pierre 11].

Un des points les plus importants sur ce type de courbe est le taux de reconnaissance pour l'abscisse 1, donc plus le degré du rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité fiables.

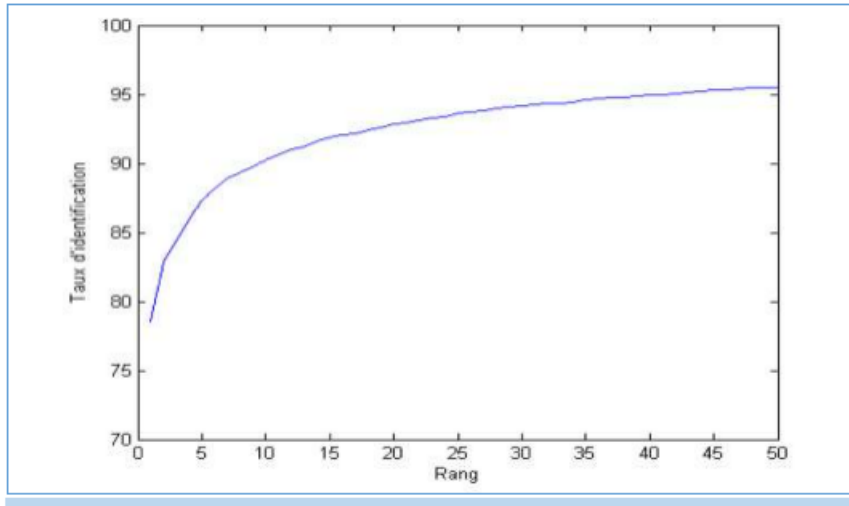


FIGURE 1.3.7 – Exemple de courbe CMC

1.4 Modalités biométriques :

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques propres à un individu : physique ou comportementale. Il est basé sur l'analyse de données liées à l'individu qui peuvent être classées en trois grandes catégories : analyse basée sur la morphologie, analyse de traces biologiques et l'analyse comportementale. Il peut être représenté par quatre modules principaux :

1.4.1 Les modalités morphologiques :

Cette catégorie s'appuie sur l'utilisation des traits physiques qui sont uniques et permanents chez l'individu. Plusieurs modalités ont été employées pour extraire cette information comme le visage 2D et 3D, l'empreinte digitale, la géométrie de la main, l'iris, etc.

Parmi les mesures physiologiques les plus répandues on cite :

1.4.1.1 Les empreintes digitales :

Il s'agit de la technologie biométrique la plus employée à l'heure actuelle dans le monde (plus du tiers du marché). Les empreintes digitales sont le dessin formé par les lignes de la peau des doigts, appelées aussi dermatoglyphes, c'est une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Les motifs dessinés par les crêtes et plis de la peau sont différents pour chaque individu, d'ailleurs la probabilité de trouver deux empreintes digitales identiques est très faible (de 1 sur 10 puissances 24)[Juslin 16] ; c'est ce qui motive leur utilisation par la police criminelle depuis le 19^e siècle. On distingue deux types d'empreintes : l'empreinte directe ou visible qui laisse une marque visible à l'œil nu et l'empreinte latente ou invisible qui est composée de lipides, de sueur et de saletés déposés sur un objet touché[Amina 16]. Une empreinte digitale se compose principalement de crêtes (Ridges) et de vallées (Valleys). On regroupe ces points clés de l'empreinte sous le terme de minuties. C'est l'étude des minuties qui permet d'identifier de façon certaine un individu.

Les minuties représentent les arrêts de lignes, les bifurcations, les lacs, les îlots et les points qui composent l'empreinte digitale, la combinaison des minuties est quasi infinie [zakaria 14].

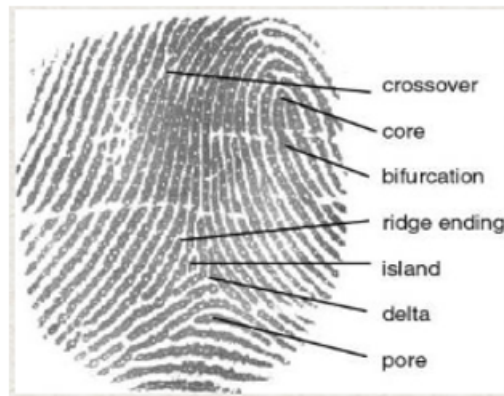


FIGURE 1.4.1 – Une empreinte digitale[zakaria 14]

Avantages et inconvénients :

Avantages	Inconvénients
-La technologie la plus éprouvée techniquement et la plus connue du grand public. -Faible coût des lecteurs -Petite taille du lecteur facilitant son intégration dans la majorité des applications - Traitement rapide -Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.	- Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). -Difficulté de lecture : sensibilité aux altérations pouvant survenir au cours de la vie et à certaines variations - Acceptabilité moyenne de la part du grand publique

1.4.1.2 La géométrie de la main :

La géométrie de la main est une technologie biométrique récente. Comme son nom l'indique, ce système fait appel à la forme de la main[Deluzarche 06].

La silhouette de la main est une caractéristique unique à chaque individu. Des paramètres (jusqu' à 90 caractéristiques de la main sont mesurées) tels que la longueur des doigts, leur épaisseur et leur position relative sont acquises grâce à un scanner spécialisé.



FIGURE 1.4.2 – Appareil d'acquisition de la géométrie de la main

Avantages et inconvénients :

Avantages	Inconvénients
- Bien acceptée de la part des usagés. - Très simple à utiliser. - Le résultat est indépendant de l'humidité et de l'état de propreté des doigts. - Simple à mettre en œuvre	-Trop encombrant pour un usage sur le bureau, dans une voiture ou dans un téléphone. - Risque de fausses acceptations pour des jumeaux ou des membres d'une même famille - la forme de la main change avec l'age

1.4.1.3 L'iris :

L'identification d'iris est devenue une technique biométrique populaire, elle est généralement reconnue qu'étant peut être la technique la plus précise en termes d'apparier différents modèles d'iris.

L'iris est le disque coloré de la partie antérieure de l'œil, ne change pas après l'adolescence. Il comprend de très nombreux motifs distinctifs qui permettent d'affirmer son unicité. La texture de l'iris, avec ses crêtes et ses sillons, peut être facilement encodée pour comparaison. C'est un des procédés les plus fiables, car la fraude est très difficile : une copie de l'iris, présentée devant un lecteur, serait immédiatement décelée en raison de l'absence d'oscillation du diamètre de la pupille[Marc 14], mais la fraude étant néanmoins possible en utilisant des lentilles. L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Elle est très sensible (précision, reflet) et relativement désagréable pour l'utilisateur car il doit être éclairée par une source lumineuse pour assurer un contraste correct.

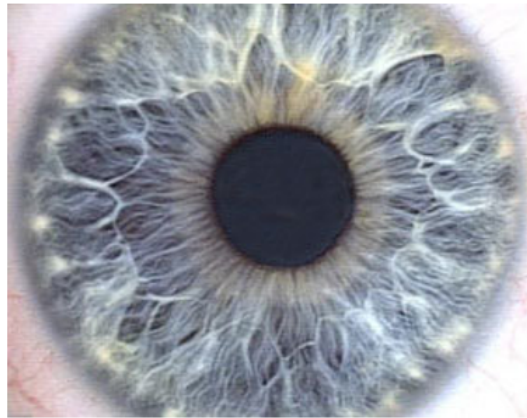


FIGURE 1.4.3 – L'iris [zakaria 14]

Avantages et inconvénients :

Avantages	Inconvénients
-Grande quantité d'information contenue dans l'iris. -Vrais jumeaux non confondus	-L'iris est aisément visible et peut être photographié. -mal acceptée par les utilisateurs.

1.4.1.4 La rétine :

Le balayage rétinien est une technique biométrique primaire développée au début pour le contrôle d'accès dans les environnements militaires. C'est l'un des modes d'identification les plus précis. On appelle La rétine la membrane tapissant le fond de l'œil, la carte rétinienne est tapissée de très nombreux vaisseaux sanguins [Amina 16]. La grande variété de configurations de ces vaisseaux présente la même diversité que les empreintes digitales. L'aspect des vaisseaux peut être modifié par l'âge ou la maladie, mais la position respective des vaisseaux reste inchangée durant toute la vie de l'individu.

Elle est mise en évidence par éclairage, obligeant la personne à placer son œil très près du capteur, ce qui n'est pas le cas pour l'iris [Fouad 18].

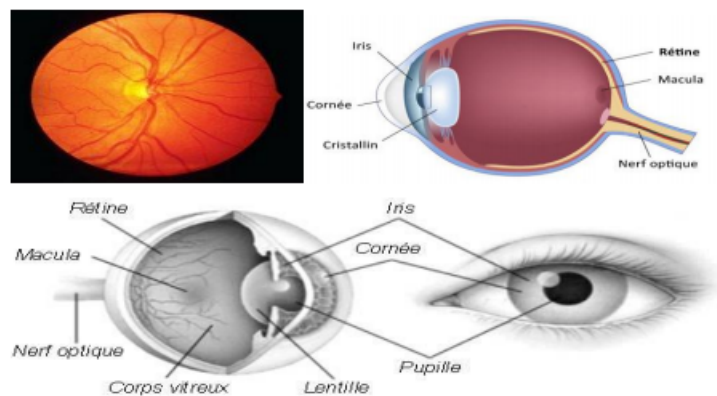


FIGURE 1.4.4 – la rétine[Fouad 18]

Avantages et inconvénients :

Avantages	Inconvénients
-L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure). -Les taux de faux rejets et de fausse acceptations sont faibles. - stable durant la vie d'un individu. - très efficace. -Carte vasculaire propre à chaque individu et différente, même entre jumeaux. - Haute sécurité.	-Système intrusif, il faut placer l'œil près du capteur et mauvaise acceptation du public. -Coût plus important que d'autres technologies -Pas adapté pour un flux de passage important -L'aspect des vaisseaux sanguins peut être modifié par la maladie ou l'âge.

1.4.1.5 Le visage :

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 avances 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[Amina 16]. Les images faciales sont probablement la caractéristique biométrique la plus communément employée par l'homme pour effectuer une identification personnelle.

La reconnaissance faciale possède plusieurs avantages sur les autres technologies biométriques puisque elle est naturelle, non intrusive et facile à utiliser. Idéalement, un système de reconnaissance faciale doit pouvoir identifier des visages présents

dans une image ou une vidéo de manière automatique selon deux modes : authentification ou identification ; on peut également noter qu'il existe un autre type de scénario de reconnaissance faciale mettant en jeu une vérification sur une liste de surveillance ("watch-list"), où un individu est comparé à une liste restreinte de suspects. Le principe de fonctionnement de base d'un système de reconnaissance faciale peut être résumé en quatre étapes : les deux premières s'effectuent en amont du système (détection et normalisation du visage [Sofiane 12]) et les deux dernières représentent la reconnaissance (extraction et comparaison des caractéristiques).



FIGURE 1.4.5 – Reconnaissance du visage

Avantages et inconvénients :

Avantages	Inconvénients
-Très bien accepté par le public. - Seule une opération chirurgicale modifiant la forme du visage peut affecter la fiabilité. -Seule technique utilisable sans le consentement de la personne. - utilisation facile et peu coûteuse.	- Ne permet pas d'identifier des personnes en mouvement. - Les vrais jumeaux ne sont pas différenciés. -Technologie sensible aux variables d'environnement (éclairage, pose, ...)

1.4.2 Les modalités comportementale :

Elle se base sur l'analyse de certains comportements d'une personne. Cette catégorie regroupe la reconnaissance vocale, la dynamique de frappe au clavier, la dynamique de la signature, l'analyse de la démarche, etc .

Parmi les mesures comportementales les plus répandues on cite :

1.4.2.1 La reconnaissance vocale :

Chaque personne possède une voix propre caractérisée par une fréquence, une intensité et une tonalité et que l'on peut analyser par enregistrement avec un microphone. Même si deux voix peuvent sembler similaires pour l'oreille, le traitement informatique permet de les isoler.

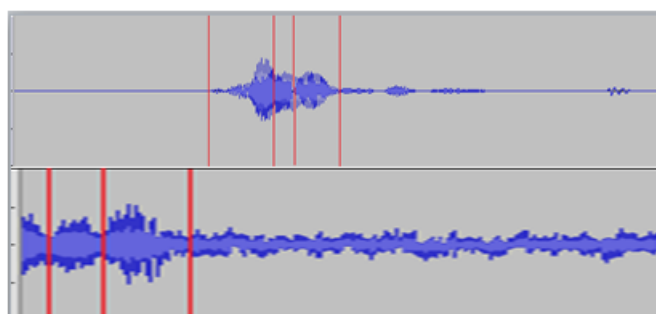


FIGURE 1.4.6 – Spectre d'un signal de voix[Douib 16]

Avantages et Inconvénient :

Avantages	Inconvénients
-Technologie biométrique facile à mettre en œuvre et sécurisé. -Généralement très bien acceptée car la voix est un signal naturel à produire. - Une des seules techniques permettant de reconnaître quelqu'un à distance. -impossible d'imiter la voix.	- Technologie biométrique vulnérable aux attaques. - Nécessite une excellente qualité audio. -Sensible aux bruits ambiants. -La voix change dans le temps et peut être altérée (rhume, forte émotion, etc.).

1.4.2.2 La signature :

C'est une technique peu répandue, et peu de constructeurs la proposent. La vérification dynamique de signature est basée sur la différentiation entre les parties d'une signature qui sont habituelles et celles qui changent avec presque chaque signature [Amina 16]. Les systèmes d'authentification de signature incluent habituellement un crayon lecteur et une tablette à digitaliser électronique .

Les systèmes de reconnaissance de l'écriture s'appuient sur l'analysent des caractéristiques spécifiques d'une signature comme la vitesse, la pression sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé.



FIGURE 1.4.7 – La signature[Amina 16]

Avantages et inconvénient :

Avantages	Inconvénients
- Bien acceptée comme moyen d'identification. - Couramment utilisée pour les transactions.	- dépend de l'état physique de la personne. - Non utilisable pour des contrôles d'accès en extérieur. - Sensible à l'état émotionnel de l'individu. - Besoin d'une tablette graphique.

1.4.2.3 La dynamique de frappe au clavier :

Il s'agit d'une technique de reconnaissance des personnes basée sur le rythme de frappe qui leur est propre. C'est une solution biométrique « Software Only » , car Le système est basé sur la dynamique de frappe au clavier, il ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier[Amina 16]. Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ 1000 fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin que soit constitué un gabarit de référence [Ibtissam 16].

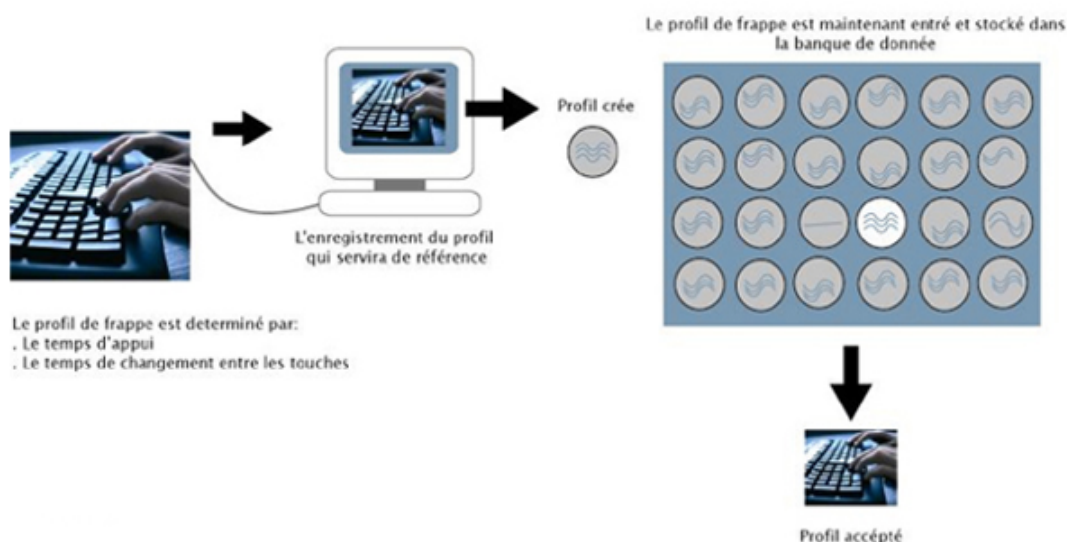


FIGURE 1.4.8 – La dynamique de frappe au clavier[Céline 13]

Avantages et inconvénients :

Avantages	Inconvénients
-Non intrusif (geste naturel pour un individu).	-Dépend de l'état de la personne (physique, émotionnel...)

1.4.2.4 Analyse de la démarche :

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (en fonction de sa vitesse, son accélération, mouvements du corps...), en analysant des séquences d'images [S. Shigematsu 99]. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle, mais des vêtements amples, par exemple, peuvent compromettre une bonne identification . Les paramètres communs de l'analyse de la marche sont [Fouad 18] :

- Paramètres cinématiques tels que le genou, les mouvements de la cheville et les angles
- Paramètres spatiotemporels tels que la longueur et la largeur des marches, la vitesse de marche .

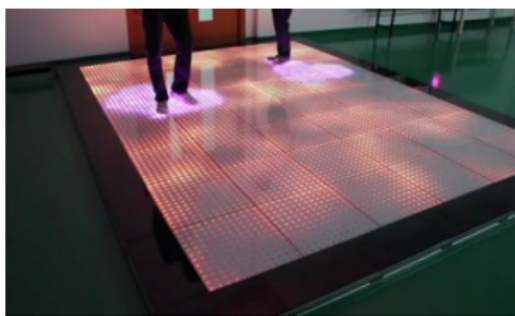


FIGURE 1.4.9 – La démarche

1.4.3 Les modalités biologiques :

Ce type de biométrie est basé sur l'identification de traits biologiques particuliers pour chaque individu à l'aide de son ADN, de son sang, ou de sa salive...

1.4.3.1 L'ADN :

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification c'est la marque biologique la plus sûre du monde. Dans le cas des tests de paternité, on atteint une fiabilité de 99,999%.

Cette technologie est issue directement de l'évolution de la biologie moléculaire [Amina 16]. Elle est devenue en quelques années l'un des outils majeurs de la criminalistique, la science de l'identification des indices matériels. Elle est couramment utilisée en criminologie pour identifier une personne à partir d'un morceau de peau d'un cheveu ou d'une goutte de sang. Mais l'inconvénient de cette analyse réside dans le fait qu'elle nécessite des délais de plusieurs semaines, ce qui interdit toutes les applications d'identification en temps réel [Fouad 18].



FIGURE 1.4.10 – l'ADN

Avantages et inconvénients :

Avantages	Inconvénients
-Une Très grande précision. -Il impossible que le système fait des erreurs. -Il est standardisé	-Très cher

1.4.3.2 Veines de la main :

On a longtemps considéré que le modèle des veines dans l'anatomie humaine peut être unique aux individus. Le sang chargé en oxygène arrive dans les mains par les artères, puis repart vers le cœur par les veines [Romain 12]. Le sang appauvri en oxygène n'a pas le même filtre d'absorption que le sang artériel : il absorbe la lumière à des longueurs d'onde proches de l'infrarouge (autour de 760 micromètres).

Quand la main est éclairée avec une lumière infrarouge, le réseau veineux apparaît en noir[Romain 12]. Il est enregistré sous forme de "carte d'identité" dans une base de données, et pourra ensuite servir de comparaison lors de l'authentification.



FIGURE 1.4.11 – Veines de la main

Avantages et Inconvénients

Avantages	Inconvénients
-Très haut niveau de sécurité, à ce jour aucun moyen de frauder. -biométrie dite "sans trace". -TFA « taux de fausses acceptations » (personnes authentifiées comme quelqu'un d'autre) est $< 0,0001\%$. -Biométrie sans badge et sans code.	-Utilisation uniquement en intérieur. -Capteur sensible à la lumière, toutefois les constructeurs ont apporté des protections limitant le problème. -La bonne identification de l'utilisateur implique de poser correctement la main sur le capteur. -L'utilisateur doit être volontaire pour appliquer sa main correctement.

1.4.3.3 Odeur corporelle :

Chaque personne dégage une odeur qui lui est particulière. Les systèmes biométriques qui exploitent cette technologie analysent les composantes chimiques contenues dans l'odeur pour ensuite les transformer en données comparatives [Ibtissam 16].

L'identification humaine à partir de l'odeur corporelle n'est pas nouvelle. Les polices s'en servent depuis plus d'un siècle. Et avec les moyens techniques dont nous disposons aujourd'hui des chercheurs de l'université polytechnique de Madrid ont franchi une étape importante en démontrant que l'identification d'un individu à partir de son odeur est scientifiquement réalisable en se servant de l'apprentissage automatique, ils sont parvenus à élaborer un système biométrique basé sur l'odeur corporelle [Marc 14], il s'agit d'un capteur utilisant la spectrométrie de masse, ils ont pu identifier 13 personnes à partir de l'odeur de leurs mains avec un taux de réussite de 85 %.

1.4.3.4 d. La reconnaissance de la thermographie :

Une caméra thermique est utilisée pour réaliser un cliché infrarouge du visage. Cela permet de faire apparaître une répartition de la chaleur unique à chaque individu qui dépend de plusieurs facteurs comme la localisation des veines, de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc, voire de cartographier le réseau veineux du visage invisible à l'œil nu [Amina 16].

L'avantage de cette technique est que l'on peut distinguer de vrais jumeaux, et contrairement à la reconnaissance faciale, on peut l'utiliser même dans l'obscurité ou de mauvaises conditions de visibilité [Mohamed 07]. Mais les conditions de prise de vue peuvent conduire à des erreurs. Ce système reste expérimental et très cher.

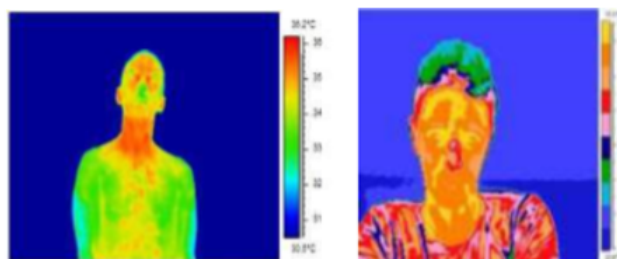


FIGURE 1.4.12 – La thermographie faciale

1.4.4 Les multimodalités :

Face aux nombreuses limitations imposées par l'utilisation des systèmes biométriques unimodaux, la biométrie multimodale s'impose de manière indéniable comme une alternative d'avenir dans le domaine de la sécurité des personnes et leurs biens. Bien que le couplage des systèmes biométriques peut être effectué à différents niveaux, la fusion au niveau des scores est la plus courante puisqu'elle a été généralement prouvée plus efficace que le reste des niveaux de fusion [Ibtissam 16]. La combinaison de plusieurs systèmes biométriques donne naissance à ce qu'on appelle la multimodalité biométrique. Elle apporte plusieurs avantages permettant de réduire certaines limitations des systèmes biométriques, comme l'impossibilité d'acquérir les données de certaines personnes ou la fraude intentionnelle, tout en améliorant les performances de reconnaissance.

1.5 Caractéristiques des modalités biométriques

Bien que n'importe quelle mesure physiologique ou comportementale puisse être utilisée dans un système de reconnaissance biométrique, elles ne sont pas toutes aussi performantes les unes que les autres. Ainsi, toute bonne mesure biométrique doit satisfaire les critères suivants [Bettahar Abdessettar 14] :

Universelle : Par ceci, nous voulons dire que la caractéristique biométrique doit être présente pour tous les individus.

Distinctive : La mesure effectuée sur un individu doit être suffisamment différente de celles effectuées sur les autres individus pour permettre de discriminer entre eux. Comme le code génétique qui varie significativement d'une personne à l'autre tandis que la taille est une mesure que plusieurs individus partagent.

Permanente : puisque le corps humain vieillit un certain laps de temps, donc une mesure biométrique faite sur un individu peut être très différente de la mesure initiale utilisée pour l'inscription dans le système, d'où la nécessité de choisir une caractéristique biométrique qui reste stable durant la vie de l'individu. Le motif

présent dans l'iris ou même le code génétique de l'individu présente un bon exemple pour ceci.

Facile à mesurer : Ceci représente la facilité de recueillir et de quantifier la mesure biométrique. Il est facile d'enregistrer le son de la voix d'un individu à l'aide d'un microphone, mais il est beaucoup moins facile d'obtenir une image de bonne qualité de la rétine des individus.

Efficace : L'efficacité fait référence à la quantité de ressources nécessaires afin d'obtenir le niveau de qualité désiré dans le temps requis.

Acceptable : c'est le fait qu'elle soit acceptable culturellement par les utilisateurs [Ahmed 15] même si avec la surabondance de caméras de sécurité, la population normale ne se soucie plus d'avoir son image recueillie par de multiples systèmes.

Robuste : la robustesse ici fait référence à la difficulté de forcer le système à produire une prédiction erronée par l'utilisation d'une technique frauduleuse c'est-à-dire qu'il est difficilement falsifiable [Ahmed 15].

Le tableau ci-dessus montre une comparaison des modalités biométriques principales selon les propriétés suivantes :

Universalité(U), Unicité(N), Permanence(P), Mesurabilité(M), Performance(F), Acceptabilité(A), Circonvention(C)

Biométrie	U	N	P	M	F	A	C
ADN	Haute	Haute	Faible	Faible	Haute	Faible	Faible
Visage	Haute	Faible	Moyenne	Haute	Faible	Haute	Haute
Thermo Visage	Haute	Haute	Faible	Haute	Moyenne	Haute	Haute
Empreinte	Moyenne	Haute	Haute	Moyenne	Haute	Moyenne	Moyenne
Démarche	Moyenne	Faible	Faible	Haute	Faible	Haute	Moyenne
Géométrie main	Moyenne	Moyenne	Moyenne	Haute	Moyenne	Moyenne	Moyenne
Veines mains	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Moyenne	Faible
Iris	Haute	Haute	Haute	Moyenne	Faible	Moyenne	Moyenne
Frappe clavier	Faible	Faible	Faible	Moyenne	Faible	Moyenne	Moyenne
Odeur	Haute	Haute	Haute	Faible	Faible	Moyenne	Faible
Rétine	Haute	Haute	Moyenne	Faible	Haute	Faible	Faible
Signature	Faible	Faible	Faible	Haute	Faible	Haute	Haute
Voix	Moyenne	Faible	Faible	Moyenne	Faible	Haute	Haute

TABLE 1.1 – Comparaison entre les techniques biométriques [Hanane 12].

1.6 Domaine d'application de la biométrie

Dans notre société mondialisée interconnectée, l'établissement et la détermination des identités des personnes avec un haut degré de confiance devient capital et crucial [Jain 08]. De plus, le progrès rapide que les réseaux et les moyens de communication et transport nécessite au fur et à mesure la mise en place des systèmes de gestion d'identités concurrents aussi fiables pour diminuer les inquiétudes autour de ceux-ci. Tout cela incite le cadre biométrique, qui à son tour, possède un pouvoir et un savoir répondre à plusieurs interrogations et questions paralysant les systèmes de gestion d'identité traditionnels [Day 09]. En conséquence, la biométrie a pu pénétrer de plus amples scénarios faisant appel à de nombreuses applications dont il convient de distinguer trois classes :

1.6.1 Les applications commerciales :

Ces applications couvrent le contrôle d'accès logique tels-que l'accès aux ordinateurs et aux réseaux informatiques, le contrôle d'accès physique aux endroits de haute sensibilité, la gestion de ponctualité des employés [Day 09]. On trouve aussi de diverses applications telles que : le commerce électronique et la vente au détail, la téléphonie mobile, l'enseignement à distance, la gestion et la maintenance dans les services de santé et le suivi des patients ... etc.

1.6.2 Les applications gouvernementales :

Ces applications comprennent les projets des cartes d'identité nationales, les permis de conduire, la surveillance des frontières, le contrôle des passeports [Lazarick 08], et tous les autres projets gouvernementaux au cours d'étude qui ont en besoin de construction dans les différents pays du monde couvrant en général l'identification individuelle, la sécurité sociale, et le suivi des cibles.

1.6.3 Les applications judiciaires :

Ces applications incluent l'identification des cadavres, l'enquête criminelle, la détermination de la paternité, l'identification des terroristes, et le contrôle des prisonniers ... etc.

1.7 Les avantages et les limites de la biométrie

1.7.1 Les avantages de la biométrie

La biométrie est une technologie récente et commence à être adoptée par de grands constructeurs de matériel informatique. L'usage de la biométrie est un complément de l'utilisation des méthodes d'authentification comme des mots de passe, des badges, des cartes à puce [Ibtissam 16].

— Suppression des mots de passe, Suppressions des clés :

Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur.

— Utilisation d'une signature biométrique :

Grande sécurité, intransmissible à une autre personne. Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données). Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr. La biométrie offre le chaînon manquant dans la triade du problème de sécurité :

- Diminution de la fraude.
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.
- Diminution des frais administratifs.
- Accélération des services.

Puisque la biométrie fait appel à ce que l'on est, elle comporte un avantage primordial sur les méthodes traditionnelles, dans le sens où elle évite l'usage d'un grand nombre de mots de passe complexe, de badges, etc. Le tableau 1.2 présente un parallèle entre la biométrie et les méthodes d'authentification traditionnelles[Deluzarche 06]. Ce tableau montre que les systèmes biométriques facilitent le processus d'authentification et résiste aux différentes attaques existantes sur les systèmes basés sur un secret ou une possession. Cependant, ces systèmes présentent plusieurs inconvénients concernant le respect de la vie privée et l'incertitude de l'information biométrique. Une comparaison de ces techniques est détaillée ici :

Authentification biométrique	Authentification par mot de passe/clé
-basée sur des mesures morphologiques, comportementales ou biologiques. -utilisation facile. -authentifie l'individu. -l'information est en relation étroite à l'utilisateur de façon permanente. -utilise une comparaison probabiliste. -l'information biométrique peut être modifiée et/ou altérée avec le temps, il est incertain. -problème de respect de la vie privée. -difficile de révoquer l'information.	-basée sur que l'on sait ou possède. -pouvant être plus compliquée (mots de passe complexe). -authentifie la clé. -il peut être perdu, volé ou oublié -utilise une comparaison exacte -l'information ne varie pas, elle est sûre. -moindre impact sur la vie privée. -changement aisé.

TABLE 1.2 – Comparaison entre l'authentification biométrique et par mot de passe clé

1.7.2 Les limites de la biométrie

La biométrie présente malheureusement un certain nombre d'inconvénients parmi eux : le problème de la qualité de l'authentification. Ces méthodes ne sont en effet pas toujours fiables à 100%, ce qui empêche des utilisateurs de bonne foi d'accéder à leur système [Ibtissam 16]. Car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, donc on évolue et les mesures changent .

— **Les limites fonctionnelles :**

Les systèmes d'authentification biométrique représentent une grande partie des limites fonctionnelles [Ibtissam 16]. En effet, les systèmes biométriques laissent la place à un certain nombre de faux rejets et de fausses acceptations. Ils ne peuvent à eux seuls garantir à 100% que seules les personnes autorisées pourront passer le contrôle. Ils ne peuvent même pas garantir qu'une personne autorisée ne sera pas rejetée par le système. Il y aura toujours une marge d'erreur à prendre en compte, ce qui n'est pas forcément très rassurant.

— **Les limites techniques :**

Bien que cela représente un travail assez conséquent, les données biométriques peuvent être imitées, notamment celles qui laissent des traces sur le passage de l'individu telles que les empreintes digitales [Ibtissam 16]. Un individu mal intentionné peut récupérer les empreintes digitales sur un objet tenu par la victime, les imiter et tenter de passer le contrôle biométrique à l'aide de ces empreintes. De plus, les données biométriques sont dans la majeure partie des cas numérisées sur un support, de préférence individuel. Si ce support n'est pas protégé contre les intrusions et le piratage, tout le système biométrique tombe à l'eau.

1.8 Le marché de la biométrie :

1.8.1 Présentation du marché :

Selon un rapport publié par TMR¹, le marché mondial des technologies biométriques devrait atteindre 23,3 milliards de dollars d'ici la fin 2019, avec un TCAC² de 20,8% entre 2013 et 2019 [Stephen 14]. Le rapport note que la sécurité de haut niveau est plus nécessaire que jamais, en raison des préoccupations croissantes suscitées par l'augmentation des attaques terroristes et des crimes.

Les récentes initiatives gouvernementales telles que le passeport électronique, les programmes d'identification nationaux, ainsi que divers projets de contrôle des frontières tels que la dactyloscopie européenne, les systèmes d'information sur les visas et le système d'information nouvelle génération Schengen peuvent expliquer la croissance rapide du marché des technologies biométriques.

Toutefois, à l'inverse, selon le rapport, les préoccupations constantes en matière de protection de la vie privée et les coûts élevés associés à la biométrie pourraient potentiellement ralentir la croissance de ce marché.

Le rapport montre également que l'utilisation croissante de la biométrie multimodale pour renforcer le niveau de sécurité ouvrira probablement de nouvelles perspectives de croissance pour ce marché dans les années à venir.

1. TMR : Transparency Market Research

2. TCAC : Taux de croissance annuel composé

En ce qui concerne le type d'application, les systèmes biométriques non-AFIS représentaient la plus grande part de chiffre d'affaires, avec 41,40% du marché total de la technologie biométrique en 2012. Parallèlement, les récents progrès technologiques ont entraîné une baisse considérable du prix des capteurs au silicium utilisés pour la reconnaissance des empreintes digitales [Stephen 14]. Ces progrès ont rendu les capteurs plus efficaces, ce qui a entraîné une réduction des coûts de production et une extension de leur application à une gamme plus étendue d'appareils.

Cela a également permis aux systèmes autres que AFIS³ de devenir plus rentables que leurs prédécesseurs en raison de leur convivialité et de leur intégration avec les téléphones intelligents et les ordinateurs portables. Le segment de reconnaissance de l'iris devrait également progresser à un TCAC de 28,6% d'ici la fin 2019, en raison de sa grande précision et de sa stabilité [Stephen 14]. En ce qui concerne l'utilisation finale, les secteurs des transports, visas, logistiques et de l'administration représentaient ensemble plus de 50% du marché total des technologies biométriques en 2012, en raison de la nécessité croissante d'examiner les informations d'identité du voyageur. Ces derniers continueront de dominer les autres segments d'utilisation finale d'ici la fin 2019.

La popularité croissante des services bancaires par Internet pour les transactions a entraîné le déploiement de la technologie biométrique dans les secteurs bancaire et financier. Le segment d'utilisation finale devrait croître au TCAC le plus élevé au cours de la période de prévision .

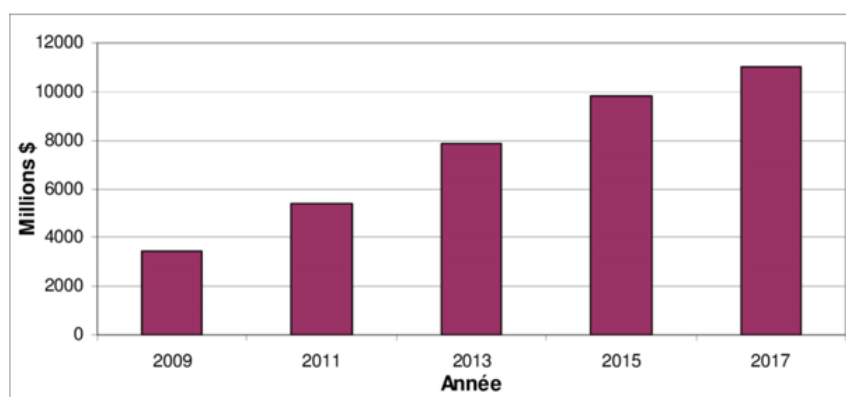


FIGURE 1.8.1 – Perspectives des revenus du marché mondial de la biométrie [Stephen 14]

3. AFIS : Automated Fingerprint Identification System (système d'identification automatique par empreinte digitale)

1.8.2 La part du marché par technologie :

Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, plus de 30% du chiffre d'affaires total (hors applications judiciaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de sources de revenus après les empreintes digitales.

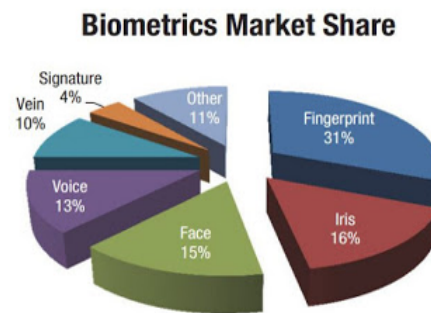


FIGURE 1.8.2 – Parts de marché des différentes méthodes biométrique

1.9 Conclusion

Dans ce chapitre nous avons décrit les technologies utilisées dans les systèmes biométriques pour l'identification des personnes, leurs architectures et leurs différentes applications, ainsi nous avons donné un aperçu sur les techniques de mesure des performances des systèmes biométriques en montrant les différentes modalités biométriques tout en soulignant les avantages et les inconvénients de chacune. Nous avons constaté aussi que les performances des systèmes biométriques dépendent de plusieurs facteurs et qu'elles varient d'un système à un autre.

Nous présentons dans le chapitre suivant un état de l'art sur la reconnaissance faciale.

Chapitre 2

Reconnaissance Automatique Du Visage

2.1 Introduction

En dépit de l'énorme progression en informatique et plus spécifiquement le traitement d'images, les systèmes appliquant les techniques de reconnaissance faciale sont considérés comme un gros «challenge» très intéressant, qui a attiré les chercheurs des différents domaines : psychologie, identification de modèles, réseaux de neurones, vision par ordinateur et infographie, ceci étant dû aux avances 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.

Certes que la reconnaissance des visages n'est pas la plus fiable comparée aux autres techniques biométriques, mais elle peut être ainsi si on utilise des approches plus efficaces en plus du bon choix des caractéristiques d'identification représentant le visage en question.

Dans ce chapitre nous expliquons pourquoi le visage, les systèmes de reconnaissance des visages, et aussi nous présenterons un état de l'art sur les techniques de reconnaissance faciale.

2.2 Pourquoi le visage ?

la reconnaissance automatique des visages est devenue un enjeu primordial, c'est la technique la plus courante et la plus fiable vu qu'elle est largement acceptable puisque elle répond à ce que les gens 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 coopé-

ration du sujet (en observant les individus à distance), et d'une autre part, la disponibilité des équipements d'acquisition, leurs simplicité et leurs coûts faibles (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)[Hanane 12]. Malgré que certains disent que la reconnaissance de visages est une biométrie relativement peu sûre, sur le fait que le changement de certains facteurs peut entraîner des erreurs, 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 pour palier à ces difficultés 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.

2.3 Systèmes de reconnaissance faciale

Le système de reconnaissance a pour rôle d'exploiter les caractéristiques du visage et les extraire pour créer une signature numérique qu'il stocke dans une base de données. Ainsi, à chaque visage de la base est associée une signature unique qui caractérise la personne correspondante. La reconnaissance d'un visage requête est obtenue par l'extraction de la signature requête correspondante et sa mise en correspondance avec la signature la plus proche dans la base de données. La reconnaissance dépend du mode de comparaison utilisé : vérification ou identification. On peut représenter les systèmes de reconnaissance par la figure suivant :

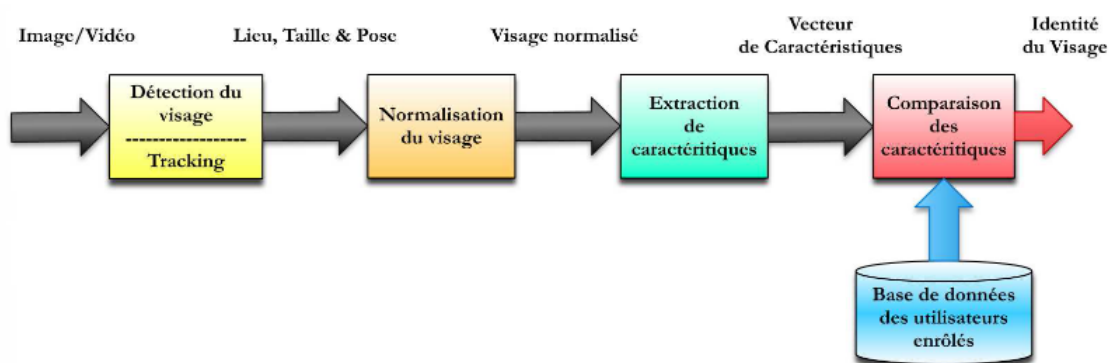


FIGURE 2.3.1 – Le processus de reconnaissance de visage[Serge 10].

2.3.1 Le monde physique

L'environnement peut avoir une influence sur l'acquisition de l'image. Cette influence peut être caractérisée par trois paramètres essentiels : L'éclairage, le changement de posture et l'échelle [Ahmed 15]. La variation de l'un de ces trois paramètres peut conduire à une distance entre deux images du même individu, supérieure à celle séparant deux images de deux individus différents, et par conséquent une fausse identification.

2.3.2 Acquisition

Cette étape consiste à extraire l'image de l'utilisateur du monde extérieur dans un état statique à l'aide d'un appareil photo ou dynamique à l'aide d'une caméra. Après, l'image extraite sera digitalisée ce qui donne lieu à une représentation bidimensionnelle au visage, caractérisée par une matrice de niveaux de gris [Bettahar Abdessettar 14]. L'image dans cette étape est dans un état brut ce qui engendre un risque de bruit qui peut dégrader les performances du système.

2.3.3 Détection de visage

Le module de détection de visages permet de fournir en sortie une image du visage isolé du reste de la scène et prête à être traitée [Ahmed 15]. L'efficacité des systèmes biométriques basés sur l'identification et/ou authentification de visage dépend essentiellement de la méthode utilisée pour localiser le visage dans l'image.

2.3.4 Les prétraitements

Le rôle de cette étape est d'éliminer les parasites causés par la qualité des dispositifs optiques ou électroniques lors de l'acquisition de l'image en entrée, dans le but de ne conserver que les informations essentielles et donc préparer l'image à l'étape suivante [Bettahar Abdessettar 14]. Elle est indispensable car on ne peut jamais avoir une image sans bruit à cause du background et de la lumière qui est généralement inconnue. Il existe plusieurs types de traitement et d'amélioration de la qualité de l'image, telle que : la normalisation, l'égalisation et le filtre médian. Cette étape peut également contenir la détection et la localisation du visage dans une image, surtout là où le décor est très complexe.

2.3.5 Extraction des paramètres

L'étape de l'extraction des paramètres représente le cœur du système de reconnaissance, son rôle consiste en l'extraction des informations nécessaires qui re-

viennent à établir un modèle du visage (vecteur de caractéristiques)[Bettahar Abdessettar 14]. ces information sont utiles pour différencier le visage de chaque personne par rapport aux autres mais au même temps pour qu'il ressemble a lui-même dans d'autres conditions d'acquisition.

2.3.6 L'apprentissage

C'est l'étape où on fait apprendre les individus au système, elle consiste à mémoriser les paramètres, après extraction, dans une base de données bien ordonnées [Ahmed 15] pour faciliter la phase de reconnaissance et la prise d'une décision, elle est en quelque sorte la mémoire du système.

2.3.7 La classification (Modélisation)

Cette étape consiste à modéliser les paramètres extraits d'un visage ou d'un ensemble de visages d'un individu en se basant sur leurs caractéristiques communes [Bettahar Abdessettar 14]. Un modèle est un ensemble d'informations utiles, discriminantes et non redondantes qui caractérise un ou plusieurs individus ayant des similarités .

2.3.8 La décision

C'est l'étape qui fait la différence entre un système d'identification d'individus et un autre de vérification[Bettahar Abdessettar 14]. Dans cette étape, un système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. Par contre, dans un système de vérification il s'agit de décider si le visage en entrée est bien celui de l'individu (modèle) proclamé ou il s'agit d'un imposteur, il est caractérisé par son EER (equal error rate).

2.4 Principales difficultés de la reconnaissance de visages

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables. Il existe deux types de variations associées aux images de visages : inter et intra sujet. La variation inter-sujet est limitée à cause de la ressemblance physique

entre les individus. Par contre la variation intra-sujet est plus vaste. Elle peut être attribuée à plusieurs facteurs que nous analysons ci-dessous.

2.4.1 Changement d'illumination

L'intensité et la direction d'éclairage lors de la prise de vue influent énormément sur l'apparence du visage dans l'image. En effet, dans la plupart des applications courante, des changements dans les conditions d'éclairage sont inévitables, notamment lorsque les vues sont collectées à des heures différentes, en intérieur ou en extérieur[Bouchra 13]. Etant donnée la forme spécifique d'un visage humain, ces variations d'éclairage peuvent y faire apparaître des ombres accentuant ou masquant certaines caractéristiques faciales.



FIGURE 2.4.1 – Exemple de variation d'éclairage[Bettahar Abdessettar 14]

2.4.2 Variation de pose

Les changements d'orientation et les changements de l'angle d'inclination du visage engendrent de nombreuses modifications d'apparence dans les images collectées et par conséquent le taux de reconnaissance de visage baisse. 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) [Bettahar Abdessettar 14]. Cependant, lorsque la rotation est supérieure à 30° , la normalisation géométrique n'est plus possible.



FIGURE 2.4.2 – Exemple de variation de pose[Bouchra 13].

2.4.3 Expression faciale

Un autre facteur qui affecte l'apparence du visage est l'expression faciale véhiculant des émotions, combinés avec les déformations induites par la parole, peuvent produire des changements d'apparence importants [C.Fredouille 06]. Ces déformations du visage sont localisées principalement sur la partie inférieure du visage. 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 [Estelle].



FIGURE 2.4.3 – Exemple de variation d'expressions.

2.4.4 Présence de composants structurels

Un visage peut être partiellement masqué par des objets ou par le port d'accessoires tels que lunettes, un chapeau, une écharpe. Les occultations peuvent être intentionnelles ou non mais elles peuvent modifier énormément les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance [Bouchra 13]. 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 complètement la forme du visage.

2.5 Etat de l'art des méthodes de reconnaissance de visage

La reconnaissance de visage est un axe de recherche ouvert et qui attire plusieurs chercheurs venant des disciplines différentes ; C'est ainsi que durant les 20 dernières années plusieurs méthodes d'identification de visage ont été proposées. Dans ce qui

suit, nous allons détailler les différentes techniques utilisées pour la reconnaissance de visage, à savoir les techniques 2D et 3D.

2.5.1 Techniques 2D de la reconnaissance de visage

Dans cette partie, nous présenterons les approches 2D de la reconnaissance de visage les plus connues. Ces dernières peuvent être subdivisées en trois catégories : les approches holistiques ou globales, les approches locales ainsi que les approches hybrides.

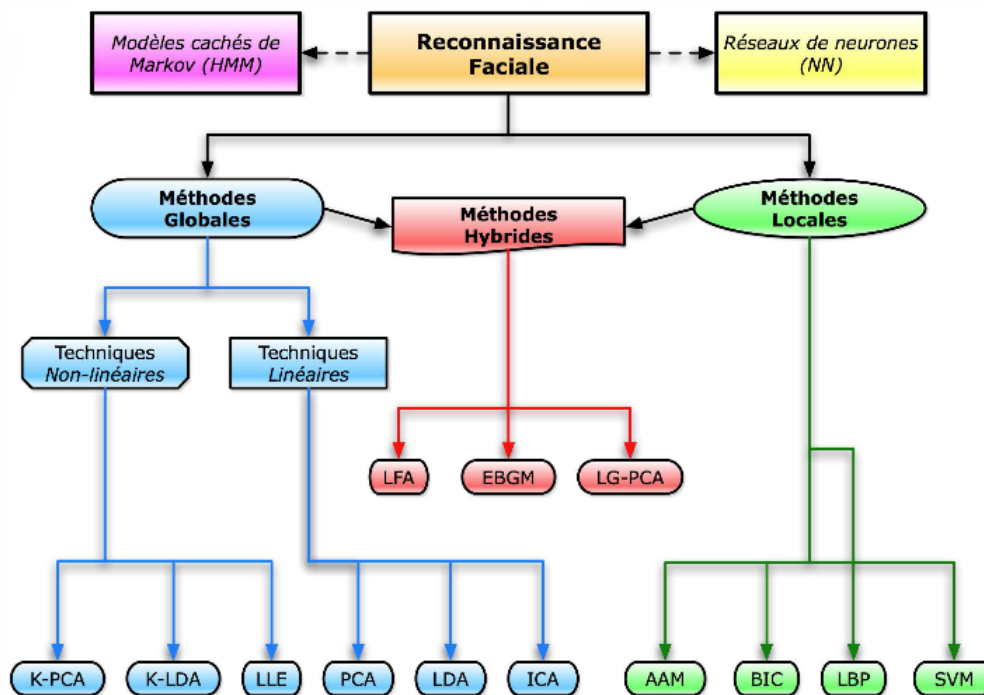


FIGURE 2.5.1 – Classification des algorithmes principaux utilisés en reconnaissance faciale[Nicolas 01]

2.5.1.1 Les méthodes globales

Les approches globales utilisent des techniques d'analyse statistique bien connues et elles les appliquent sur l'image du visage qu'elles prennent comme un tout [Bedia 12]. L'idée est généralement de projeter l'image d'entrée du visage, éventuellement vectorisée, dans un espace de plus faible dimension, où la reconnaissance est supposée être plus aisée. Pour différencier les personnes entre elles, la projection est souvent conçue pour ne sélectionner que les caractéristiques importantes et suffisamment discriminantes.

Une analyse de sous-espaces de visages est particulièrement utilisée par ces méthodes. Cette expression repose sur une expérience assez simple : une classe de "formes" qui nous intéresse (dans notre cas, les visages) réside dans un sous-espace de l'espace de l'image d'entrée [Bettahar Abdessettar 14]. Ainsi, la représentation de l'image originale est très redondante et la dimensionnalité de cette représentation pourrait être grandement réduite si l'on se concentre uniquement sur les formes qui nous intéressent. L'utilisation de techniques de modélisation de sous-espace a fait accélérer la technologie de reconnaissance faciale de manière significative.

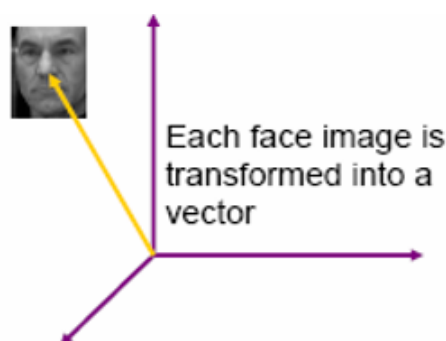


FIGURE 2.5.2 – le principe des méthodes globales.

Les méthodes globales ont plusieurs avantages et inconvénient, parmi les avantages on peut citer :

- Le problème de la reconnaissance faciale automatique est transformé en un problème d'analyse de sous-espaces de visages, pour lequel de nombreuses méthodes statistiques existent.
- Les méthodes globales sont souvent applicables à des images basses résolutions ou de mauvaises qualités.
- Les méthodes globales sont relativement rapides à mettre en œuvre et que les calculs de base sont d'une complexité moyenne.

Parmi les inconvénients on peut citer :

- Il est nécessaire de disposer de suffisamment de données représentatives des visages.
- Ces méthodes ne sont robustes qu'à des variations limitées (pose, illumination, expression).

Nous pouvons distinguer deux types de techniques parmi les méthodes globales, les techniques linéaires et les techniques non linéaires.

a. Techniques linéaires :

réalisent une projection linéaire des visages (espace dont la dimension est égale à la dimension des images, donc grande) sur un espace de plus faible dimension

[Bedia 12]. Cependant, ces techniques sont sensibles aux conditions de luminosité et aux variations de pose.

b. Techniques non linéaires :

L'utilisation de ces méthodes de projection de l'espace des images sur l'espace de caractéristiques est non linéaire et permet ainsi dans une certaine mesure de réduire la dimension des images de meilleure façon [Deluzarche 06]. Cependant, bien que ces méthodes permettent souvent l'amélioration des taux de reconnaissance sur des jeux de tests donnés, elles sont trop flexibles pour être robustes à de nouvelles données, contrairement aux méthodes linéaires.

Dans ce qui suit on détaillera les différentes méthodes globales les plus connus :

1. ACP : Analyse en Composant Principale (ou Eigen Faces)

L'ACP est une méthode permettant d'extraire efficacement de l'information au sein d'un jeu de données souvent complexe en abaissant la dimension de l'espace dans lequel ces données sont observées et en les arrangeant dans un nouvel espace d'une manière à mettre en évidence l'information utile et à éliminer celle qui est secondaire [Fiche 12].

L'algorithme ACP adapté à l'analyse et l'identification de visage est connu sous le nom d'EigenFaces (visages propres) et a été développé par M.A. Turk et A.P. Pentland en 1991. Il se divise en deux phases : l'apprentissage et la classification. Au cours de la phase d'apprentissage, un espace propre est construit à partir d'une base d'apprentissage en utilisant la méthode ACP puis ces mêmes images sont projetées sur l'espace ainsi obtenu [Fiche 12]. Durant la phase de classification, un visage test est projeté à son tour sur ce même espace pour être alors identifié en le comparant aux projections de chacun des visages de la base d'apprentissage. Cela revient à projeter les images sur une base orthogonale de vecteurs particuliers qui présentent les caractéristiques les plus indépendantes possible des visages (la redondance a donc été éliminée) pour mettre en évidence leurs différences. Rappelons que le principe de l'ACP repose sur une diminution de la redondance d'information, laquelle se traduit en terme mathématiques par la matrice de covariance. Si nous arrivons à diagonaliser cette matrice, alors les covariances (termes non diagonaux dans la matrice) sont toutes nulles .

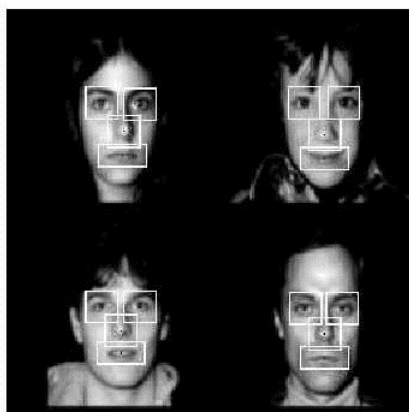


FIGURE 2.5.3 – Caractéristiques autour desquelles est réalisée une ACP

2. LDA : Analyse Discriminante Linéaire

- L'algorithme LDA est né des travaux de Belhumeur et al. De Yale University (USA), en 1997 [K. Etemad 97]. Il est aussi connu sous le nom de « Fisherfaces ». Contrairement à l'algorithme PCA, celui de la LDA effectue une véritable séparation de classes. Pour pouvoir l'utiliser, il est nécessaire d'orchestrer la base d'apprentissage d'images en plusieurs classes : une classe par personne et plusieurs images par classe. La LDA se base sur l'analyse des vecteurs propres de la matrice de dispersion des données, afin de maximiser les variations entre les images d'individus différents (interclasses) tout en minimisant les variations entre les images d'un même individu (intra-classes). Cependant, lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, une difficulté d'application de la LDA se pose, elle peut alors faire apparaître des matrices de dispersions singulières (non inversibles). Contrairement à l'ACP qui ne prend pas en compte la discrimination des classes, la LDA résout ce problème.
- les méthodes basées sur LDA standard telles que Fisherfaces, appliquent en premier lieu l'ACP pour la réduction de dimension et puis l'analyse discriminante [K. Etemad 97]. Des questions appropriées au sujet de l'ACP sont habituellement liées au nombre des composantes principales (CP) utilisées et comment elles affectent la performance. Concernant l'analyse discriminante on doit comprendre les raisons de sur-ajustage de précision et comment l'éviter. Les réponses à ces deux questions sont étroitement liées. On peut réellement montrer qu'employer plus de CP peut mener à la diminution de la performance de l'authentification. L'explication de ce comportement est que les CP correspondantes aux vecteurs qui ont des petites valeurs propres correspondent aux composantes de hautes fréquences codent habituellement le bruit. En résulte, si les vecteurs propres correspondant aux petites valeurs

propres sont employés pour définir le sous-espace réduit de PCA, le procédé FLD s'accompagne aussi bien par le bruit et par conséquent le sur-ajustage de précision a lieu. Pour cette raison le modèle amélioré du FLD (Enhanced FLD Model : EFM) est employé pour surmonter ces problèmes liés au sur-ajustage de précision, montré en détail ci-dessous.

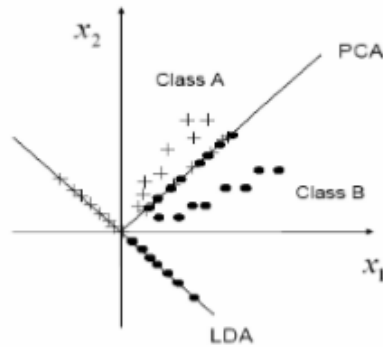


FIGURE 2.5.4 – les projections ACP et LDA d'un ensemble de données.

2.5.1.2 Les méthodes locales

Les méthodes locales utilisent les caractéristiques faciales locales pour la reconnaissance de visage (coins des yeux, de la bouche, le nez, ...), Elles sont relativement matures comparées aux méthodes holistiques [Bouchra 13]. Dans ces méthodes, le visage est représenté par un ensemble de vecteurs caractéristiques de dimensions faibles, plutôt que par un seul vecteur de grande dimension. Les méthodes locales ont plusieurs avantages et inconvénients, parmi les avantages on peut citer :

- Le modèle créé possède des relations intrinsèques bien définies avec les visages réels.
- Les modèles créés peuvent prendre en compte explicitement les variations telles que la pose, l'illumination ou les expressions. La reconnaissance est ainsi plus efficace dans le cas de fortes variations.
- La connaissance a priori sur les visages peut être intégrée aux modèles afin d'améliorer leur efficacité.

Parmi les inconvénients on peut citer :

- La construction du modèle, reposant souvent sur la détection de points caractéristiques faciaux, peut être laborieuse.
- L'extraction des points caractéristiques peut être difficile dans le cas de variations de pose, d'illumination, d'occlusion . . .
- Les images doivent être relativement de bonne qualité, et/ou être de résolution suffisante afin de pouvoir extraire les points caractéristiques.

Les méthodes locales peuvent être classées en deux catégories, les méthodes basées sur les points d'intérêt et celles basées sur l'apparence du visage.

a. Méthodes locales basées sur les points d'intérêts

On détecte tout d'abord les points d'intérêts et ensuite on extrait des caractéristiques localisées sur ces points d'intérêt. Les méthodes les plus anciennes en reconnaissance de visages appartiennent à cette catégorie [Kanade 73]. Elles s'appuient toutes sur l'extraction de caractéristiques géométriques spécifiques telles que la largeur de la tête, les distances entre les yeux,... etc. Ces données sont ensuite utilisées par des classificateurs afin de reconnaître des individus. Ces méthodes présentent les deux inconvénients suivants :

- les caractéristiques géométriques sont difficiles à extraire dans certains cas puisque la tâche de la détection précise des points caractéristiques n'est pas facile, en particulier dans les cas où des occultations ou des variations (pose, expression) de visages sont présentes.
- les caractéristiques géométriques seules ne sont pas suffisantes pour représenter réellement un visage, alors que d'autres informations utiles telles que les valeurs des niveaux de gris de l'image sont complètement écartés.

b. Les méthodes locales basées sur l'apparence du visage

Dans les méthodes locales basées sur l'apparence du visage, on divise le visage en petites régions. Généralement cette méthode basée sur des techniques d'analyse statistiques (pourcentage d'existence des modèles dans l'image) et d'apprentissage automatique pour trouver des caractéristiques significatives des visages et des non visages.

— Quelques méthodes locales :

Parmi ces méthodes locales les plus populaires nous citons :

1. Les Modèles de Markov Cachés (MMC)

Utilisés dans plusieurs domaines tels que : la reconnaissance de formes, l'intelligence artificielle ou encore le traitement automatique du langage naturel. Les modèles de Markov cachés (HMMs) sont généralement employés pour la modélisation statistique de séries de vecteurs de temps non stationnaires. En considérant l'information du visage comme étant une séquence variable dans le temps, le MMC (en anglais Hidden Markov Modal, HMM) peut être appliqué à la reconnaissance des visages [Marc 14]. Les caractéristiques faciales significatives (les cheveux, le front, les yeux, le nez et la bouche) se présentent dans une image du visage dans un ordre naturel de haut en bas. En se basant sur cette observation, l'image d'un visage peut être modélisée en utilisant un HMM unidimensionnel en assignant à chacune de ses régions un état. L'approche HMM a des performances de reconnaissance satisfaisantes, cependant elle nécessite des calculs intenses ce qui augmente le temps d'exécution [R.Djourani 06].

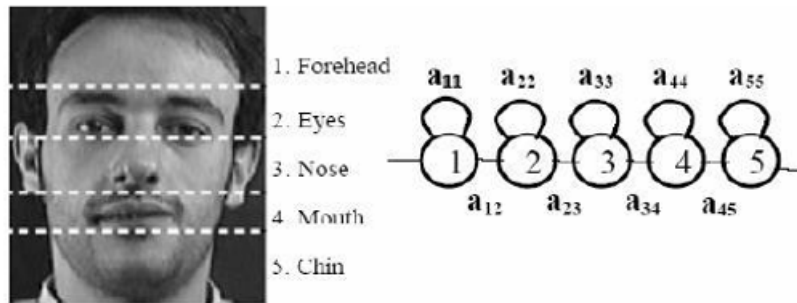


FIGURE 2.5.5 – Les 5 états d'un HMM (de haut en bas) [R.Djourani 06].

2. Les réseaux de neurones (RNA)

L'unité de base du réseau de neurones est le perceptron. Chaque perceptron effectue un travail relativement simple : il reçoit des données pondérées des voisins ou des sources externes et calcule sur cette base un signal de sortie qui est propagé à d'autres unités [Vermont 05]. On distingue entre unité d'entrée, de sortie et cachée. Un réseau de neurones doit être configuré pour que l'application d'un ensemble de données d'entrées produise le résultat désiré à la sortie. Les RNA (Réseaux Neurone Artificiel) ont été utilisés dans nombreuses applications, particulièrement pour la classification de données, la modélisation de processus complexes et le traitement non linéaire des signaux. Ces recherches ont engendré une panoplie d'architectures de réseaux dont chacune répond parfaitement à une application donnée. Dans le cas de la reconnaissance des visages, on constate que les réseaux de neurones ont été employés dans tous les modules intervenant dans la chaîne de traitements. Ils sont utilisés pour la détection de visages, pour l'extraction de signatures et pour

la classification.

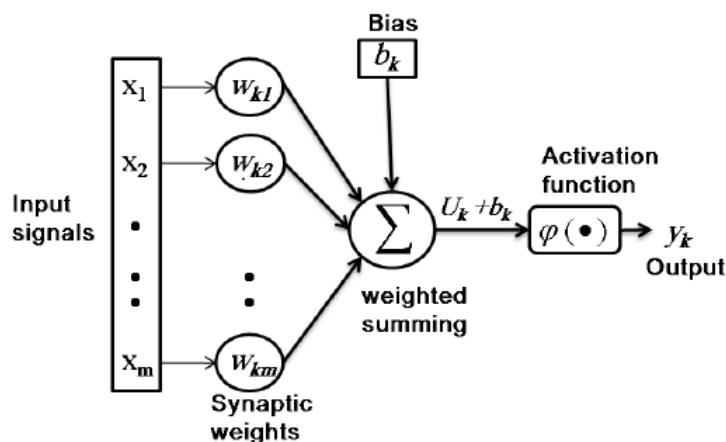


FIGURE 2.5.6 – Représentation de neurone formel

3. Local Binary Pattern (LBP)

L'opérateur LBP a été initialement proposé par T. Ojala et al [Stephen 14] en 1996 afin d'exprimer la texture des patches de l'image. Il a été largement appliqué avec divers algorithmes de systèmes de reconnaissance de visage comme une méthode d'extraction de caractéristiques locales [Y. Baohua 12]. L'opérateur LBP de base attribue à chaque pixel un motif binaire. Le LBP d'une image de pixel est produit par le seuillage du voisinage 3×3 avec le pixel central (si la valeur du pixel central était supérieure à la valeur du son pixel voisin ou non) et le transfert comme un code binaire qui est converti en un nombre décimal. Après cela, cet opérateur a été étendu pour utiliser de différents rayons de voisinages et différents points d'échantillonnage ce qui permet d'extraire les caractéristiques dans différentes échelles.

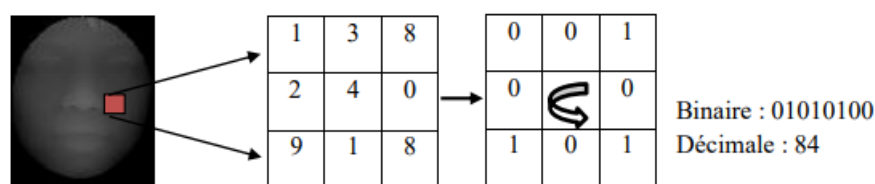


FIGURE 2.5.7 – Une illustration de LBP basique

Dans la littérature la notion LBP est généralement utilisée pour désigner l'opérateur LBP basique, tandis que la notion $LBP_{P,R}$ est utilisée pour représenter l'étendue LBP où, l'indice P représente le nombre des points d'échantillonnage et l'indice R représente le rayon du cercle.

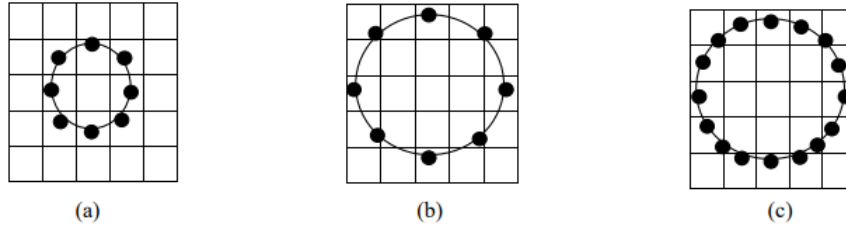


FIGURE 2.5.8 – Exemples de d'opérateur LBP

Les travaux de Ahonen et al ont montré que l'utilisation du descripteur LBP permettait d'obtenir de bonnes performances en reconnaissance de visage [Timo Ahonen 06]. Dans ces travaux, il est proposé de calculer un certain nombre de descripteurs locaux puis de les combiner pour obtenir un vecteur de description du visage. L'image originale est découpée en différentes régions. Les descripteurs associés à chacune de ces régions sont ensuite concaténés pour former un unique vecteur décrivant l'image

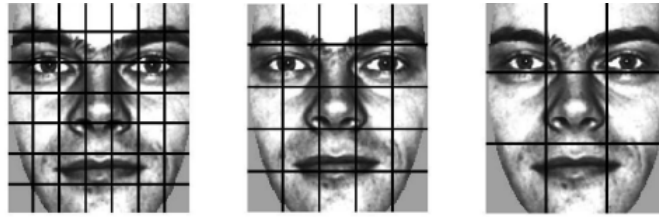


FIGURE 2.5.9 – Découpage de l'image originale en 7×7 , 5×5 et 3×3 régions [F. Perronnin 03]

Ici encore, l'utilisation de descripteurs locaux permet de robustifier la reconnaissance faciale aux variations modérées de pose ou d'illumination.

2.5.1.3 Les 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 [Bouchra 13]. Les caractéristiques locales et les caractéristiques globales ont des propriétés très différentes et peuvent offrir des informations complémentaires utiles à la tâche de classification. Un exemple de ces méthodes est : ElasticBunch Graph Matching (EBGM).

1. ElasticBunch Graph Matching

À partir d'une image de visage, on localise des points caractéristiques (coins des yeux, de la bouche, nez, etc.). Cette localisation peut se faire manuellement ou automatiquement à l'aide d'un algorithme. Un treillis élastique virtuel est ensuite appliqué sur l'image de visage à partir de ces points. Chaque point représente un nœud labélisé auquel on associe un jeu de coefficients d'ondelettes complexes de Gabor, appelés Jet. Pour effectuer une reconnaissance avec une image test, on fait une mesure de similarité entre les différents Jets et les longueurs des segments du treillis de deux images.

2.6 Conclusion

Ce chapitre nous a permis de tirer un certain nombre d'enseignements du processus de reconnaissance d'expressions faciales ou on a présenté les principales difficultés inhérentes à la reconnaissance d'expressions faciales, nous avons cité aussi les principes des systèmes de reconnaissance faciale et un état de l'art des techniques proposées jusqu'à ce jour. Dans le chapitre suivant nous enchaînerons avec l'étude d'une méthode de reconnaissance dite l'opérateur LBP qui sera utilisé plus tard dans la réalisation de notre système de reconnaissance de visage.

Deuxième partie

Extraction des caractéristiques et classification

Chapitre 3

Extraction de caractéristiques et classification

3.1 introduction

Dans le cadre de la classification et d'extraction de caractéristiques d'images contenant chacune une texture (appelées images de texture), il est essentiel d'exploiter des attributs qui caractérisent et discriminent au mieux les différentes classes d'images de texture en présence. Les caractéristiques les plus utiles et uniques des images de visage sont extraites lors de la phase dite « phase d'extraction des caractéristiques ». Par la suite vient la phase de classification où l'image du visage est comparée aux images de la base de données.

Dernièrement diverses techniques d'extraction de caractéristiques discriminatives et efficaces ont été proposés, dont les méthodes locales qui utilisent le descripteurs LBP (Local Binary Pattern) qui a fait un progrès remarquable grâce à sa rapidité de calcul et sa réponse aux contraintes des applications temps réels.

Dans ce chapitre, on présente tout d'abord l'opérateur LBP ainsi que ses diverses variantes, et leurs utilisations comme descripteur faciale, puis on traite la reconnaissance faciale d'image fixe basé sur l'approche LBP.

3.2 Pourquoi le motif binaire locale(LBP)

Les motifs binaires locaux (LBP) sont utilisés comme l'un des outils puissant d'extraction de caractéristiques de texture en raison de leurs capacité à identifier des régions à texture plate et de leurs aptitude à détecter le revêtement. L'opérateur LBP est devenu une approche populaire dans diverses applications [Matti 10] et s'avère plus performant que toutes les autres méthodes, en raison de sa simplicité de calcul, ainsi que son pouvoir d'analyser des images dans des conditions

difficiles en temps réel, ce qui justifie le choix de cet outil pour extraire l'information de texture. Cela peut être considéré comme une approche unificatrice des modèles statistiques et structurels traditionnellement divergents de l'analyse de texture. La propriété la plus importante de l'opérateur LBP dans les applications du monde réel est sa robustesse vis-à-vis du bruit et face aux changements monotoniques d'échelle de gris provoqués, par exemple, par des variations d'éclairage. Une autre propriété importante est son invariance de rotation.

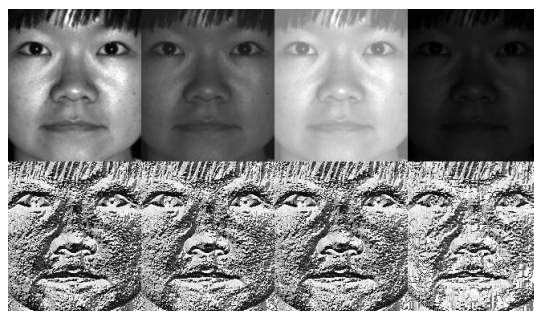


FIGURE 3.2.1 – stabilité de LBP au changement d'illumination [Serge 10]

3.3 Définition de la texture

La texture peut être définie de manière large comme étant les caractéristiques de surface visuelles ou tactiles [Muhammad 03]. Les textures peuvent être constituées de très petits éléments comme le sable, ou des éléments énormes comme des étoiles dans la voie lactée.

En informatique, une texture est une image matricielle qui sert à couvrir la surface d'un objet virtuel avec un programme de graphiques spécial, particulièrement en traitement d'images, la texture est une notion complexe et variée dont on peut citer plusieurs définitions, parmi certaines de ces définitions il y en a qui sont perceptuelles d'autres s'intéressent plus à la stabilité de mesures statistiques à l'intérieur d'une région. La plupart d'entre elles ne sont pas satisfaisantes dans le sens où elles proposent une description soit trop générale et donc quelque chose d'abstrait, difficile à définir quantitativement de façon précise. Cependant une texture peut presque toujours être décrite par des termes, des adjectifs souvent dépendants du domaine concerné (images médicales, images naturelles, matériaux, etc.) mais plus faciles à comprendre et donc plus faciles à manipuler [Isabelle 97]. Voici une définition de texture la plus connue :

- Une texture est une région d'une image pour laquelle il est possible de définir une fenêtre de dimensions minimales, telle qu'une observation au travers de celle-ci se traduit par une perception (impression) visuelle identique pour toutes les

translations possibles de cette fenêtre à l'intérieur de la région considérée.

3.4 Définition de LBP

L'opérateur d'analyse de la texture LBP (Local Binary patterns), introduit par Ojala et al (1996) est un moyen puissant de description de texture. Il s'agit d'affecter à chaque pixel P de l'image $I(i, j)$ à analyser, une valeur caractérisant le motif local autour de ce pixel. Ces valeurs sont obtenues en comparant le niveau de gris du pixel central P aux valeurs des niveaux de gris des pixels voisins.

le concept général de LBP est le suivant : il faut tout d'abord mettre l'image à l'échelle de gris, [CHeraa 16] chaque pixel central est comparé à ses huit voisins, les voisins ayant une valeur inférieure à celle du pixel central auront le bit 0, et les autres voisins ayant une valeur égale ou supérieure à celle du pixel central auront le bit 1. Après on arrange les bits en ligne selon le sens horaire à partir du premier pixel jusqu'au huitième pour obtenir la valeur binaire LBP du pixel centrale. On aura donc des pixels dont l'intensité se situe entre 0 et 255 comme dans une image 8 bits ordinaire.

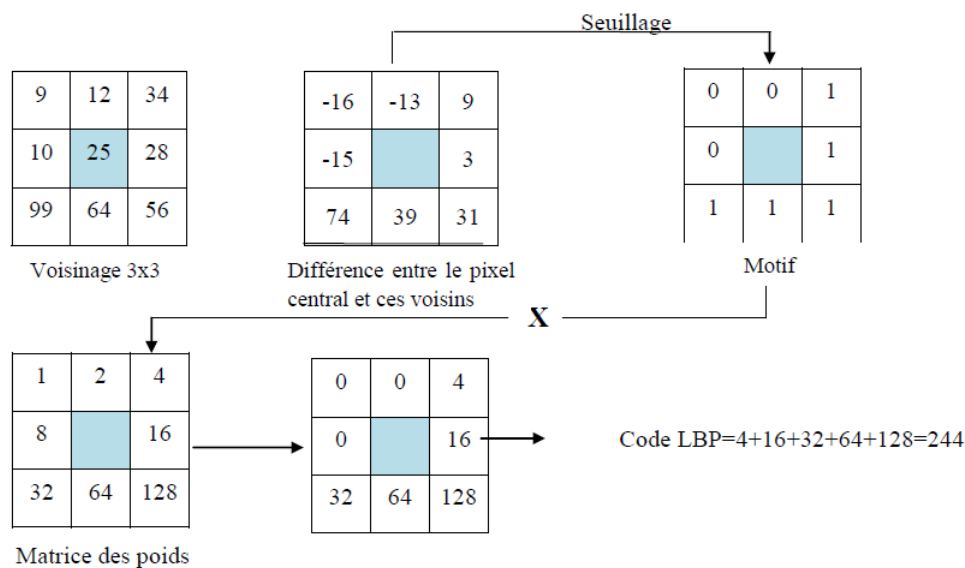


FIGURE 3.4.1 – Calcul et génération du code LBP pour un pixel d'une image

Une fois le code LBP calculé pour tous les pixels de l'image, on calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image faciale. En réalité, afin d'incorporer plus informations spatiales au vecteur représentant le visage, on divise tout d'abord l'image codée par l'opérateur

LBP en petites régions[Rodriguez 06] et l'histogramme est construit pour chaque région. Finalement, on combine tous les histogrammes des régions afin de former un grand histogramme représentant l'image des caractéristiques faciales.

3.5 LBP circulaire

Le LBP circulaire est le resultat de l'étendement de La technique LBP en utilisant des voisinages de tailles différentes. C'est à dire , un cercle de rayon R autour du pixel central et les valeurs des P points échantillonnés sur le bord de ce cercle sont prises et comparées avec la valeur du pixel central [Ghoulia 17]. Il est necessaire de faire appel a une interpolation afin d'obtenir les valeurs des P points échantillonnés dans le voisinage pour tout rayon R. La figure suivante présente des exemples de l'opération LBP ou la notation (P, R) définie les voisinages de centre de cercle P et de rayon R différents :

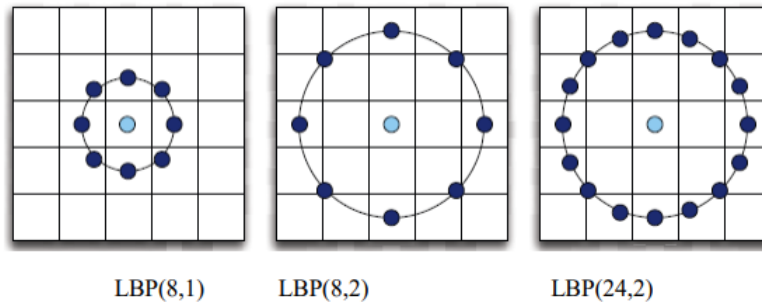


FIGURE 3.5.1 – Exemples de différents voisinages circulaires pour les LBP

On note que l'opérateur LBP de voisinage circulaire de P pixels de rayon R par $LBP_{P,R}$

Le calcul de la valeur de $LBP_{P,R}$ pour un pixel de l'image $I(x_c, y_c)$ est basé sur la formule suivante :

$$LBP_{P,R}(x_c, y_c) = \sum_{k=1}^P s(g_k - g_c) \times 2^{k-1}$$

Avec :

$$s(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{sinon} \end{cases}$$

$g_c = I(x_c, y_c)$ valeur du pixel central

$g_k = I(x_k, y_k)$ valeur du pixel voisin

$$(x_k, y_k) = (x_c + \cos(\frac{2\pi k}{P}), y_c + \sin(\frac{2\pi k}{P}))$$

3.6 LBP uniformes

Un cas particulier important de l'opérateur original (LBP) est l'uniforme. Le descripteur LBP uniforme contient au maximum deux bits transitions de 0 à 1 ou vice versa. Cela signifie qu'on définit un motif uniforme comme étant un motif possédant exactement 0 ou 2 transitions 01 ou 10. 11111111 et 10001111 sont les exemples de modèles binaires uniformes avec zéro transitions au niveau du bit et deux transitions au niveau du bit, respectivement. Si P est le nombre total de points de prélèvement sur le bord du cercle [W. Ben Soltana 14], alors on peut classer l'ensemble des 2^P codes de LBP en deux catégories (uniformes et non uniformes) tel que les codes non uniformes sont regroupés dans une seule classe, le nombre de codes uniformes sera à $P(P-1)+3$ (P est le nombre de voisinage) ce qui donne pour $P=16$, 234 codes avec LBP uniforme au lieu de 65536 codes.

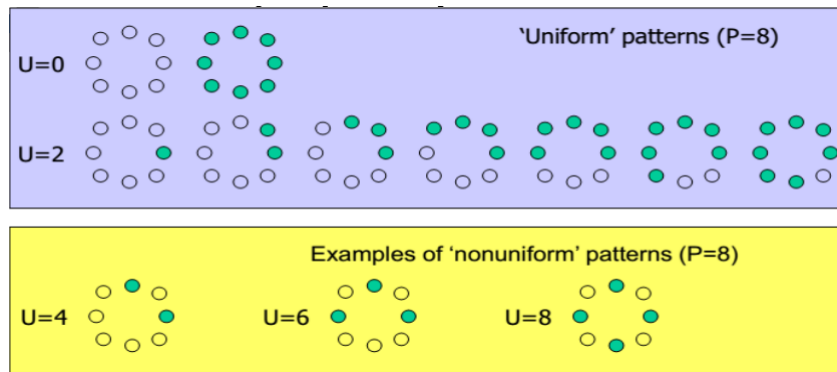


FIGURE 3.6.1 – Exemple d'un modèle uniforme et non uniforme

Une autre raison pour laquelle l'uniforme LBP devrait être utilisé est qu'il ne détecte que les plus importantes caractéristiques des images prétraitées, comme les endroits, les fins de ligne, les bords et les coins. Ceci est fait en divisant une image en plusieurs petites régions dans lesquelles les caractéristiques sont extraites [W. Ben Soltana 14]. Ces caractéristiques consistent en des modèles binaires qui décrivent les environs de pixels dans les régions de points d'échantillonnage sur un cercle de rayon. Cette méthode est couramment utilisée dans les problèmes de classification de textures.

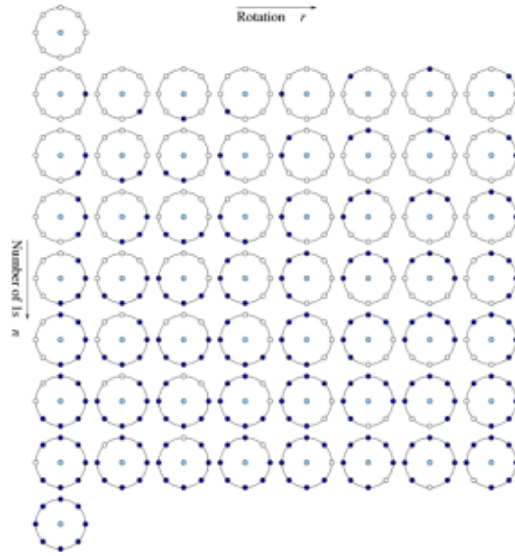


FIGURE 3.6.2 – Les 58 différents motifs uniformes dans un voisinage $(8,R)$ [Juslin 16]

3.7 Histogramme LBP

C'est une représentation unidimensionnelle de la distribution des codes LBP, cette mesure statistique est plus facile à manipuler que l'image LBP, elle est généralement utilisée comme vecteur caractéristique de la texture. Le calcul de l'histogramme LBP noté LBP se fait à partir de l'image $P_{P,R}$, noté LBP par la formule suivante :

$$H_{LBP}(i) = \sum_{0 \leq x < W} \sum_{0 \leq y < H} I(M_{LBP}(x,y) = i) , i=0,...,2^p-1$$

ou :

: fonction indicatrice

$$I(x) = \begin{cases} 0 & x \text{ est faux} \\ 1 & x \text{ est vrai} \end{cases}$$

W : largeur de l'image LBP

H : longueur de l'image LBP

P : nombre de pixels du voisinage

i : code LBP

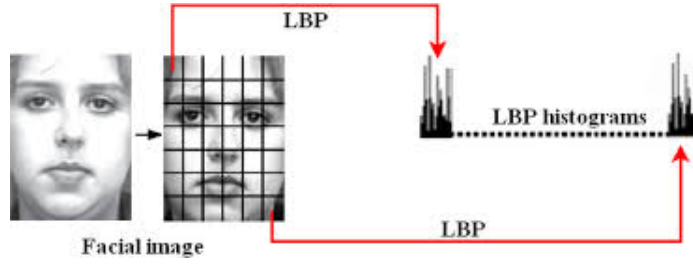


TABLE 3.1 – Exemple d’histogramme LBP

3.8 Reconnaissance de visage avec LBP

La méthode LBP ne montre pas seulement une performance supérieure dans l’analyse de la texture et de la classification de l’application, mais obtient aussi le même bon effet dans les applications de la reconnaissance faciale. Ahonen et al ont appliqué une représentation LBPH (histogramme LBP) pour faire de la reconnaissance du visage et ils ont eu de très bons résultats sur la base de données FERET. Leur méthode s’analyse comme suit :

Après avoir calculé le code LBP pour tous les pixels de l’image du visage, on calcule l’histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l’image faciale. La première chose à faire c’est de diviser tout d’abord l’image codée par l’opérateur LBP en petites régions [Rodriguez 06], l’histogramme est ensuite construit pour chaque région pour incorporer plus d’informations spatiales au vecteur représentant le visage. Après on concatène tous les histogrammes des régions afin de former un grand histogramme représentant l’image des caractéristiques faciales (voir figure 3.8.1). L’efficacité du code LBP comme indice faciale réside dans sa capacité de caractériser les détails d’un visage. Quand seules les LBPs uniformes sont utilisés, tous les codes LBPs non-uniformes sont étiquetés avec une étiquette unique, alors que chacun des codes uniformes est regroupé dans un histogramme unique. Par exemple, quand $P = 8$, nous avons 58 codes uniformes mais l’histogramme est de dimension 59. De même manière $P = 6$ produit un histogramme de dimension 33.

Prennant par exemple deux histogrammes de LBP nommés respectivement ; H^1 et H^2 ; de deux visages, l’étape suivante consiste à utiliser une métrique χ^2 pour calculer la similarité entre ces deux histogrammes . En testant les trois métriques χ^2 , Histogrammes intersection et Log likelihood statistic, Ahonen et al ont observé que la première métrique permet d’obtenir les meilleurs résultats :

$$\chi^2(H^1, H^2) = \sum_i \frac{(H_i^1 - H_i^2)^2}{(H_i^1 + H_i^2)}$$

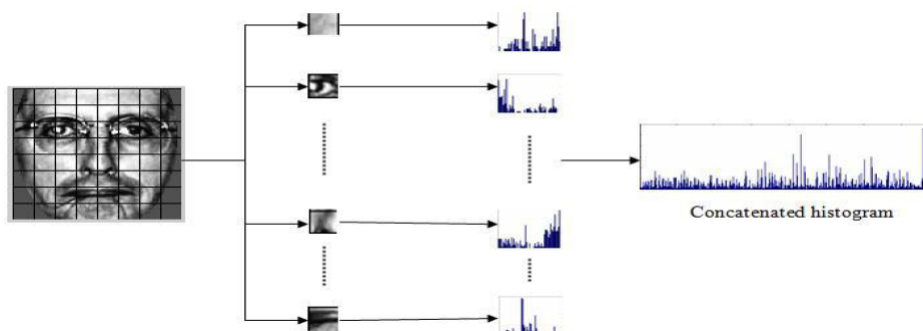


FIGURE 3.8.1 – Illustration de la procédure d'extraction de LBP[Bettahar Abdessettar 14].

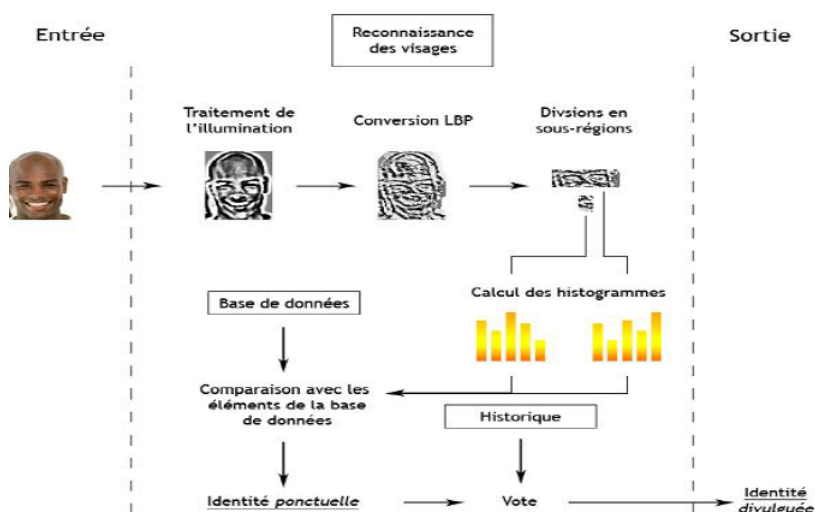


FIGURE 3.8.2 – Illustration du stage de reconnaissance.

3.9 variantes de l'opérateur LBP :

Les modèles binaires locaux (LBP) sont considérés parmi les plus puissants extracteurs de caractéristiques de texture les plus efficaces en termes de calcul. Cependant, la méthode LBP est très sensible au bruit d'image et incapable de capturer les informations de macrostructure. Afin de remédier au mieux à cet inconvénient, nous présentons dans ce qui suit de nouveaux descripteurs pour la classification de la texture.

3.9.1 Complete local binary pattern (CLBP)

Les LBP ne prennent en compte que l'information de signe des différences autour d'un pixel central, négligeant l'amplitude des variations qui peut également contenir de l'information pertinente. De même, la valeur du pixel central est également susceptible de contribuer à cette information complémentaire [Mickaël 14]. Pour cela, Guo et al. (2010) introduisent un nouveau système noté CLBP complétant les LBP afin de considérer ces trois caractéristiques.

Completed Local Binary Pattern (CLBP) [P.Vickram 13], a trois composantes, le signe, la magnitude et le centre pixel. CLBP-S représente le signe positif ou négatif indiquant la différence entre le pixel central et le pixel local, CLBP-M représente la magnitude qui indique la différence entre le pixel central et le pixel local et CLBP-C représente la valeur centrale qui indique la différence entre la valeur de pixel locale et la valeur de pixel centrale moyenne. CLBP capture avec succès plus d'informations discriminantes en combinant les signe, magnitude et niveau de gris central, comme indiqué sur la figure 8.1.

$$S_p = s(g_p - g_c)$$

$$M_p = |g_p - g_c|$$

- L'opérateur CLBP_S est identique au LBP conventionnel , son équation est définie comme suit :

$$CLBP_S_{P,R} = \sum_{K=1}^P s(g_K - g_C) 2^{K-1}$$

- Le CLBP_M peut être défini comme suit :

$$CLBP_M_{P,R} = \sum_{k=0}^{P-1} s(M_P, c) 2^k, s(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{sinon} \end{cases}$$

tel que :

- M_p est la différence de niveau de gris entre le pixel voisin K et le pixel central
- c : est la moyenne différence local de niveaux M_P de toute l'image.

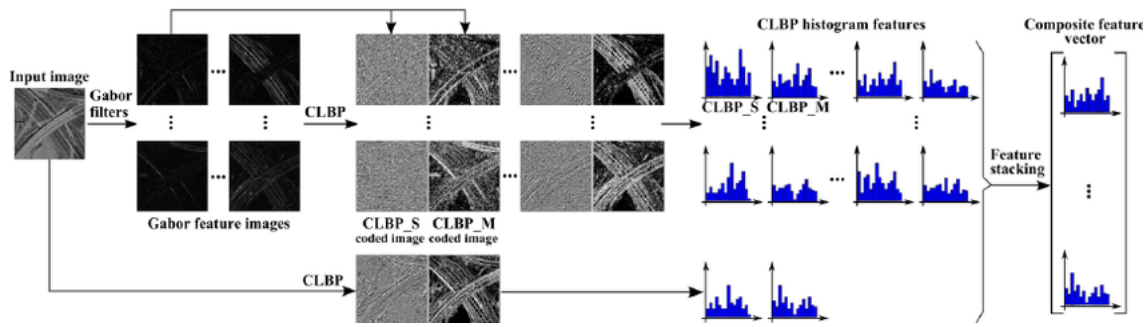


FIGURE 3.9.1 – Méthodologie de CLBP

3.9.1.1 Extraction des caractéristiques avec la CLBP

Une fois les codes CLBP_S et CLBP_M calculés pour tous les pixels de l'images, on passe au calcul de l'histogramme pour former le vecteur caractéristique représentant l'image faciale CLBP [Zhenhua Guo]. Comme pour le calcul de l'histogramme LBP, on divise l'image codée par les opérateurs CLBP_S, CLBP_M en petites régions ensuite on construit un histogramme pour chaque région indépendamment en concaténant l'histogramme de magnitude à celui de signe. Enfin on concatène tous les histogrammes afin de former un histogramme global représentant l'image des caractéristiques faciales.

3.9.2 LBP Allongée (ELBP)

Liao et al ont proposé la méthode LBP allongé (ELBP) pour la reconnaissance faciale, il ont développé une nouvelle fonctionnalité qui est appelée moyenne amplitude maximale de gradient à distance (AMDGM). AMDGM intègre la différence de niveau de gris des informations entre le pixel de référence et voisins pixels dans chaque modèle de ELBP[Mekkani 84]. Il ya trois paramètres associées à l'approche de ELBP : le grand axe de l'ellipse, noté A, le petit axe de l'ellipse, notée par B, et le nombre de pixels voisins m.

La figure 9.2 montre des exemples de schémas de ELBP avec différentes valeurs de A, B, ANDM.

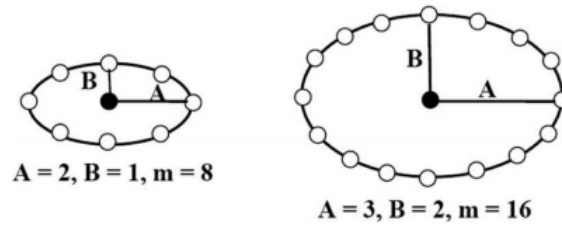


FIGURE 3.9.2 – Des exemples de ELBP avec différentes valeurs de A, B, et m[Mekkani 84]

En fait, les caractéristiques de ELBP sont plus générales que le LBP classique, plus précisément, le LBP classique peut être considérée comme un cas particulier de ELBP lors du réglage des valeurs de A et B(égaux entre eux). Le ELBP est capable de capturer des informations anisotrope à partir des images du visage, comme les yeux, la bouche sont tous des structures allongées. Par conséquent, on s'attend à ce que le ELBP peut avoir plus de pouvoir par rapport au LBP classique.

3.9.3 Ligne des motifs binaires locales (LLBP)

Petpon et al introduit une nouvelle méthode de représentation de visage pour la reconnaissance du visage, appelé schéma binaire de ligne locale (LLBP), qui résume la structure spatiale locale d'une image par le seuillage de la fenêtre binaire locale avec poids et l'introduction d'un nombre décimal comme une texture présentation. En outre, il nécessite moins de temps de calcul [Mekkani 84]. La manière de codage par LLBP est représenté sur la figure 9.3 .

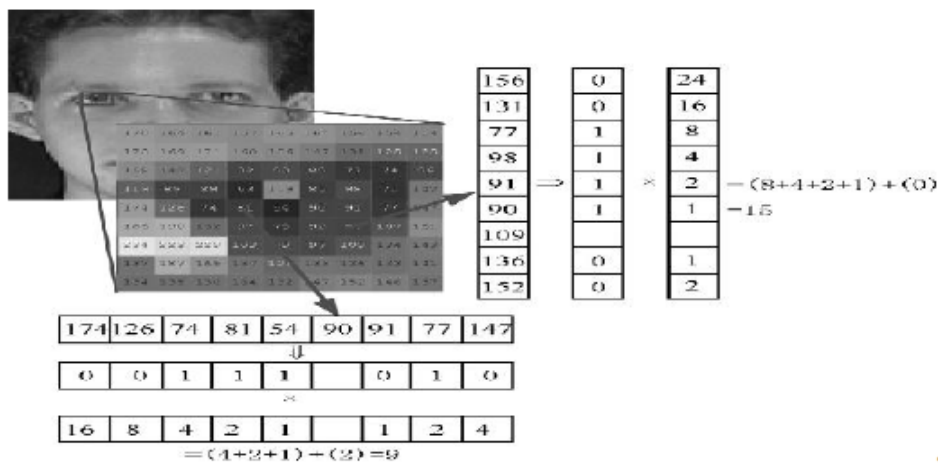


FIGURE 3.9.3 – opérateur LLBP avec une longueur de ligne de 9 pixels [Mekkani 84]

L'idée de base de LLBP est d'obtenir d'abord le code binaire en ligne avec le sens horizontal($LLBP_h$) et vertical ($LLBP_v$) séparément puis calculer sa magnitude($LLBP_m$) , qui caractérise le changement de l'intensité de l'image telle que les bords et les coins. Par conséquent, LLBP est plus discriminante que les autres méthodes, même en condition d'éclairage extrêmes.

3.9.4 Applications de LBP et de ses variantes

3.9.4.1 La détection et le suivi d'objets

Cela faisait plusieurs années que des techniques de soustraction de fond étaient utilisées dans les applications de vision et d'image pour la détection de mouvement. Cependant, la plupart des méthodes ne permettent pas d'obtenir des résultats précis en raison de l'arrière-plan dynamique, des variations d'éclairage, du bruit, etc. Dans l'éditorial, il est proposé de développer une représentation d'arrière-plan stable à partir d'une certaine suite de vidéos [Midhula 17]. Le fond est mis à jour à l'arrivée de chaque image. Pour détecter des objets en mouvement, le fond construit a été comparé à différentes images de la suite vidéo. Pour cela, le modèle d'arrière-plan est développé en utilisant une combinaison de modèle binaire local (LBP) et de moyenne gaussienne. La moyenne gaussienne utilise différentes formes qui, avec le temps, limitent l'opulence sous-jacente du fond. De même, une région spatiale de maintien est utilisée par LBP. La proposition projetée dépend des formes spatio-temporelles apparaissant avec le temps pour fabriquer un arrière-plan de modèle approprié. L'efficacité de la proposition projetée est établie en comparant les résultats avec certaines des méthodes de soustraction d'avant-garde existantes sur des enregistrements standard ouverts.

3.9.4.2 La biométrie :

la LBP a également été utilisée dans de nombreuses autres applications de la biométrie, notamment la localisation des yeux, la reconnaissance de l'iris, la reconnaissance des empreintes digitales, la reconnaissance des empreintes palmaires, la reconnaissance de la démarche et la classification de l'âge du visage.

3.9.5 Classification

Après l'étape d'extraction des caractéristiques, nous procédons à la phase de classification du visage. Elle consiste à attribuer au visage l'identité de la personne qui lui ressemble le plus dans l'ensemble d'apprentissage.

Il existe plusieurs méthodes de classification dont on peut citer les CNN(plus proche voisin), SVM (Support Vector Machine), et dans notre cas on a utilisé la

classification par métriques de distances et les réseaux de neurones grâce à leurs efficacités et leurs flexibilités au niveau des protocoles d'expérimentation.

3.9.5.1 La distance

Pour tester la similarité entre deux vecteurs, la distance est utilisée. Elle permet de mesurer le degré de différence entre deux vecteurs. Il existe plusieurs types de distance parmi lesquels on trouve [P.Vickram 13] :

— **La distance Euclidienne** : (aussi appelée la distance à vol d'oiseau).

$$d(X,Y) = \sqrt{\sum_{i=1}^n (y_i - x_i)^2}$$

Où : x, y sont des vecteurs.

— **La distance de Minkowsky** :

$$d(X,Y) = \left(\sum_{i=1}^n |x_i - y_i|^p \right)^{\frac{1}{p}}$$

Où : x, y sont des vecteurs.

— **La distance de Manhattan** : (appelée aussi taxi-distance) :

$$d(X,Y) = \sum_{i=1}^n |x_i - y_i|$$

Où : x, y sont des vecteurs.

— **distance 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 entre eux. Cette métrique est fréquemment utilisée en fouille de textes.

Soit deux vecteurs A et B , l'angle θ s'obtient par le produit scalaire et la norme des vecteurs :

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

Où : x, y sont des vecteurs.

— **La distance de Mahalanobis** :

Elle est définie comme étant la mesure de dissimilarité entre deux vecteurs aléatoires x, y de même distribution avec une matrice de covariance :

$$d(X,Y) = \sqrt{(x - y)^T \Sigma^{-1} (x - y)}$$

3.10 Conclusion

Dans ce chapitre nous avons discuter l'approche de modélisation LBP, ses diverses variantes dans l'analyse de texture et classification, la reconnaissance et l'analyse de visage. les problèmes importants actuels de la méthode de LBP sont analysés et l'avenir pour la méthode de LBP est fait remarquer.

Dans le chapitre suivant on va présenter un état de l'art sur les réseaux de neurones.

Chapitre 4

État de l'art sur les reseaux de neurones

4.1 Introduction

Lors de l'émergence d'une nouvelle technique, l'ingénieur se demande naturellement en quoi elle peut lui être utile. Si elle est dotée d'un nom plus métaphorique que scientifique, ce qui est évidemment le cas pour les réseaux de neurones, dont le nom est lié fortement à la biologie. Alors techniquement parlant, les réseaux de neurones artificiels (RNA) sont de nature purement mathématique et statistique.

Les réseaux de neurones artificiels constituent l'une des approches d'intelligence artificielle dont le développement se fait à travers les méthodes par lesquelles l'homme essaye toujours d'imiter la nature et de reproduire des modes de raisonnement et de comportement qui lui sont propres.

Nous présentons donc dans ce chapitre un état de l'art de ces réseaux de neurones. D'abord, nous rappellerons la définition et les propriétés des réseaux de neurones, avant de décrire les architectures neuronales les plus utilisées, à savoir les modèles statiques et dynamiques. Nous poursuivrons en exposant les différents types d'apprentissage, ainsi que les domaines d'applications et leurs contributions en classification d'images.

4.2 Pourquoi les réseaux de neurones ?

Grâce aux résultats théoriques et pratiques obtenus au cours des dernières années, les réseaux de neurones forment une solution idéale pour certains problèmes qui nécessitent un raisonnement, ou qui sont de complexité élevée.

Les réseaux neuronaux sont remarquables par leur capacité d'adaptation : ils se modifient eux-mêmes en fonction de l'entraînement initial et les exécutions sui-

vantes leurs apportent encore plus d'informations sur le monde qui les entourent. Le modèle d'apprentissage le plus élémentaire est axé sur la pondération des flux d'entrée, autrement dit sur l'évaluation par chaque nœud de l'importance des entrées provenant de chacun de ses prédécesseurs. Les entrées qui contribuent à mener aux bonnes réponses ont un coefficient plus fort.

Compte tenu de ces caractéristiques et de leurs domaines d'application étendus, les réseaux de neurones sont particulièrement bien adaptés à l'application de problématiques concrètes dans les domaines de la recherche scientifique, commerciale et industrielle[Antoine]. Ils sont utilisés essentiellement pour résoudre des problèmes de classification, de reconnaissance de formes, d'association, d'extraction de caractéristique, et d'identification, ... etc.

4.3 Le neurone

4.3.1 Le neurone biologique

Le neurone biologique est le maillon élémentaire de la chaîne de transmission de l'influx dans le système nerveux. Il s'agit d'une cellule différenciée qui existe sous diverses formes mais dont le principe de fonctionnement est invariant [David 08].

Un neurone tire en transmettant des signaux électriques le long de son axone. Quand les signaux atteignent la fin de l'axone, ils libèrent les neurotransmetteurs qui sont conservés dans des poches appelées vésicules. Les neurotransmetteurs se lient aux molécules de récepteur sur les surfaces de neurones adjacents. Le point de contact virtuel est connu comme la synapse [Ismail 11]. La fonction d'un neurone donc consiste à recevoir un signal et le transmettre à un autre neurone.

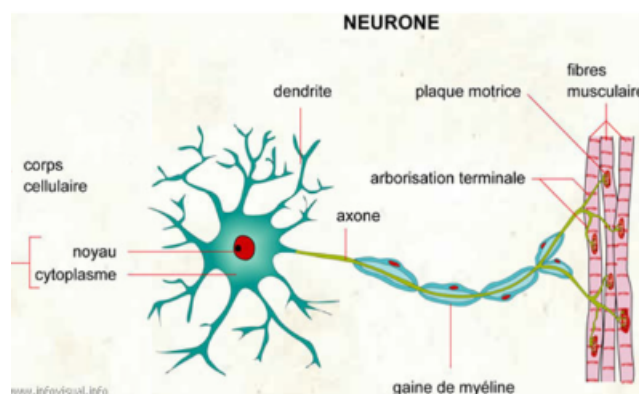


FIGURE 4.3.1 – Schéma simplifié d'un neurone biologique.

Un neurone est composé principalement de core, dendrites et axone. Le point

de connexion entre un neurone et un autre est appelé synapse.

- **Dendrites** : Ils sont similaires à un arbre de fibres. Ils forment une interface réceptrice pour les signaux d'entrée des neurones.
- **Synapse** : Il reçoit les informations à partir des capteurs et des autres neurones et il fournit la sortie via l'axone.
- **Le corps cellulaire (soma)** : c'est l'unité de traitement ; Il reçoit les informations synaptiques et exécute davantage un traitement sur ces informations.
- **Axone** : La sortie qui apparait sous forme d'un potentiel d'action sera transmise aux autres neurones pour des traitements ultérieurs.

4.3.2 Le neurone artificiel

Un neurone artificiel est une représentation informatique d'un neurone biologique. Il est conçu comme un automate doté d'une fonction de transfert qui transforme ses entrées en sorties selon des règles précises.

4.3.2.1 Structure

Chaque neurone artificiel peut être vu comme un processeur élémentaire. Il reçoit un nombre variable d'entrées en provenance de neurones amonts. A chacune de ces entrées est associée un poids w abréviation de weight (poids en anglais) représentatif de la force de la connexion [Claude 92b]. Chaque processeur élémentaire est doté d'une sortie unique, qui se ramifie ensuite pour alimenter un nombre variable de neurones avals. A chaque connexion est associée un poids.

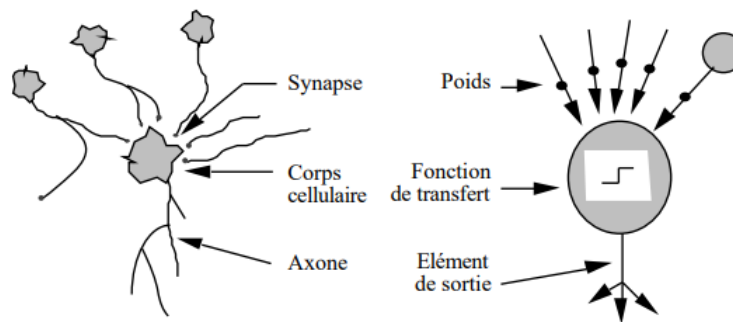


FIGURE 4.3.2 – Mise en correspondance neurone biologique/neurone artificiel[Claude 92b]

4.3.2.2 Comportement

Un neurone formel (artificiel) est une unité de traitement qui reçoit des données provenant des entrées x_i par l'intermédiaire des connexions auxquelles on associe des

poids, sous la forme d'un vecteur, et produit une sortie réelle [Younes 14]. Cette sortie est une fonction des entrées et des poids des connexions.

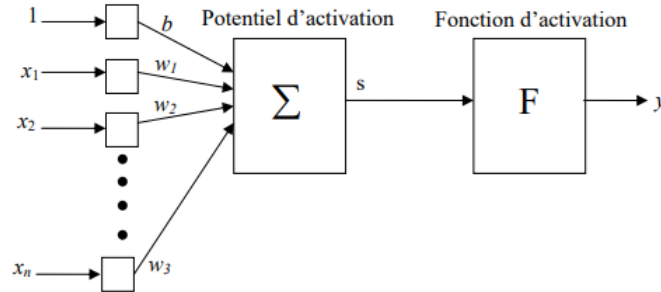


FIGURE 4.3.3 – Modèle d'un neurone formel

Le comportement du neurone artificiel peut être modélisé par deux phases[Claude 92b] :

La première phase, appelée activation, représente le prétraitement des données reçues en calculant la somme pondérée des entrées selon l'expression suivante :

$$a_i = \sum_j w_{ij} x_j$$

Où :

x_j représente les valeurs d'entrées

w_{ij} représente les poids synaptiques entre le neurone d'entrée x_j et le neurone x_i

Dans la deuxième phase, une fonction de transfert calcule la valeur de l'état interne du neurone. C'est cette valeur qui sera transmise aux neurones en aval. Plusieurs possibilités existent pour spécifier la nature de la fonction d'activation du modèle. Les fonctions mathématiques les plus souvent utilisées tel que les fonctions linéaires, sigmoïdes et gaussiennes sont schématisées sur la figure 4.3. A la différence des neurones biologiques dont l'état est binaire, la plupart des fonctions de transfert sont continues, offrant une infinité de valeurs possibles comprises dans l'intervalle $[0, +1]$ ou $[-1, +1]$. Ainsi, le neurone peut être défini mathématiquement comme étant une fonction algébrique, a priori non linéaire (suivant la fonction d'activation f) et bornée, avec des entrées x et paramétrée par les poids w_{ij} .

Soit g la fonction de transfert qui peut être appelée également fonction d'activation calcule la valeur de l'état interne S_j du neurone j à partir de la valeur du potentiel j . Cette valeur désignera la sortie du neurone. Elle sera transmise aux neurones aval.

La formule : $S_j = g(v_j) = g(\sum_{i=1}^n w_{ji} x_i)$

Nom de la fonction	Relation d'entrée/sortie	Icône
seuil	$a = 0$ si $n < 0$ $a = 1$ si $n \geq 0$	
seuil symétrique	$a = -1$ si $n < 0$ $a = 1$ si $n \geq 0$	
linéaire	$a = n$	
linéaire saturée	$a = 0$ si $n < 0$ $a = n$ si $0 \leq n \leq 1$ $a = 1$ si $n > 1$	
linéaire saturée symétrique	$a = -1$ si $n < -1$ $a = n$ si $-1 \leq n \leq 1$ $a = 1$ si $n > 1$	
linéaire positive	$a = 0$ si $n < 0$ $a = n$ si $n \geq 0$	
sigmoïde	$a = \frac{1}{1+\exp^{-n}}$	
tangente hyperbolique	$a = \frac{e^n - e^{-n}}{e^n + e^{-n}}$	
compétitive	$a = 1$ si n maximum $a = 0$ autrement	

FIGURE 4.3.4 – Les modèles de fonctions d'activation

4.4 Réseau de neurones

Les RNA (réseaux de neurones artificiels) sont des réseaux fortement connectés de processeurs élémentaires fonctionnant en parallèle [Wadihaji 03]. Chaque processeur élémentaire calcule une sortie unique sur la base des informations qu'il reçoit. Toute structure hiérarchique de réseaux est évidemment un réseau.

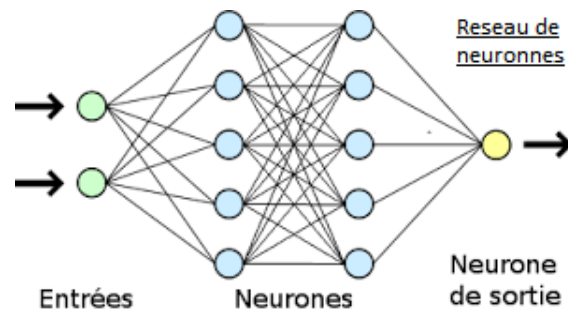


FIGURE 4.4.1 – Forme générale d'un Réseaux de neurone

Comme les neurones formels sont interconnectés entre eux, leur niveau d'interconnexion définit des couches [Lynda 09]. On distingue trois types de couches dans

un RNA :

- La première couche est appelée couche d'entrée. Elle recevra les données source que l'on veut utiliser pour l'analyse. Sa taille est donc directement déterminée par le nombre de variables d'entrées.
- La seconde couche est une couche cachée. Les fonctions d'activations sont en général non linéaires sur cette couche mais il n'y a pas de règle à respecter. Le choix de sa taille n'est pas implicite et doit être ajusté. Il sera souvent préférable pour obtenir la taille optimale, d'essayer le plus de tailles possibles.
- La troisième couche est appelée couche de sortie. Elle donne le résultat obtenu après compilation par le réseau des données entrées dans la première couche. Sa taille est directement déterminée par le nombre de variables qu'on veut en sortie.

Les réseaux de neurones artificiels regroupent en réseaux un certain nombre de neurones formels connectés entre eux de diverses manières. Un réseau est défini par sa topologie, qui représente le type de connexion existant entre les divers neurones du réseau, par la fonction d'activation qui le caractérise et par les méthodes d'apprentissage utilisées pour trouver une relation non linéaire optimale par approximation entre les variables d'entrées et de sorties.

4.5 Topologie des réseaux de neurones

la topologie d'un réseau de neurone représente la façon dont les neurones qui composent le réseau sont reliés, qui peut être quelconque, mais le plus souvent il est possible de distinguer une certaine régularité.

4.5.1 Réseau multicouche

Les neurones sont arrangés par couche. Les neurones d'une même couche ne se communiquent pas, et les connexions ne se font qu'avec les neurones des couches suivantes [Claude 92b]. En général, chaque neurone d'une couche est connecté à tous les neurones de la couche suivante et celle-ci seulement. Ceci nous décrit la notion de sens de parcours de l'information au niveau d'un réseau et donc définir les concepts de neurone d'entrée, neurone de sortie.

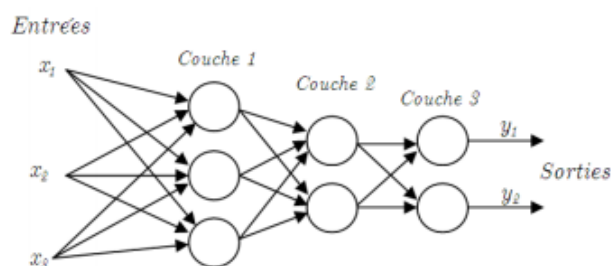


FIGURE 4.5.1 – Réseau multicouche

4.5.2 Réseau à connexions locales .

Il s'agit d'une structure multicouche, mais qui à l'image de la rétine conserve une certaine topologie. Chaque neurone entretient des relations avec un nombre réduit et localisé de neurones de la couche aval. Les connexions sont donc moins nombreuses que dans le cas d'un réseau multicouche classique.

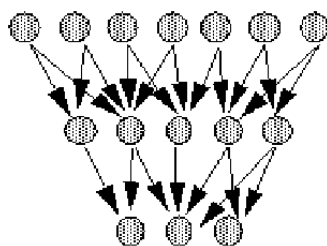


FIGURE 4.5.2 – Réseau à connexions locales[Yasmine 99]

4.5.3 Réseau à connexions récurrentes (dynamiques)

Les connexions récurrentes ramènent l'information en arrière par rapport au sens de propagation défini dans un réseau multicouche. Ces connexions sont le plus souvent locales.

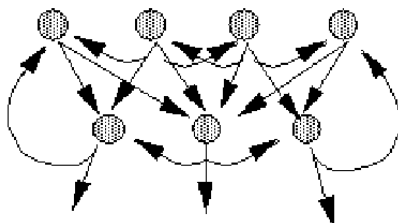


FIGURE 4.5.3 – Réseau à connexions récurrentes[Yasmine 99]

4.5.4 Réseau à connexion complète

C'est la structure d'interconnexion la plus générale. Chaque neurone est connecté à tous les neurones du réseau (et à lui-même).

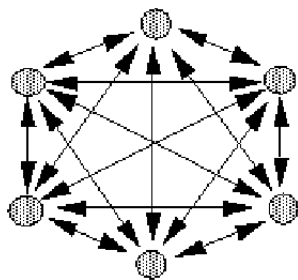


FIGURE 4.5.4 – Réseau à connexion complète[Yasmine 99]

4.6 Type de réseaux de neurones

Un réseau de neurones est une structure de réseau constituée d'un nombre de nœuds interconnectés par des liaisons directionnelles. Chaque nœud représente une unité de traitement et les liaisons représentent les relations causales entre les nœuds. Un réseau neuronal se compose de plusieurs neurones ordonnés dans des plans appelés couches. Les neurones peuvent être reliés par des connexions pondérées avec les neurones des autres couches ou avec celles de la même couche.

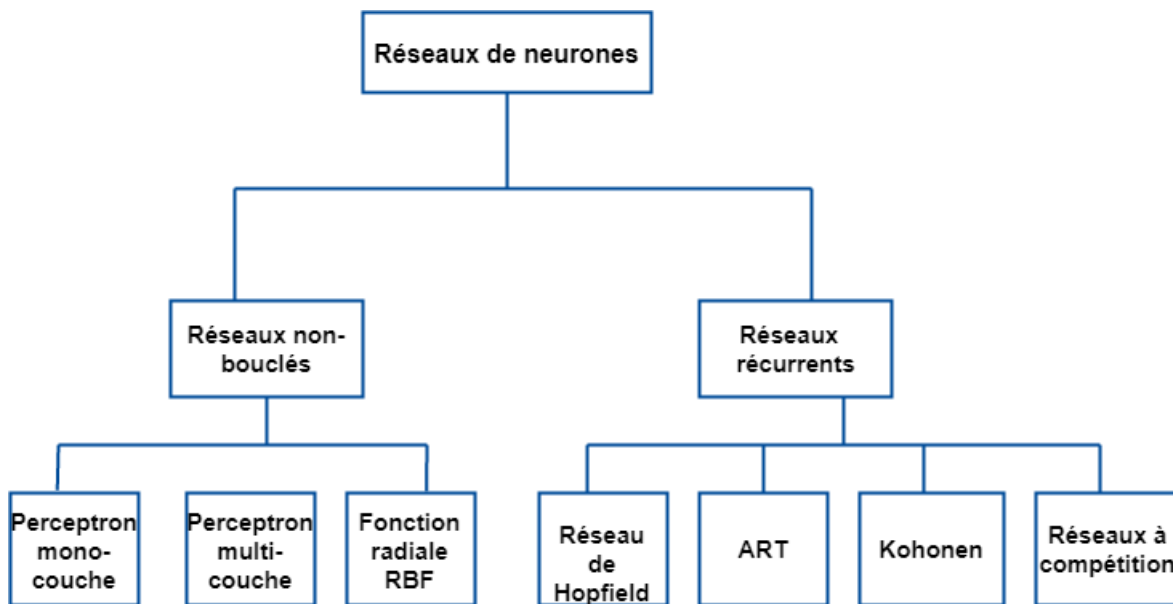


FIGURE 4.6.1 – Topologie des réseaux de neurones[James G 17].

On distingue deux types de réseau :

4.6.1 Réseaux de neurones non bouclés

Un réseau de neurones non bouclé (feed-forward), dit aussi statique est représenté graphiquement par un ensemble de neurones « connectés » entre eux. Le graphe d'un réseau non bouclé est dit acyclique, l'information circulant des entrées (qui portent les valeurs des variables étudiées dans le monde externe) vers les sorties (qui constituent les prévisions, ou signaux de contrôle) est sans « retour en arrière » c'est-à-dire : si l'on se déplace dans le réseau, à partir d'un neurone quelconque, en suivant les connexions, on ne peut pas revenir au neurone de départ [Y 98]. Le mot statique peut faire référence au temps tel que si les entrées sont indépendantes du temps, les sorties le sont également. Si l'on représente le réseau comme un graphe dont les nœuds sont les neurones et les arêtes les "connexions" entre ceux-ci, la représentation de la topologie d'un réseau par un graphe est très utile. Toutefois, il peut exister des neurones cachés qui vont jouer un rôle interne dans le réseau qui effectuent des calculs intermédiaires. Il est nécessaire que les neurones d'entrée, les neurones cachés et les neurones de sortie qui effectuent le dernier calcul de la composition de fonctions soient connectés [Bishop.C 95].

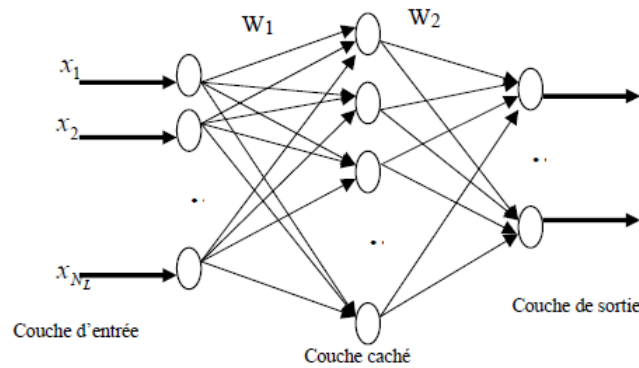


FIGURE 4.6.2 – un réseau de neurone non bouclé [Zahir 14].

4.6.1.1 . Réseau de neurone monocouche (Perceptron)

C'est Le réseau le plus simple appelé le perceptron et caractérisé de la manière suivante : Il possède N informations en entrée et il est composé de p neurones, que l'on représente généralement alignés verticalement. Chacun peut en théorie avoir une fonction d'activation différente. En pratique, ce n'est généralement pas le cas ; Chacun des p neurones est connecté aux N informations d'entrée.[abdelhamid] Si nous considérons n variables d'entrée $x_1, \dots, x_n \in \mathbb{R}$. Le perceptron mono-couche est composé de p neurones, chacun étant connecté à toutes les variables d'entrée. Globalement, ce réseau dispose donc de n entrées et de p sorties et il peut être représenté comme sur la figure suivante :

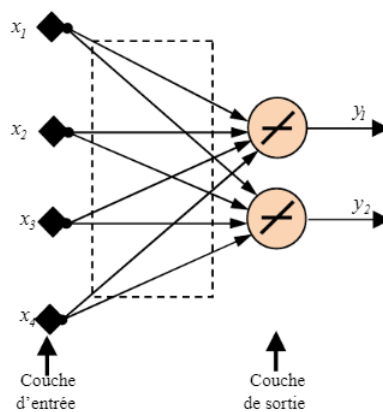


FIGURE 4.6.3 – Perceptron Multi Couche PMC [Philippe]

Les sorties des neurones ne peuvent prendre que deux états (-1 et 1 ou 0 et 1).

Seuls les poids des liaisons entre la couche d'association et la couche finale peuvent être modifiés. La règle de modification des poids utilisée est la règle de Widrow-Hoff : si la sortie du réseau (donc celle d'une cellule de décision) est égale à la sortie désirée, le poids de la connexion entre ce neurone et le neurone d'association qui lui est connecté n'est pas modifié. Dans le cas contraire le poids est modifié proportionnellement. À la différence entre la sortie obtenue et la sortie désirée : $w \leftarrow w + k(d - s)$, Où s est la sortie obtenue, d la sortie désirée et k une constante positive[Nawal 14].

4.6.1.2 Perceptron Multicouches

Les Perceptrons multicouches (PMC) proposé par Rumelhart constituent sans conteste l'architecture la plus fréquemment utilisée actuellement, et il suit un apprentissage supervisé avec la règle de correction de l'erreur [Philippe]. C'est un modèle de réseau à propagation par couche, une couche d'entrée, une couche de sortie et entre les deux une ou plusieurs couches intermédiaires, appelées aussi couches cachées. Les neurones de la première couche reçoivent le vecteur d'entrée, ils calculent leurs sorties qui sont transmises aux neurones de la seconde couche qui calculent eux même leurs sorties et ainsi de suite de couche en couche jusqu'à celle de sortie. Il n'existe pas de connexion entre les neurones d'une même couche, et il n'y a pas de connexions entre les cellules d'une même couche. En revanche tout neurone d'une couche est connecté à tous les neurones de la couche suivante [A. Schmitt 01]. La présence d'une couche cachée permet de modéliser des relations non linéaires entre les entrées et la sortie. En théorie une seule couche cachée suffit, mais le fait de disposer d'une seconde couche cachée permet de modéliser plus facilement une fonction de discrimination non continue. On note aussi que les réseaux multicouches sont beaucoup plus puissants que les réseaux simples à une seule couche. En utilisant deux couches (une couche cachée et une couche de sortie), à condition d'employer une fonction d'activation sigmoïde sur la couche cachée, on peut entraîner un réseau à produire une approximation de la plupart des fonctions, avec une précision arbitraire (cela peut cependant requérir un grand nombre de neurones sur la couche cachée). Sauf dans des rares cas, les réseaux de neurones artificiels exploitent deux ou trois couches.[Youcef 17] Ils peuvent résoudre des problèmes non linéairement séparables.

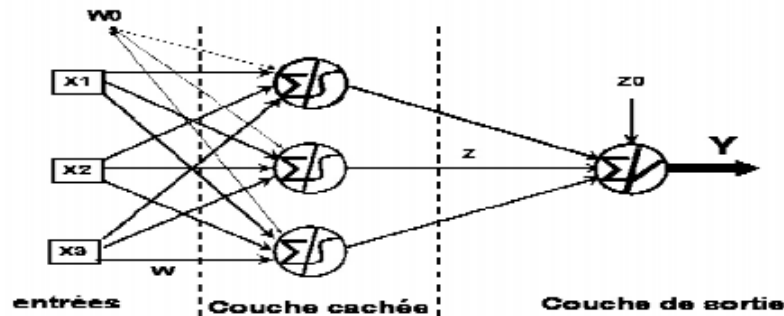


FIGURE 4.6.4 – Perceptron Multi Couche PMC [Philippe]

La sortie du réseau a pour expression :

$$Y = g [Z [f(WX + W_0)] + Z_0]$$

Avec :

f et g les fonctions de transfert, des couches cachées et de sorties respectivement, Y sortie du réseau, X vecteur des entrées.

W : matrice des poids de connexions liant la couche d'entrée à la couche cachée.

W_0 : vecteur des biais des cellules de la couche cachée.

Z : matrice des poids des connexions liant la couche cachée à la couche de sortie.

Z_0 : vecteur des biais des cellules de la couche de sortie.

4.6.1.3 Les Réseaux de Neurones à Fonctions à Base Radiale

Un autre type d'architecture de réseaux de neurones proposé est connu sous le nom de Fonctions à Base Radiale (RBF). Les réseaux RBF constituent probablement le type de réseaux de neurones le plus utilisé après les PMC. À de nombreux égards, les réseaux RBF s'apparentent aux réseaux PMC. Tout d'abord, ils possèdent également des connexions unidirectionnelles vers l'avant (feed-forward) et chaque neurone est entièrement connecté aux unités de la couche suivante. Les neurones sont organisés selon une topologie en couche avec une dynamique feed-forward (des entrées vers les sorties, sans boucle). Il n'en reste pas moins que les modèles de réseaux de neurones RBF sont fondamentalement différents dans la manière dont ils modélisent la relation entre les entrées et les sorties. Tandis que les réseaux PMC modélisent la relation entrée-sortie en une seule étape, un réseau RBF va partitionner ce processus d'apprentissage en deux étapes indépendantes et bien distinctes. Au cours de la première étape, et grâce aux neurones de la couche cachée connus sous le nom de fonctions à base radiale, les réseaux

RBF vont modéliser la distribution de probabilités des données d'entrée. Au cours d'une seconde étape, le réseau RBF va apprendre comment mettre en relation des données.[Bishop.C 95] Les réseaux RBF possèdent deux types de paramètres :

1. la position et la dispersion radiale des fonctions de base et
2. les poids qui permettent de connecter ces fonctions de base aux unités de sortie.

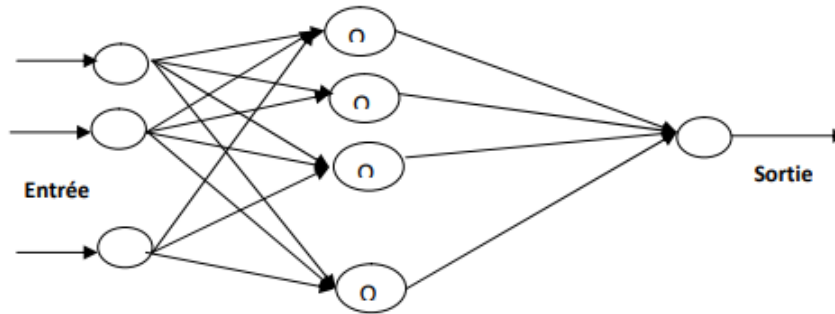


FIGURE 4.6.5 – Architecture générique d'un RBF

4.6.2 Les réseaux de neurones bouclés

Contrairement aux réseaux de neurones non bouclés dont le graphe de connexions est acyclique, les réseaux de neurones bouclés appelé aussi réseaux récurrents, dont le graphe des connexions est cyclique peuvent avoir une topologie de connexions quelconque, qui comporte notamment des boucles qui ramènent aux entrées la valeur d'une ou plusieurs sorties. lorsqu'on se déplace dans le réseau en suivant le sens des connexions, il est possible de trouver au moins un chemin qui revient à son point de départ (un tel chemin est désigné sous le terme de « cycle »). Pour qu'un tel système soit causal, il est obligatoire d'associer à toute boucle un retard : un réseau de neurones bouclé est donc un système dynamique, régi par des équations différentielles ; comme l'immense majorité des applications sont réalisées par des programmes d'ordinateurs, on se place dans le cadre des systèmes à temps discret, où les équations différentielles sont remplacées par des équations aux différences. Il s'agit donc de réseaux de neurones avec retour en arrière (feedback network or recurrent network). [Youcef 17]. Un réseau de neurone bouclé à temps discret est donc régi par une (ou plusieurs) équations aux différences non linéaires, résultant de la composition des fonctions réalisées par chacun des neurones et des retards associés à chacune des connexions. Ce type de réseau est notamment utilisé pour effectuer des tâches de modélisation des systèmes dynamiques, de commande de processus ou de filtrage [Merzouka 09].

4.6.2.1 Réseau de Hopfield(HNN)

Le modèle de Hopfield fut présenté en 1982. Ce modèle très simple est basé sur le principe des mémoires associatives. C'est d'ailleurs la raison pour laquelle ce type de réseau est dit associatif (par analogie avec le pointeur qui permet de récupérer le contenu d'une case mémoire). Il s'agit d'un réseau constitué de neurones à deux états (-1 et 1, ou 0 et 1), dont la loi d'apprentissage est la règle de Hebb (1949), qui veut dire qu'une synapse améliore son activité si et seulement si l'activité de ses deux neurones est corrélée (c'est-à-dire que le poids d'une connexion entre deux neurones augmente quand les deux neurones sont activés au même temps)[Mokri 17]. Ce modèle utilise l'architecture des réseaux entièrement connectés et récurrents (dont les connexions sont non orientées et ou chaque neurone n'agit pas sur lui-même). Les sorties sont en fonction des entrées et du dernier état pris par le réseau. [Youcef 17]

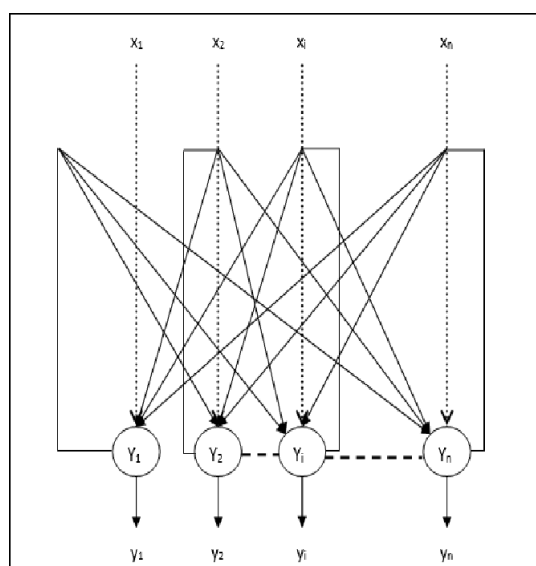


FIGURE 4.6.6 – Architecture de Hopfield

4.6.2.2 La carte auto-organisatrice de Kohonen (SOM)

Contrairement aux réseaux de Hopfield où les neurones sont modélisés de la façon la plus simple possible, on recherche ici un modèle de neurone plus proche de la réalité. Ces réseaux sont inspirés des observations biologiques du fonctionnement des systèmes nerveux de perception des mammifères. [Mokri 17] Une loi de Hebb modifiée (tenant compte de l'oubli) est utilisée pour l'apprentissage. La connexion est renforcée dans le cas où les neurones reliés ont une activité simultanée et diminuée dans le cas contraire (alors qu'il ne se passait précédemment rien dans

ce cas). Tous ces réseaux ont des applications dans la classification, le traitement d'image, l'aide à la décision et l'optimisation.

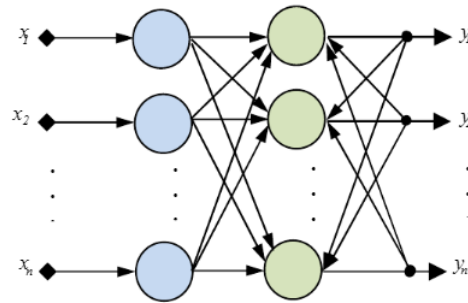


FIGURE 4.6.7 – Topologie de Kohonen[Youcef 17]

Les neurones de la couche de sortie sont placés dans un espace d'une ou de deux dimensions en général, chaque neurone possède donc des voisins dans cet espace. Et qu'enfin, chaque neurone de la couche de sortie possède des connexions latérales récurrentes dans sa couche (le neurone inhibe, les neurones éloignés et laisse agir les neurones voisins) [Youcef 17].

4.6.2.3 Les réseaux compétitifs

Ce sont des réseaux où chaque neurone d'entrée est relié à chaque neurone de sortie, et chaque neurone de sortie inhibe tous les autres et s'auto excite. Cette architecture génère une compétition inter-neurones aboutissant à ce que le réseau ait tendance à reproduire l'organisation topographique des formes d'entrée. En d'autres termes, si l'on présente à ce type de réseau des objets quelconques, le réseau va reproduire dans ses états internes ses traits structuraux [Mokri 01]. Les réseaux compétitifs reproduisent une particularité du fonctionnement biologique des neurones, à savoir l'inhibition latérale. On sait en effet que lorsqu'un neurone biologique est excité, il transmet son excitation aux neurones voisins dans un rayon très court et inhibe par contre les neurones situés à plus grande distance.

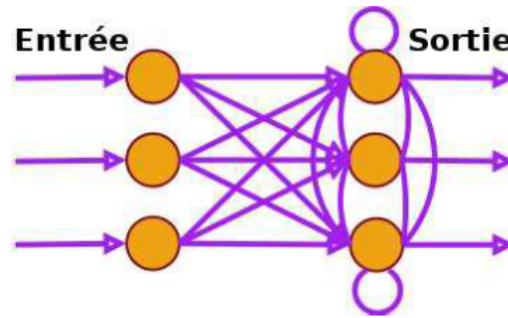


FIGURE 4.6.8 – Les réseaux à compétition

4.6.2.4 Les Réseaux ART

ART (Adaptive Resonance Theory) est un modèle de RNA à architecture évolutive, développé en 1987 par Carpenter et Grossberg. Dans la plupart des réseaux de neurones, deux étapes sont mises en œuvre : La première est dite phase d'apprentissage durant laquelle les poids des connexions sont modifiés selon une règle donnée. La deuxième est la phase d'exécution où les poids ne sont plus modifiés. Avec le réseau ART, ces deux étapes sont réalisées simultanément[Claude 92a]. Le réseau en phase de test s'adapte à des entrées inconnues en construisant de nouvelles classes (ajout de neurones) tout en dégradant au minimum les informations déjà mémorisées. Un réseau ART possède deux caractéristiques en apparence contradictoires : plasticité et stabilité face à des entrées arbitraires ; il est capable de s'adapter à des entrées non familières en construisant de nouvelles catégories ou classes (plasticité) mais aussi d'adapter les classes déjà apprises tout en dégradant peu les informations mémorisées (stabilité). Le problème traditionnellement posé par ces deux notions antagonistes est ainsi résolu par le recours à une architecture évolutive.

Il existe plusieurs versions de réseaux, dont :

- ART1 qui est destiné aux entrées binaires
- ART2 qui prend des entrées continues
- Fuzzy ART qui est une amélioration d'ART1 en vue de simplifier ART2

4.7 Apprentissage des réseaux de neurones

Toute l'information que peut contenir un réseau neuronal réside dans les poids synaptiques. L'apprentissage est la caractéristique principale des réseaux de neurones ; c'est le processus d'adaptation des paramètres d'un système pour remplir au mieux la tâche pour laquelle le réseau est destiné[Merzouka 09], il consiste donc

à ajuster ces derniers pour qu'ils puissent générer correctement la sortie correspondante à chaque point de l'espace d'entrée[Zahir 14]. Ainsi, l'apprentissage peut être défini comme une phase du développement d'un réseau de neurone durant laquelle le comportement du réseau est modifié jusqu'à l'obtention du comportement désiré. Cette définition implique qu'un réseau se doit d'être stimulé par un environnement, qu'il subisse des changements en réaction avec cette stimulation, et que ceux-ci provoquent dans le futur une réponse nouvelle vis-à-vis de l'environnement. Ainsi, le réseau peut s'améliorer avec le temps [Youcef 17].

4.7.1 Types d'apprentissage

Le type d'apprentissage est déterminé par la manière dont les paramètres sont adaptés, il existe plusieurs méthodes et algorithmes pour adapter ces paramètres, on peut distinguer trois types d'apprentissage :

4.7.1.1 Apprentissage supervisé (supervised Learning)

Pour les réseaux à apprentissage supervisé, on présente au réseau des entrées, et au même temps les sorties désirées pour cette entrée. Le réseau doit ajuster ses poids de manière à minimiser une certaine norme de l'erreur de sortie constituée par la différence entre la sortie réelle du réseau et la valeur désirée correspondante (fournie par le professeur)[Zahir 14]. Cette procédure est répétée jusqu'à ce qu'un critère de performance soit satisfait. L'algorithme le plus utilisé est celui de la rétro propagation de l'erreur.

4.7.1.2 Apprentissage non supervisé (unsupervised Learning)

Pour les réseaux à apprentissage non supervisé, aucune information sur la réponse désirée n'est fournie au réseau, le réseau organise lui-même les formes d'entrée en classes [Merzouka 09]. On présente une entrée au réseau et on le laisse évoluer librement jusqu'à ce qu'il se stabilise de façon à minimiser un critère de performances. Ce comportement est connu sous le nom «auto organisation ».

4.7.1.3 Apprentissage par renforcement (Apprentissage semi supervisé)

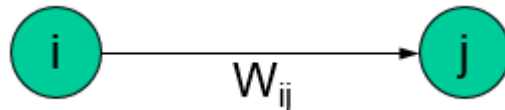
Est une approche utilisée dans les problèmes de planification à travers le temps. Elle utilise deux réseaux : un réseau d'action et un réseau d'évaluation qui joue le rôle d'un superviseur et qui génère un signal d'avertissement à chaque fois que les actions prises sont mauvaises. Ce signal sert à entraîner le réseau d'action[Zahir 14]. Les poids du réseau d'évaluation sont altérés dans le sens de renforcer les bonnes actions et de sanctionner les mauvaises.

4.7.1.4 Apprentissage mixte (hybride)

Dans l'apprentissage mixte, l'apprentissage à partir d'explications n'utilise qu'un seul exemple. L'apprenant n'est pas «parfait», il peut avoir besoin d'explications sur d'autres exemples pour bien comprendre un concept[Karine 09]. Le mode mixte reprend en fait deux autres approches puisque une partie des poids va être déterminée par apprentissage supervisé et l'autre partie par apprentissage non-supervisé.

4.7.2 Les règles d'apprentissage

Les stratégies des modifications des poids des connections entre les neurones synaptiques sont dérivées des règles générales suivantes :



4.7.2.1 Règle de Hebb

La loi de Hebb (1949) s'applique aux connexions entre neurones, comme le représente la figure :

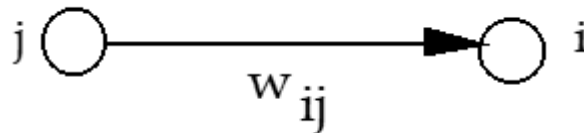


FIGURE 4.7.1 – *i* le neurone amont, *j* le neurone aval et w_{ij} le poids de la connexion

Elle s'exprime de la façon suivante :

"Si 2 cellules sont activées en même temps alors la force de la connexion augmente". La modification de poids dépend de la Co activation des neurones pré synaptique et post synaptique, ainsi que le montre la table 1. x_i et x_j sont respectivement les valeurs d'activation des neurones *i* et *j*, w_{ij} (dérivée partielle du poids) correspond à la modification de poids réalisée [Claude 92a].

x_i	x_j	w_{ij}
0	0	0
0	1	0
1	0	0
1	1	+

FIGURE 4.7.2 – La loi de Hebb

La loi de Hebb peut être modélisée par les équations suivantes ($w(t+1)$ est le nouveau poids, $w_{ij}(t)$ l'ancien) : $w_{ij}(t+1) = w_{ij}(t) + x_i \cdot x_j$ (la coactivité est modélisée comme le produit des deux valeurs d'activation) L'algorithme d'apprentissage modifie de façon itérative (petit à petit) les poids pour adapter la réponse obtenue à la réponse désirée. Il s'agit en fait de modifier les poids lorsqu'il y a erreur seulement.

4.7.2.2 Apprentissage par compétition

L'apprentissage du réseau se fait par le principe d'apprentissage par compétition, qui signifie que seul(s) le ou les neurone(s) sélectionnés ont le droit de modifier leurs poids. Le principe s'exprime alors par la règle d'apprentissage suivante :

$$\Delta \vec{w}_i = \alpha (\vec{x} - \vec{w}_i) \times z_i$$

où :

$\vec{w}_i$: Vecteur de modification des poids du neurone i et α c'est :

Coefficient d'apprentissage déterminant la vitesse de l'apprentissage.

$\vec{x}$: Vecteur d'entrée.

$\vec{w}_i$: Vecteur poids du neurone i .

z_i : Sortie du neurone i , qui est 1 si le neurone est sélectionné, 0 sinon.

L'apprentissage par compétition fonctionne de la même manière que les nuées dynamiques. Il permet ainsi aux neurones de la deuxième couche d'identifier des classes d'objets. Dans le cas idéal, le vecteur poids de chaque neurone correspond au barycentre d'une concentration de vecteurs (en anglais : cluster), qui appartiennent tous à la même classe. Il existe beaucoup de données de ce type, comme les sons vectorisés des lettres dans le domaine de la reconnaissance de la parole, où les vecteurs correspondant à la même lettre se trouvent concentrés à un certain endroit de l'espace d'entrée [Kary 13].

4.7.2.3 Règle de Correction d'erreur

Cette règle est inspiré de l'apprentissage supervisé, c'est-à-dire dans le cas où l'on donne au réseau l'entrée et la sortie correspondante. Si on prend «y » comme étant la sortie calculée par le réseau, et «m »la sortie désirée, le principe de cette règle est d'utiliser l'erreur («m - y »), afin de modifier les connexions et de diminuer ainsi l'erreur globale du système. Donc le réseau va s'adapter jusqu'à ce que «y »soit égal à «m ». sachant que l'apprentissage n'intervient seulement que lorsqu'une erreur est faite, dans le cas contraire, les poids demeurent inchangés [Karine 09]. Cette règle est donc considérée une forme modifiée de la règle d'apprentissage de Hebb.

4.7.2.4 Apprentissage de Boltzman

Les réseaux de Boltzmann sont des réseaux symétriques récurrents. Ils possèdent deux sous-groupes de cellules, le premier étant relié à l'environnement (cellules dites visibles) et le second ne l'étant pas (cellules dites cachées). Les machines de Boltzmann opèrent en deux modes distincts : le mode _gé («clamped» en anglais), dans ce cas les cellules visibles sont affectées à une valeur déterminée par l'environnement ; le mode libre évolution («free-running») dans lequel l'ensemble des cellules, qu'elles soient visibles ou cachées, peuvent changer d'état librement. La règle d'apprentissage est de type stochastique, elle est dérivée de la théorie de l'information et des principes de la thermodynamique [Karine 09]. L'objectif de cet apprentissage est d'ajuster les poids des connexions, de sorte que l'état des cellules visibles satisfasse une distribution probabiliste souhaitée.

4.8 Les avantages et les inconvénients des réseaux de neurone

4.8.1 Les avantages des réseaux de neurones

Les RNA fonctionnent sans programme, n'exécutent pas d'instructions, et ne manipulent pas de nombres. La destruction d'une partie de ces circuits n'empêche pas le réseau de fonctionner. Ces principales propriétés sont [Nassima 12] :

- **réutilisabilité** : un réseau de neurone n'est pas programmé pour une application mais pour une classe de problèmes, après une phase d'apprentissage adéquate, il peut traiter de nombreuses tâches.
- **tolérance aux pannes** : le dysfonctionnement d'une faible proportion des neurones n'affecte pas profondément le fonctionnement général.
- **machine à découvrir les règles** : le fonctionnement des RN implique qu'ils identifient les relations entre les données soumises. on peut envisager qu'ils

- (re)découvrent empiriquement des lois gouvernant les domaines traités.
- **robustesse** : les couches cachées du réseau forment une représentation abstraite des données (concepts), qui permettent de savoir catégoriser des données non traitées lors de l'apprentissage
 - **logique floue** : le traitement modal des données est couvert implicitement par les RN.
 - **Souplesse** : les réseaux de neurones sont capables de traiter une gamme très étendue de problèmes. Classification, filtrage, compression de données, contrôleur, etc...
 - **Bonne résolution** : ils donnent de bons résultats même dans des domaines complexes car ils sont beaucoup plus puissants que les statistiques ou les arbres de décisions.
 - **Bonne adaptation** : une fois que les données sont codées, ils traitent aussi bien des variables continues qu'énumératives.
 - **Parallélisme** : c'est l'exécution de plusieurs tâches (données numériques et non pas symboliques) en même temps, ce qui explique la grande rapidité de calcul des RNA.
 - **Capacité d'apprentissage** : elle permet aux réseaux de tenir compte des contraintes et des données provenant de l'extérieur. Elle se caractérise dans certains réseaux par leur capacité d'auto organisation qui assure leur stabilité.
 - **Mémoire distribuée** : la mémoire est répartie sur plusieurs entités et sur tout le réseau.
 - **Généralisation** : elle permet au réseau de trouver une solution généralisée applicable à tous les exemples du problème, même s'ils contiennent des erreurs ou sont inachevés ou ne sont pas présentés pendant l'apprentissage.
 - **Outils disponibles** : il existe de nombreux produits sur le marché intégrant la technique des réseaux de neurones (4thought, saxon, Neural connections, Clémentine, Intelligent Miner, SAS...).

4.8.2 Les points faibles des réseaux de neurones

Un réseau de neurones ne dispense pas de bien connaître son problème, de définir ses classes avec pertinence, de ne pas oublier de variables importantes, etc. Un réseau de neurones est une « boîte noire » qui n'explique pas ses décisions. Les réseaux de neurones ont une très bonne prédiction statistique (ayant la capacité de s'accommoder de valeurs très bruitées ou même manquantes), mais ils sont complètement impossibles à inspecter. La perte partielle de compréhension est compensée par la qualité des prédictions.

On peut résumer ces inconvénients par les points suivants [Nassima 12] :

- **processus d'apprentissage** :

- peut etre extrememnt long
- l'apprentissage par rétro-propagation des erreurs peut converger vers une solution sous optimale
- paralysie du réseau : les poids synaptiques deviennent si grands que leurs modification est inopérante sur le comportement des neurones (dépassement de la zone de variation de ségmoïde)
- surspécification : lorsque l'apprentissage est trop prolongé ,le RN perd son pouvoir de généralisation. Il reconnait les données de l'échantillon d'apprentissage, mais plus de nouvelles données.
- **explicaibilité** : il est quasi impossible d'expliquer de manière compréhensible les résultats fournis par un RN. Un RN peut découvrir empiriquement des lois et les exploiter dans la résolution des problèmes, mais il ne peut formuler ces lois.
- **Codage des entrées** : toutes les entrées d'un réseau de neurone doivent se trouver dans un intervalle défini en général entre 0 et 1, ce qui entraîne des transformations qui impliquent des traitements supplémentaires, et risque de fausser les résultats.
- **• Lisibilité** : les réseaux de neurones ne fournissent pas l'explication de leur résultat. Ce qui peut être gênant si on cherche à comprendre un phénomène.
- **Détermination de la taille** : afin que l'échantillon fournisse de bons résultats, sa taille doit être calculée en fonction du nombre d'entrée, du nombre des couches et du taux de connexion ce qui entraîne une augmentation du nombre d'exemple qui ne sont pas toujours disponibles.
- **Performance** : le nombre de calculs à effectuer pour définir un réseau optimal peut être très consommateur de puissance, ce qui peut donner de mauvaises performances à cette technique.

4.9 Domaines d'applications

La reconnaissance d'images est l'un des premiers domaines d'application réussie des réseaux neuronaux, mais la technologie s'est étendue à bien d'autres, Cidessous, un certain nombre de domaines dans lesquels les réseaux de neurones ont été appliqués avec succès [A. Houamed 15] :

- **Traitement d'image** : compression d'images, reconnaissance de caractères et de signatures, reconnaissance de formes et de motifs, cryptage, classification, ..
- **le traitement automatique des langues** : la traduction et la génération automatique de textes en langue naturelle, segmentation en mots, représentation sémantique des mots (plongements lexicaux), étiquetage morphosyntaxique, traduction automatique, ...

- les prévisions boursières, sélection d'investissements, Prévision du coût de la vie, attribution de crédits...
- la planification et l'optimisation des tournées de livraison, la découverte et l'élaboration de médicaments
- **Traitement du signal** : traitement de la parole, identification de sources, filtrage, classification, ...
- **Environnement** : évaluation des risques, analyse chimique, prévisions et modélisation météorologiques, gestion des ressources...
- **Contrôle** : diagnostic de pannes, commande de processus, contrôle qualité, robotique.
- **Optimisation** : allocation de ressources, planification, régulation de trafic, gestion, finance, ..
- **Aérospatial** : pilotage automatique, simulation du vol. . .
- **Automobile** : système de guidage automatique, . . .
- **Défense** : guidage de missile, suivi de cible, reconnaissance du visage, radar, sonar, lidar, traitement du signal, compression de données, suppression du bruit. . .
- **Electronique** : prédiction de la séquence d'un code, vision machine, synthétiseur vocal, modèle non linéaire, . . .
- **Simulation** : simulation boîte noire, prévisions météorologiques.
- Modélisation de l'apprentissage et perfectionnement des méthodes de l'enseignement.
- Approximation d'une fonction inconnue ou modélisation d'une fonction connue mais complexe à calculer avec précision
- Prévision de consommation d'eau (Lyonnaise, CGE), d'électricité (EDF), de trafic routier (Cofiroute), de cours boursiers...
- Identification de procédé industriel (Air liquide, ElfAtochem, ciments Lafarge...)

4.10 Réseaux de neurones et classification d'images

Le problème de l'approche classique de la reconnaissance des images est qu'un bon extracteur de caractéristiques est très difficile à construire, et qu'il doit être repensé pour chaque nouvelle application. Bien que l'imagerie numérique semble être le domaine d'application par excellence des réseaux de neurones, ce domaine se caractérise aussi par l'importance et la complexité des données à traiter. Les réseaux de neurones fournissent les techniques pour les résolutions de ces problèmes. Deux méthodes seront présentées dans ce qui suit :

1. Jusqu'à récemment, les systèmes de reconnaissance des images classiques étaient composés de deux blocs : un extracteur de caractéristiques (feature

extractor en anglais), suivi d'un classifieur entraînable simple. L'extracteur de caractéristiques consiste à transformer le tableau de nombres représentant l'image en une série de nombres sous forme d'un vecteur de caractéristiques. Ce vecteur est envoyé au classifieur. Ce dernier calcule une somme pondérée des caractéristiques : chaque nombre est multiplié par un poids avant d'être sommé. Si la somme est supérieure à un seuil, la classe est reconnue. Les poids sont différents pour les classifieurs de chaque catégorie, et ce sont eux qui sont modifiés lors de l'apprentissage [MM.Zakaria 17]. Les premières méthodes de classification linéaire entraînable datent de la fin des années cinquante et sont toujours largement utilisées aujourd'hui. Elles prennent les deux noms de perceptron ou régression logistique.

2. L'apprentissage profond ou deep Learning intervient après avoir un problème avec l'approche classique de la reconnaissance d'images à cause de sa difficulté de construction et qu'il doit être repensé pour chaque nouvelle application. L'idée du deep Learning est simple : le système entraînable est constitué d'une série de modules chacun représentant une étape de traitement. Chaque module est entraînable, comportant des paramètres ajustables similaires aux poids des classifieurs linéaires. Le système est entraîné de bout en bout : à chaque exemple, tous les paramètres de tous les modules sont ajustés de manière à rapprocher la sortie produite par le système de la sortie désirée.

Pour pouvoir entraîner le système de cette manière, il faut savoir dans quelle direction et de combien ajuster chaque paramètre de chaque module [Philippe 10]. Pour cela il faut calculer un gradient, c'est-à-dire pour chaque paramètre ajustable, la quantité par laquelle l'erreur en sortie augmentera ou diminuera lorsqu'on modifiera le paramètre d'une quantité donnée. Le calcul de ce gradient se fait par la méthode de rétro propagation. Dans sa réalisation la plus commune, une architecture profonde peut être vue comme un réseau multicouche d'éléments simples, interconnectés par des poids entraîlables.

4.11 Conclusion

Dans ce chapitre, nous avons exposé l'un des puissants outils de l'IA, à savoir les réseaux de neurones, que ce soit les réseaux statique(non bouclés) ou dynamique(bouclés), leurs topologie et on a défini aussi l'apprentissage ses types, et les règles qui lui sont associés, leur classification et on a fini par citer les avantages et les inconvénients des réseaux de neurones et leur domaine d'application.

Dans le chapitre suivant on va bien détailler les différentes étapes de conceptions et de réalisations.

Chapitre 5

Conception et Réalisation

5.1 Introduction

Ce chapitre est consacré à l'étude analytique du fonctionnement du système, la description des différentes étapes de sa réalisation, et les détails d'implémentation des différents modules.

Nous commencerons par montrer les différents cas d'usage, en passant par les méthodes de mesure de performances, aussi les outils utilisés pour la réalisation de notre application, on présentera quelque interface de cette dernière et enfin, la structure algorithmique et modulaire du système.

5.2 Mise en situation

Le but de notre travail consiste à réaliser un système de reconnaissance de visage qui répond aux exigences de performance suivantes :

- concevoir un système fiable.
- assurer d'avoir les taux d'identification et d'authentification acceptables.
- reconnaître le maximum de personnes possible.
- pouvoir ajuster les paramètres pour avoir une bonne identification.

Donc notre objectif primordial consiste à choisir la configuration adéquate pour obtenir le meilleur système biométrique possible en terme de taux de performance.

5.3 Conception du système

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.

5.3.1 Les acteurs du système

L'administrateur

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

— **son rôle :**

- gestion de la base de données.
- gère les clients du système.
- Test et réglage des différents paramètres du système.

individu Test

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

— **son rôle :**

- s'identifier/s'authentifier au près du système.

5.3.2 Le diagramme de cas d'utilisation global :

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 :

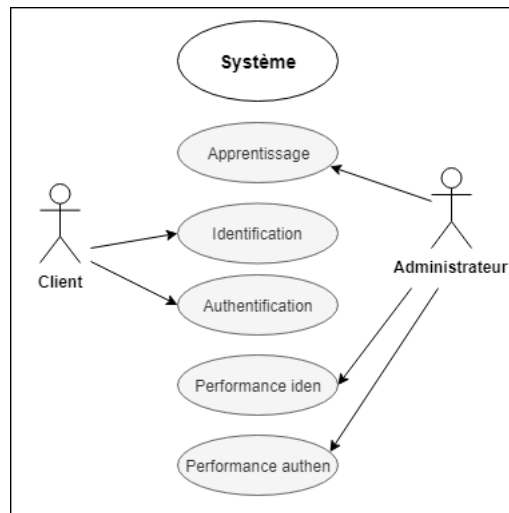


FIGURE 5.3.1 – Diagramme de cas d'utilisation global

5.3.3 Description textuelle des cas d'utilisation

5.3.3.1 Description du cas d'utilisation « Apprentissage »

Dans cette phase, nous allons décrire le fonctionnement du système, afin d'en faciliter la réalisation.

Cas d'utilisation : Apprentissage
Acteur : l'administrateur.
Résumé : Ce cas d'utilisation permet à l'administrateur de récupérer les 5 images de chaque client du système à partir d'une base de données (ORL). Ces images du visage sont utilisées pour générer un modèle unique qui sera stocké avec les informations personnelles dans une base de données pour une utilisation ultérieure.
Scénario nominal :
1- On prend N images de la base de données pour faire l'apprentissage. 2- Application des prétraitements nécessaires sur les N images, pour éliminer le bruit. 3- L'extraction des paramètres de l'ensemble des images d'apprentissage en utilisant l'approche LBP uniforme. 4- Le résultat (Matrice LBP uniforme). 5- Enregistrement des modèles d'apprentissage (Matrice LBP uniforme) dans la base de données. 6-Affichage des résultats (message de réussite).

5.3.3.2 Description du cas d'utilisation « identification »

Cas d'utilisation : Identification
Acteur : Client.
Résumé : Quand l'utilisateur cherche à s'identifier, le système charge une image à partir d'une base de données. 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.
Scénario nominal :
1. on prend une image de la base de données de l'individu test. 2. Application des prétraitements nécessaires sur l'image pour éliminer le bruit. 3. Extraction des paramètres pertinents de l'image test à l'aide de l'approche LBP uniforme. 4. Calculer le degré de vraisemblance entre les paramètres de l'image test et tous les modèles clients stockés dans la base de données, à la fin de cette phase on aura des scores résultants . 5. Trier les scores résultants de l'étape précédente pour indiquer la personne la plus proche de l'individu test. 6. Affichage des résultats (l'identifiant, les informations client).

5.3.3.3 Description du cas d'utilisation « authentification »

Cas d'utilisation : authentification
Acteur : Client.
Résumé : C'est le cas d'un individu qui proclame une identité pour une autorisation d'accès par exemple. Le système charge une image à partir d'une base de données pour vérifier si elle correspond à l'identité proclamée ou pas.
Scénario nominal : .
1. Le client introduit son identifiant. 2. on prend une image de la base de données de l'individu test. 3. Application des prétraitements nécessaires sur l'image pour éliminer le bruit. 4. Extraction des paramètres pertinents de l'image test à l'aide de LBP uniforme. 5. Calculer le degré de vraisemblance entre le modèle de l'individu test et son modèle enrôlé dans la base de données, à la fin de cette phase nous aurons un score résultant. 6. Comparer le score résultant avec le seuil optimal du système (ou bien celui choisi par l'administrateur). 7. Affichage des résultats (client ou imposteur, les informations client).

5.3.3.4 Description du cas d'utilisation « Performane Identification »

Cas d'utilisation :Performance Identification
Acteur : Administrateur.
Résumé : Dans ce cas, l'administrateur fait des tests sur une base de données d'images. Ceci, afin d'évaluer le système, mesurer la performance (Taux d'identification « TID »).
Scénario nominal
1. Il choisit la configuration. 2. La sélection de la base de données pour faire les tests. 3. Chargement des modèles d'apprentissage et de test déjà enregistrés et le seuil pour la configuration choisie 4. La mesure de performances du système : le calcul du TID. 5. Affichage des résultats : TID.

5.3.3.5 Description du cas d'utilisation «performance vérification »

Cas d'utilisation : Performance Vérification
Acteur : Administrateur.
Résumé : Dans ce cas, l'administrateur fait des tests sur une base de données d'images. Ceci, afin d'évaluer le système, mesurer les performances (Taux de faux rejets «FRR »,taux de fausses acceptations«FAR »).
Scénario nominal
1. L'utilisateur choisi la configuration. 2. La sélection de la base de données pour faire les tests. 3. Chargement des modèles d'apprentissage et de test déjà enregistrés. 4. La mesure de performances du système : le calcul du FAR,FRR et le seuil pour la configuration choisie 5. Affichage des résultats : FAR,FRR.

5.3.4 Diagrammes de séquence (cas d'utilisation détaillés) :

Afin de décrire le fonctionnement du système et ces différentes phases, on utilise les diagrammes de séquences pour décrire comment les éléments du système interagissent entre eux et avec les acteurs.

5.3.4.1 Cas d'utilisation : Apprentissage

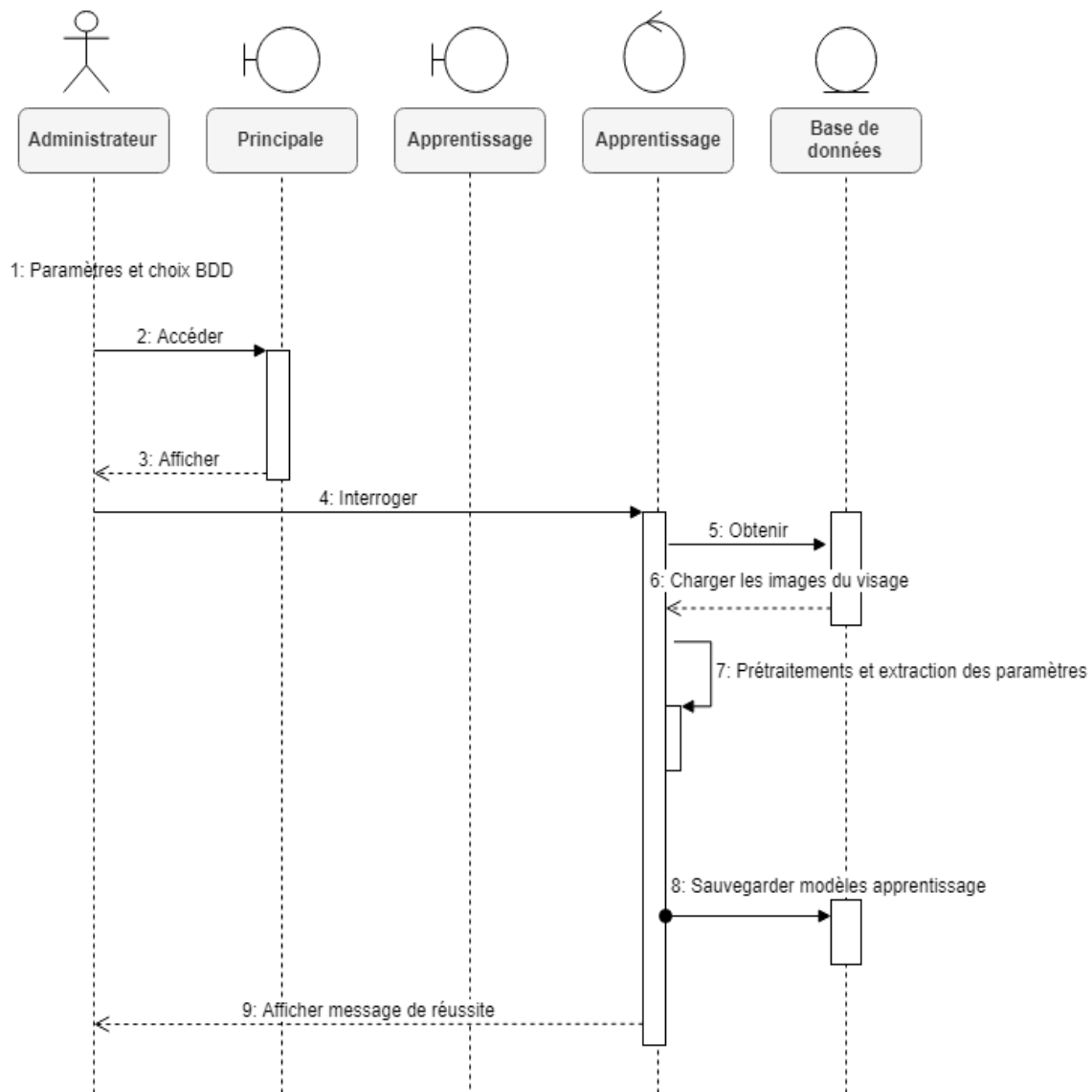


FIGURE 5.3.2 – Diagramme de séquence cas d'utilisation « Apprentissage ».

Description du scénario d'apprentissage :

1. L'administrateur choisi la configuration et la sélection de la base de données pour faire l'apprentissage.
2. L'extraction des paramètres de l'ensemble des images d'apprentissage en utilisant l'approche LBP uniforme.

3. Le résultat.
4. Enregistrement des modèles d'apprentissage dans la base de données.
5. Affichage des résultats (message de réussite).

5.3.4.2 Cas d'utilisation : Identification

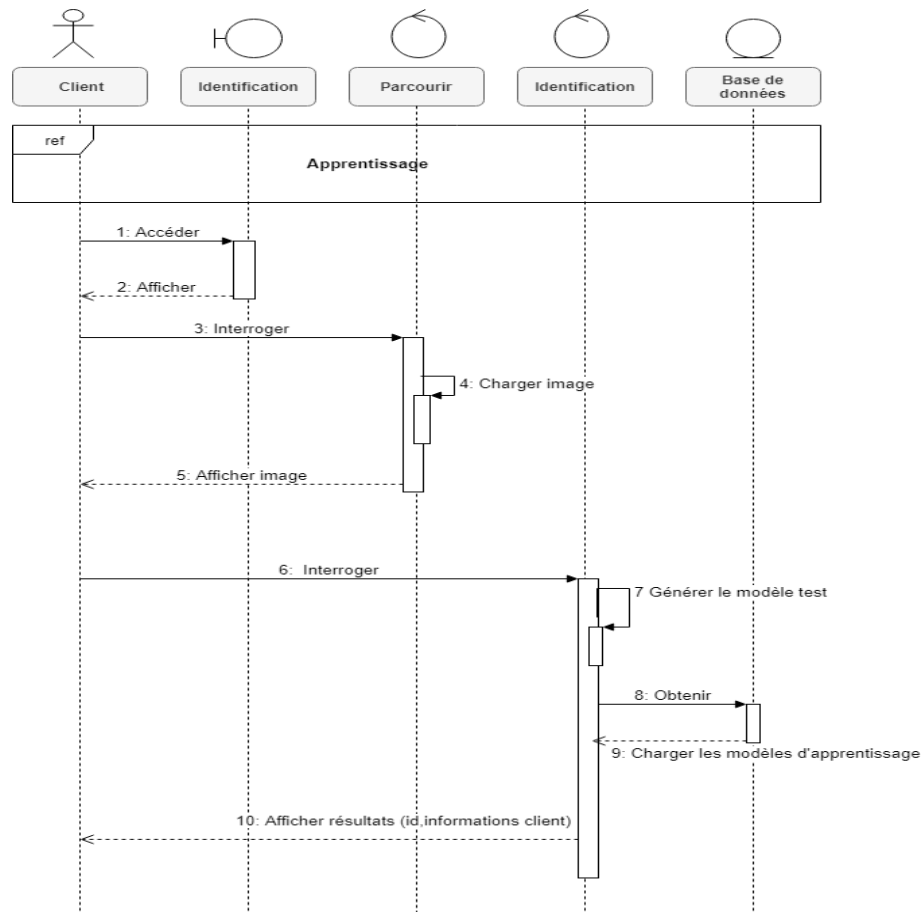


FIGURE 5.3.3 – Diagramme de séquence cas d'utilisation « Identification ».

Description du scénario identification :

1. On prend une image de la base de données de l'individu test.
2. Application des prétraitements nécessaires sur l'image pour éliminer le bruit.
3. Extraction des paramètres pertinents de l'image test à l'aide de LBP uniforme.

4. Calculer le degré de vraisemblance entre les paramètres de l'image test et tous les modèles clients enrôlés et stockés dans la base de données, à la fin de cette phase on aura des scores résultants.
5. Trier les scores résultants de l'étape précédente pour indiquer la personne la plus proche de l'individu test.
6. Affichage des résultat (identité de la personne).

5.3.4.3 Cas d'utilisation : Authentification

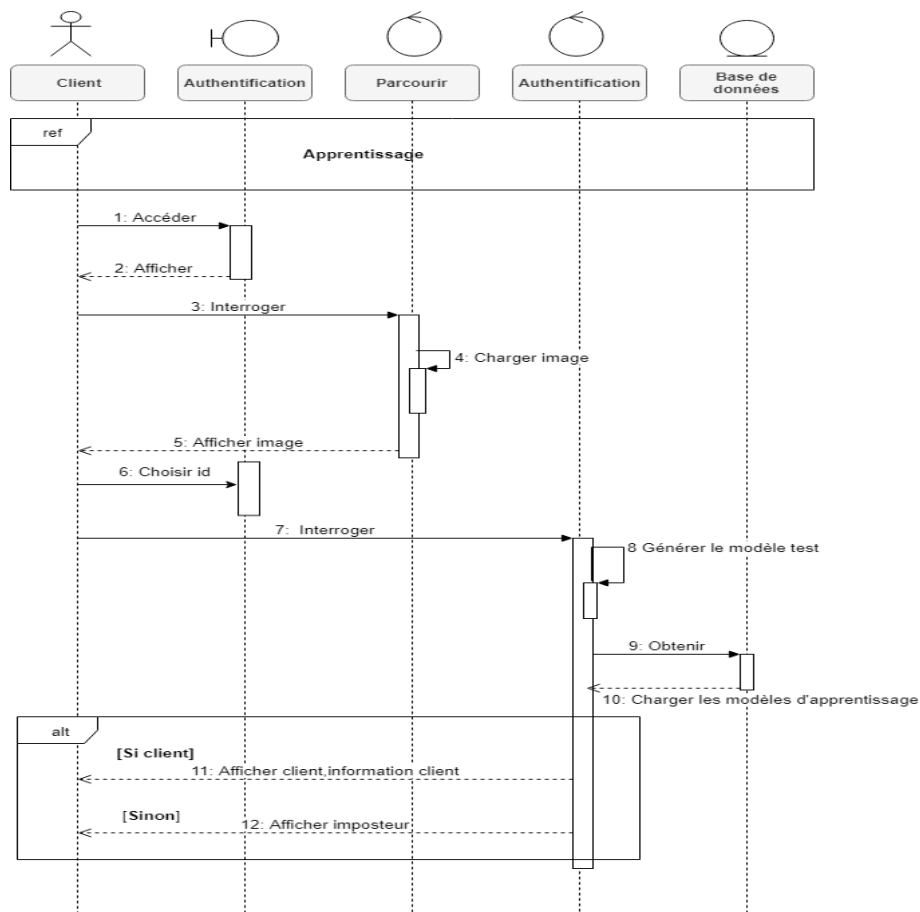


FIGURE 5.3.4 – Diagramme de séquence cas d'utilisation « Authentification ».

Description du scénario authentification :

1. On prend une image de la base de données de l'individu test.
2. Le client introduit son identifiant.

3. Application des prétraitements nécessaires sur l'image pour éliminer le bruit.
4. Extraction des paramètres pertinents de l'image test à l'aide de LBP uniforme.
5. Calculer le degré de vraisemblance entre le modèle de l'individu test et son modèle enrôlée dans la base de données.
6. Comparer le score résultant avec le seuil optimal du système.
7. Affichage des résultats.

5.3.4.4 Cas d'utilisation : Performance identification

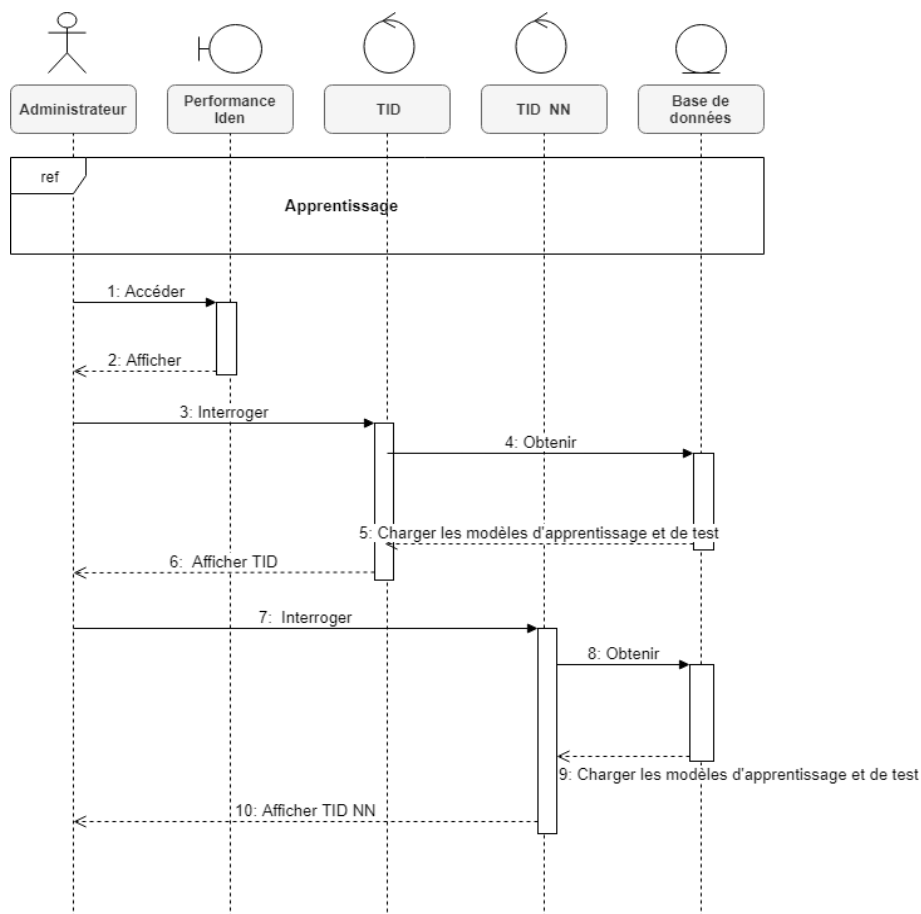


FIGURE 5.3.5 – Diagramme de séquence cas d'utilisation « Performance identification ».

Description du scénario performance identification :

1. L'administrateur choisi la configuration.

2. La sélection de la base de données pour faire les tests.
3. Chargement des modèles d'apprentissage et de teste déjà enregistrés.
4. La mesure des performances du système : le calcul du TID, TIDnn et Seuil pour la configuration choisie.
5. Affichage des résultats : TID, TIDnn.

5.3.4.5 Cas d'utilisation : Performance vérification

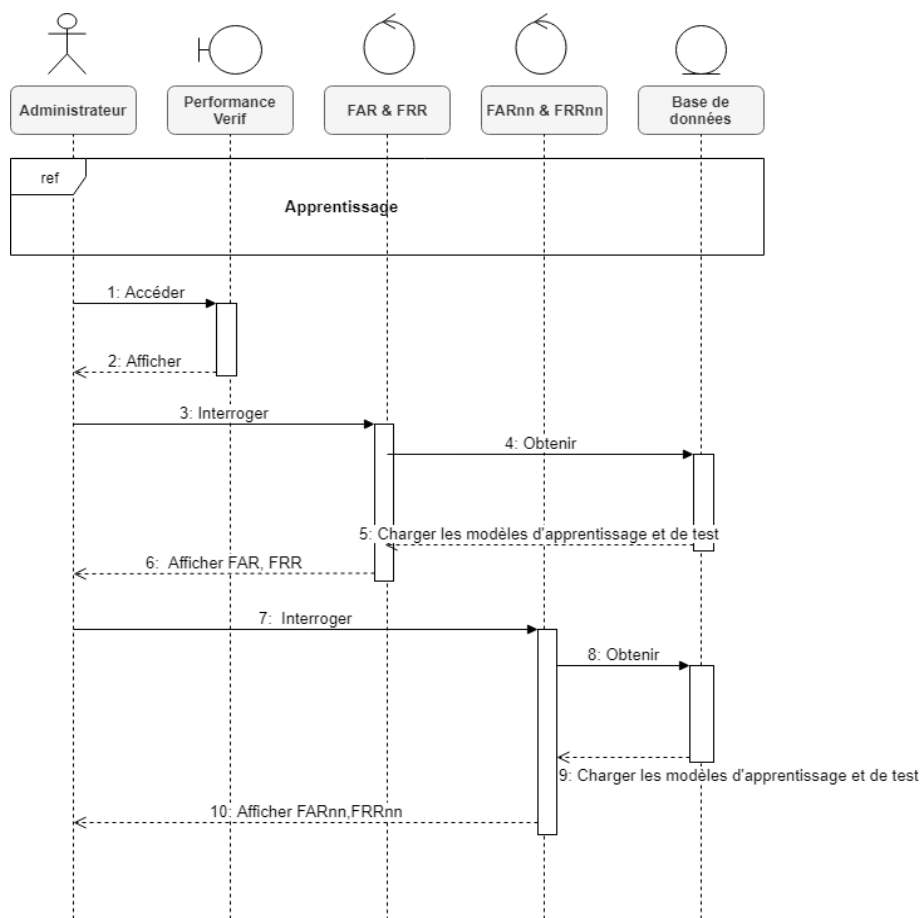


FIGURE 5.3.6 – Diagramme de séquence cas d'utilisation « Vérification ».

Description du scénario performance vérification :

1. L'administrateur choisi la configuration.
2. La sélection de la base de données pour faire les tests.
3. Chargement des modèles d'apprentissage et de teste déjà enregistrés.

4. La mesure des performances du système : le calcul du FAR, FRR, FARnn, FRRnn et Seuil pour la configuration choisie.
5. Affichage des résultats : FAR, FRR, FARnn, FRRnn .

5.3.5 Architecture et fonctionnement du système

Tous les systèmes de reconnaissance de visages qui ont été développés intègrent globalement la même procédure de traitement composée de deux étapes : l'apprentissage et l'extraction de paramètres, la reconnaissance et la prise de décision. Le schéma suivant illustre le fonctionnement de notre système :

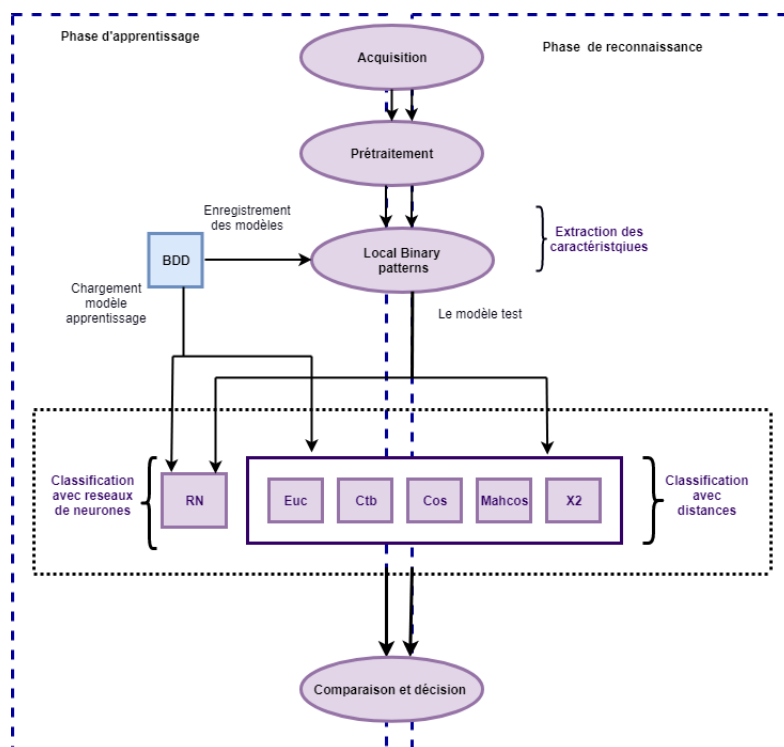


FIGURE 5.3.7 – Diagramme de fonctionnement du système

Dans ce qui suit nous définirons les modules qui constituent chaque unité, ainsi que les algorithmes utilisés, enfin le calcul des performances du système.

5.3.5.1 L'Apprentissage

Le processus d'apprentissage est illustré ci-dessous (Figure 5.8) et les différents modules qui le composent sont détaillés par la suite :



FIGURE 5.3.8 – Représentation modulaire de la phase apprentissage

5.3.5.2 Module prétraitement :

Il est utilisé pour éliminer le bruit dans l'image choisie.



TABLE 5.1 – Représentation de l'étape prétraitement

5.3.5.3 Module extraction des paramètres :

L'extraction des paramètres est une phase importante dans un système de reconnaissance de visage. Elle permet d'extraire les caractéristiques pertinentes de chaque image de visage, ces caractéristiques sont propres à chaque individu et varie d'une personne à une autre. L'extraction des caractéristiques est appliquée par l'approche LBP uniforme.

Dans la figure ci dessous nous illustrons les étapes d'extraction de paramètres :

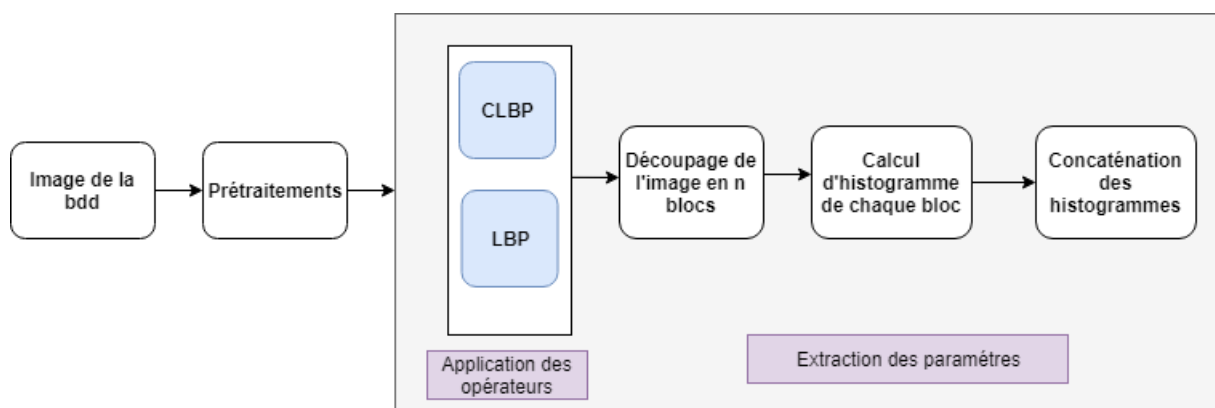


TABLE 5.2 – Module Extraction de paramètres

1. Algorithme du calcul de l'opérateur LBP :

Le calcul du code LBP pour un pixel I [x,y]

Etant donné :

P : le nombre de pixels du voisinage circulaire

CodeLBP : la variable qui va retourner le code LBP d'un pixel I(x,y)

Debut

CodeLBP $\leftarrow$ 0

Faire pour $i \leftarrow 0, \dots, P-1$

Calculer les coordonnées de chaque voisins circulaire

$dx \leftarrow x + \cos(2 * \pi * i / P)$

$dy \leftarrow y + \sin(2 * \pi * i / P)$

Si les cordonnées sont des entiers alors

valeur $\leftarrow$ Image[dx,dy]

Sinon

valeur $\leftarrow$ interpolation_bilinaire(dx,dy)

Fin-si

$S \leftarrow \text{Signe}(\text{valeur} - \text{Image}[y,x])$

CodeLBP $\leftarrow$ CodeLBP + $S * 2^i$

FinPour

TABLE 5.3 – Calcul du code LBP uniforme pour un pixel

2. Algorithme de l'histogramme LBP :

Etant donné :

His : L'histogramme de l'image(vecteur caractéristiques)

P : le nombre de pixels du voisinage circulaire(le nombre de bits du code lbp)

Tab : tableau qui affecte pour chaque valeur uniforme, le numéro de sa case dans l'histogramme uniforme

Z=0 ;

Faire pour $i \leftarrow 0, \dots, 2^P$

Si i est uniforme

Tab[i]=Z ;

Z++ ;

Finsi

1-calcul de l'image LBP

2-découpage de l'image en n blocs

3-pour chaque bloc de l'image

pour $i \leftarrow 0, \dots, 2^P$

Si i est uniforme alors

His[Tab[i]]++ ; nombre de pixels dans le bloc s qui vont contenir la valeur i

TABLE 5.4 – Calcul de l'histogramme LBP uniforme

5.3.5.4 Module de sauvegarde :

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

5.3.5.5 Phase de reconnaissance et la prise de décision

Cette phase vient après l'étape d'apprentissage qui se termine par l'enregistrement des clients dans la base de données et l'étape d'extraction des caractéristiques à l'aide de LBP uniforme, elle consiste à présenter notre méthode de classification basée sur l'application d'un réseau de neurone ou les normes de distances selon les deux modes : Identification ou Authentification (vérification).

Classification par les normes de distances :

Cette phase vient après l'étape d'extraction des caractéristiques, Elle consiste à attribuer au visage l'identité de la personne qui lui ressemble le plus dans l'ensemble d'apprentissage, cette méthode nécessite de choisir une distance .

Classification par les réseaux de neurones :

Un réseau neuronal s'inspire du fonctionnement des neurones biologiques, ce qui permet l'apprentissage et la résolution de problèmes sans algorithme. Réseaux de neurones artificiels est un ensemble de neurones formels interconnectés permettant la résolution de problèmes complexes tels que la reconnaissance des formes ou le traitement du langage naturel. La mise en place du réseau a été effectuée en trois étapes :

1- Préparation de la base d'apprentissage :

Avant de créer le réseau il faut préparer la base de données dans un format accepté par réseau de neurone. Ce dernier prend la base de donnée sous forme de deux matrices :

- Une matrice Inputs contient les modèles de donnée de façon à ce que chaque colonne représente un modèle ; un modèle est un vecteur qui contient les caractéristique, le nombre des caractéristiques varie selon le type du rayon et le nombre de voisinage utilisé pour LBP uniforme .
- Une matrice Targets contient la classe associée à chaque exemple contenu dans Inputs ; cette matrice doit respecter la même disposition que celle de Inputs, c.-à-d. si dans Inputs chaque colonne représente un exemple, alors dans Targets chaque colonne contient le vecteur caractéristique d'un sujet. Pour utiliser un réseau de neurone, toutes les données devient entre -1 et 1, ou bien entre 0 et 1, c'est-à-dire que toute valeur en dehors de ces intervalles doit être normalisée. On a utilisé donc l'instruction suivante :

$$an_i = \frac{2(a_i - a_{min})}{a_{max} - a_{min}} - 1$$

Où :

$[a_{min}, a_{max}]$: intervalle d'origine

a_i :valeur à normaliser dans l'intervalle $[-1,1]$

an_i : valeur normalisée

2- Réalisation de notre réseau :

On crée notre premier réseau de neurone avec des paramètres aléatoires avec le code suivant, et on variera ces paramètres prochainement dans l'évaluation du système jusqu'au on obtient un réseau performant.

```

Programme réseau de neurones
function [ net ] = test_neurone( P, T )
inputs = P;
targets = T;
[ R, Q ] = size( inputs );
[ S2, Q ] = size( targets );
S1 =100;
net = newff( minmax( inputs ), [ S1, S2 ], { 'tansig', 'tansig' },
'traingda' );
net.LW{ 2, 1 } = net.LW{ 2, 1 } * 0.01;
net.b{ 2 } = net.b{ 2 } * 0.01;
net.trainParam.showWindow = false;
net.performFcn = 'mse';
net.trainParam.goal = 0.000000001;
net.trainParam.show = Inf;
net.trainParam.epochs = 100;
net.trainParam.mc = 0.95;
setdemorandstream(672880951)
[ net, tr ] = train( net,inputs, targets );

```

TABLE 5.5 – Programme du réseau

3- Affinage des paramètres du réseau :

Après plusieurs tests expérimentaux (voir chapitre 6) dans les deux modes identification et authentification, on a trouvé que l'utilisation de d'un réseau de neurone sur la méthode LBP uniforme donne un bon résultat voire un TID de 88%. On fixe notre réseau alors comme suit :

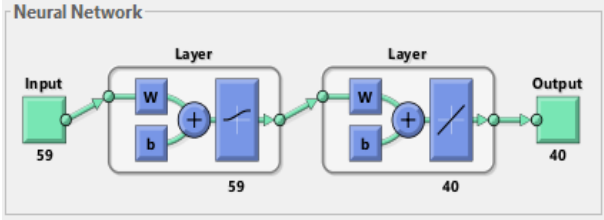
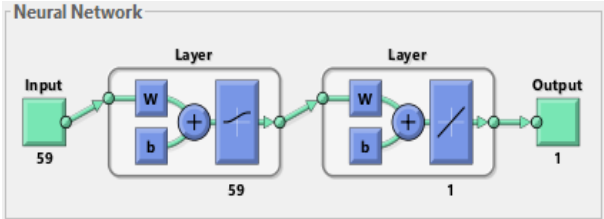
Nom du réseau :	Perceptron Muli couche	
Structure :	identification	
	authentification	
Type :	Feed forwad	
Couche neurale :	1 couche d'entrée 1 couche de sortie 1 couche cachée	
Nombre de neurones dans la couche d'entrées :	La couche d'entrée est composée de 59 neurones, chaque neurone permet d'introduire un seul caractéristique au réseau et nous avons 59caractéristiques avec la méthode LBP(2,8) pour une division d'un seul bloc (voir chapitre 6).	
Nombre de neurones de la couche de sortie :	La couche de sortie est composée de 40 neurones pour l'identification elle représente les 40 classe de visage et 1 neurone pour authentification.	
Nombre de neurones dans la couches cachée :	59 neurones (voir chapitre 6)	
Type de donnée d'entrée	Normaliser ; entre -1 et 1	
Fonction (ou méthode) d'apprentissage :	C'est un algorithme de retro-propagation du descendant gradient avec taux d'apprentissage adaptatif	
Fonction de transfert :	La couche cachée : Sigmoïde tangente hyperbolique (tansig) La couche de sortie : Sigmoïde tangente hyperbolique (tansig)	
Mesure de performance :	La mesure utilisée pour la performance est la MSE (Mean Squared Error ou erreur quadratique moyenne)	
Taux d'apprentissage :	0.01(voir chapitre 6)	

TABLE 5.6 – Tableau capitulatif des paramètres du réseau neuronal utilisé¹¹¹

Identification

Cette étape consiste à choisir l'identité correcte d'une personne inconnue parmi des identités sauvegardées au préalable dans une base de données. On l'appelle « un parmi plusieurs », parce que le système doit accomplir une comparaison entre le modèle de l'individu test et tous les modèles sauvegardés dans la base de données. Le système peut soit prendre la « meilleure » ressemblance, soit donner tous les utilisateurs possibles qui conviennent et les ordonnées par ordre de similarité.

Authentification

Cette méthode consiste à vérifier si une personne est vraiment celle qui prétend être. On l'appelle « un à un », comme le système doit accomplir une comparaison entre le modèle de l'individu test et un seul modèle choisi enregistré dans la base de données.

5.3.6 Calcul des performances du système

Ce module a pour objectif de présenter les techniques de calcul des indices de performance et sur lesquelles le système pourra être jugé meilleur et fiable ou non, en jugeant aussi 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. Donc, TID est le rapport entre le nombre de clients correctement identifiés et le nombre total des clients enregistrés dans la base donnée multipliés par 100.

$$\text{TID} = \frac{\text{Nombre de clients correctement identifiés}}{\text{Nombre total des clients}} * 100$$

Ainsi, plus le TID est proche de 100, plus le système est performant (d'où la configuration est intéressante).

2. Mode vérification :

Pour mesurer les performances d'un système de reconnaissance des visages opérant en mode vérification on s'intéresse au taux de faux rejet (TFR) et taux de fausse acceptation (TFA).

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

vérification.

Le seuil a été fixé au point de convergence c'est à dire où $FRR = FAR$.

Le taux de faux rejet (FRR) est le rapport entre le nombre de faux rejets et le nombre total de test clients. 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 ← Faux_rejet + 1
Fin si
FRR ← (Faux_rejet / nbr_Test_intra) × 100
Fin pour

```

TABLE 5.7 – Calcul du FRR

Le taux de fausse acceptation (FAR) est le rapport entre le nombre de fausses acceptations et le nombre total des tests imposteurs. 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 si
FAR ← (Fausse_acceptation / nbr_Test_extra) × 100
Fin pour

```

TABLE 5.8 – Calcul du FAR

5.4 Implémentation et Réalisation

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

5.4.1 Outils de test et 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 Matlab.

5.4.1.1 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. C'est un langage de calcul scientifique de haut niveau et un environnement interactif pour le développement d'algorithmes, la visualisation et l'analyse de données, ou encore le calcul numérique. C'est un environnement puissant, performant et complet en plus de sa disponibilité assurée sur plusieurs plateformes. Il est ouvert et programmable qui permet de remarquables gains de productivité et de créativité.

Le langage MATLAB met à la disposition du développeur les opérations vectorielles et matricielles, fondamentales pour les problèmes d'ingénierie et scientifiques. Il permet un développement et une exécution rapide par rapport aux langages de programmation traditionnels, car il n'est pas nécessaire d'effectuer les tâches de programmation de bas niveau, comme la déclaration des variables, la spécification des types de données et l'allocation de la mémoire. Matlab Contient également une interface graphique puissante. Ce qui prouve son utilisation dans différents domaines tels que l'éducation, la recherche et l'industrie. Nous avons implémenté le système de reconnaissance de visage dans l'environnement de programmation MATLAB 2018 qui offre une grande simplicité de manipulation des images. Ce langage possède des avantages très intéressants pour les applications sur l'image tel que :

1. La portabilité de logiciel (simplifie le processus de programmation sous Windows).
2. L'utilisation des bases de données.
3. Facilité de manipulation des matrices ce qui est fort important dans le cas de notre application.
4. Un large choix de bibliothèques qui prennent en charge tous les outils mathématiques utiles au traitement et à l'analyse des images.

5.4.2 L'implémentation de notre système :

5.4.2.1 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.

Interface apprentissage :

The screenshot shows the 'Facerecognition' application window. The 'Apprentissage' tab is active. On the left, there are three sections: 'Base de données' with a 'Choisir BDD' button and an 'ORL' dropdown; 'Extraction des caractéristiques' with a 'Choisir une méthode' button, an 'LBP(2,4)' dropdown, and a 'Nombre de sujets' dropdown set to '40'; and 'Classification' with a 'Choisir une distance' button and an 'Euclidienne' dropdown. The main area has a top bar with tabs: 'Apprentissage', 'Prétraitement', 'Identification', 'Authentification', 'Performance Idem', and 'Performance Verif'. Below this, there are two buttons: 'Apprendre' and 'Apprentissage' (highlighted with a blue border). A large grey box contains the results: 'Résultat d'apprentissage' with 'Apprentissage réussi', 'Temps d'apprentissage' with '00:00:33.02', and 'Nombre de blocs' with 'quatre bloc'. On the right, there are two sections: 'Paramètres RN' with 'Nombre de neurones' (50), 'Taux d'apprentissage' (0,01), and 'Nombre d'itérations' (100); and 'Division en blocs' with 'Nombre de blocs' (4).

TABLE 5.9 – Interface Apprentissage

1. Choix de la base de données.
2. Choix du nombre de blocs(1,4,16)
3. nombre du sujet dans la base de données (1 à 40).
4. Choix de méthode d'extraction (LBP^U , $CLBP^U$).
5. Résultat d'apprentissage.
6. Temps d'exécution de la phase apprentissage

Interface performance Identification :

pour TID avec les distances :

The screenshot shows the 'Facerecognition' application window. The 'Identification' tab is active. The left sidebar has three sections: 'Base de données' with a 'Choisir BDD' dropdown set to 'ORL'; 'Extraction des caractéristiques' with 'Choisir uen methode' set to 'LBP(2,8)' and 'Nombre de sujets' set to '18'; and 'Classification' with 'Choisir une distance' set to 'Cosine'. The main area shows two rows of performance data. The first row, labeled 'TID', shows a 'Taux d'identification' of 92 and a 'Temps d'identification' of 00:04:39.79. The second row, labeled 'TID NN', shows a 'Taux d'identification' of 90 and a 'Temps d'identification' of 00:00:25.04. The right sidebar has 'Paramètres RN' with 'Nombre de neurones' set to 500, 'Taux d'apprentissage' set to 0.30, and 'Nombre d'iterations' set to 50. Below it, 'Division en blocs' has 'Nombre de blocs' set to 16.

TABLE 5.10 – Interface performance identification

1. Choix nombre du sujet dans la base de données (1 à 40).
2. Choix de la distance (euclidienne, norme CTB, cosine, mahcos, sqr).
3. Choix de la base de données.
4. Choix du nombre de blocs(1,4,16).
5. Choix de méthode d'extraction (LBP^U , $CLBP^U$).
6. Taux d'identification (TID)
7. Temps d'exécution de taux d'identification

pour TID avec le réseau de neurone :

1. Choix nombre du sujet dans la base de données (1 à 40).
2. Choix du taux d'apprentissage.
3. Choix du nombre d'itérations.
4. Choix du nombre de neurones.
5. Choix de la base de données.
6. Choix de méthode d'extraction (LBP^U , $CLBP^U$).
7. Taux d'identification (TID).
8. Temps d'exécution de calcul de performance d'identification.

Interface performance vérification :

The screenshot shows the 'Facerecognition' application window. The 'Performance Verif' tab is active. The left sidebar has three sections: 'Base de données' (Choose BDD: ORL), 'Extraction des caractéristiques' (Choose uen methode: LBP(1,16), Number of subjects: 38), and 'Classification' (Choose une distance: mahcos). The main area shows two rows of performance metrics. The first row is for 'FRR&FAR' with 'Taux de faux rejet' (23.8), 'Taux de fausse acceptation' (26.5385), and 'Temps d'exécution' (00:00:00.54). The second row is for 'FRR&FAR NN' with 'Taux de faux rejet' (20.2), 'Taux de fausse acceptation' (20.5128), and 'Temps d'exécution' (01:33:19.43). The right sidebar has 'Paramètres RN' (Number of neurons: 500, Learning rate: 0.01, Number of iterations: 50) and 'Division en blocs' (Number of blocks: 1).

Méthode	Taux de faux rejet	Taux de fausse acceptation	Temps d'exécution
FRR&FAR	23.8	26.5385	00:00:00.54
FRR&FAR NN	20.2	20.5128	01:33:19.43

TABLE 5.11 – Interface vérification

pour FAR, FRR avec les distances :

1. Choix nombre du sujet dans la base de données (1 à 40).
2. Choix de la distance (euclidienne, norme CTB, cosine, mahcos, sqr).
3. Choix de la base de données.
4. Choix du nombre de blocs(1,4,16).
5. Choix de méthode d'extraction (LBP^U , $CLBP^U$).
6. Taux de faux rejet (FRR).
7. Taux de fausse acceptation (FAR).
8. Temps d'exécution de calcul de performance vérification.

pour FAR, FRR avec le réseau de neurone :

1. Choix nombre du sujet dans la base de données (1 à 40).
2. Choix du taux d'apprentissage.
3. Choix du nombre d'itérations.
4. Choix de nombre de neurones.
5. Choix de la base de données.

6. Choix de méthode d'extraction (LBP^U , $CLBP^U$).
7. Taux de faux rejet (FRR).
8. Taux de fausse acceptation (FAR).
9. Temps d'exécution de calcul de performance vérification.

Interface identification :

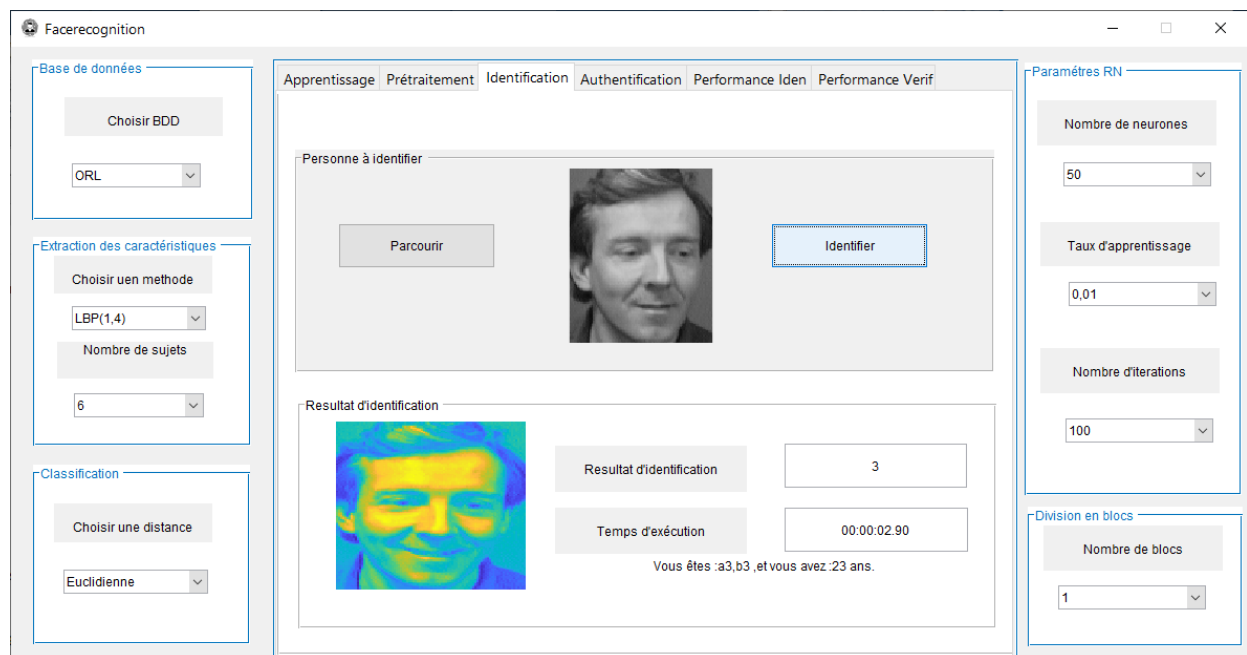


TABLE 5.12 – Interface identification

1. Choix de la base de données.
2. choix du .
3. choix des paramètres du réseau.
4. Chargement de l'image de l'individu test (personne à identifier).
5. Image de la personne à identifier.
6. Image de la personne identifiée.
7. Résultat d'identification (identifiant client).
8. Temps d'exécution de la phase identification.
9. Les informations personnelles de la personne identifiée.

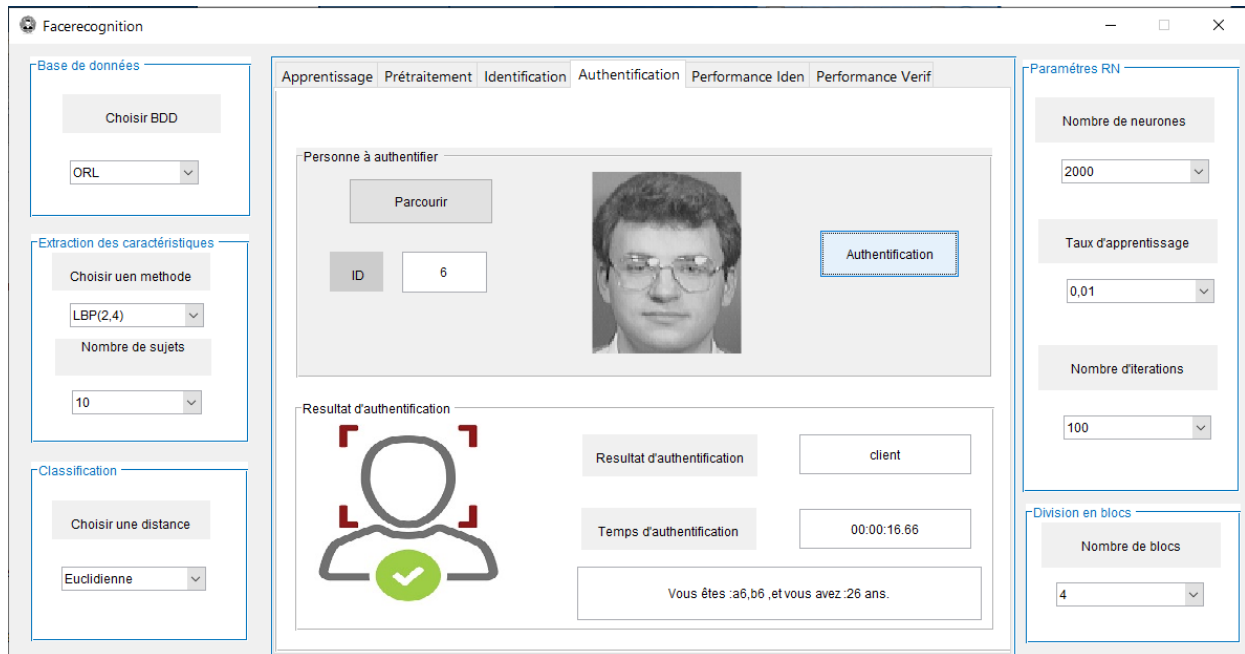
Interface authentication :

TABLE 5.13 – Interface authentication

1. Choix de la base de données.
2. choix du sujet.
3. choix des paramètres du réseau.
4. Chargement de l'image de la personne à vérifier.
5. Choix de l'identifiant.
6. Image de la personne à vérifier.
7. Résultat de la vérification (client ou imposteur).
8. Temps d'exécution de la phase vérification.
9. Les informations personnelles de la personne à vérifier.

Interface Prétraitement :

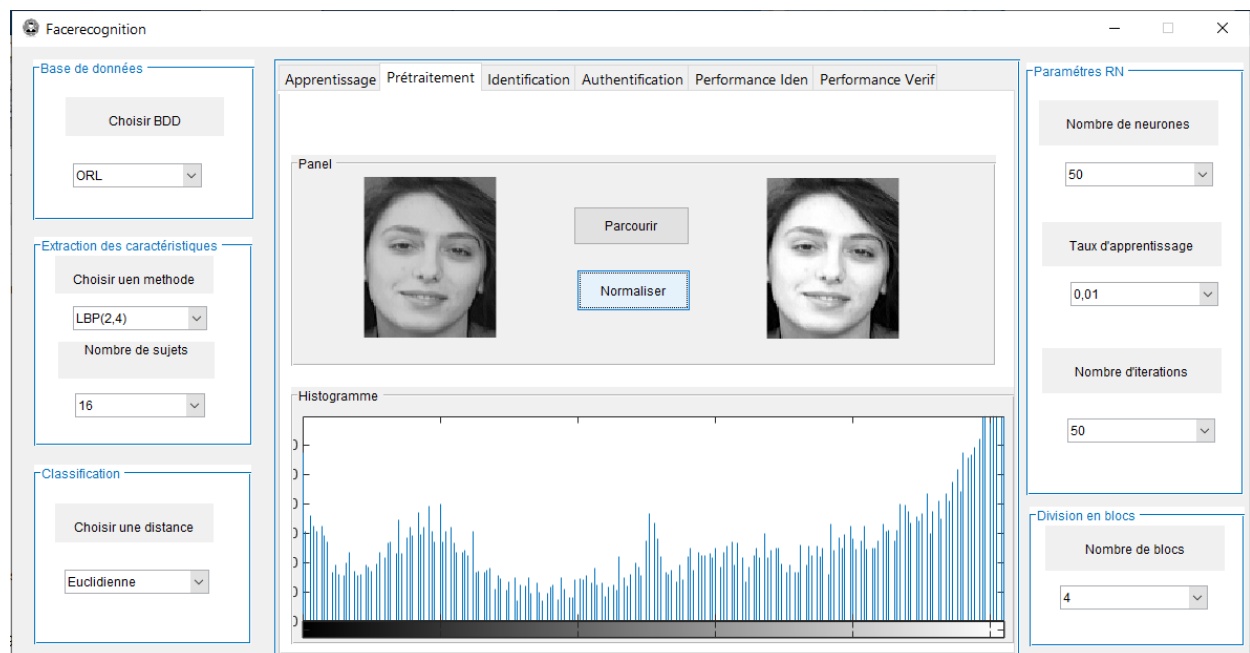


TABLE 5.14 – Interface Prétraitement

1. Parcourir une image.
2. L'image avant la normalisation.
3. La normalisation de l'image.
4. L'image après la normalisation.
5. Afficher l'histogramme de l'image prétraité (niveau de gris entre 0 et 255).

5.5 Conclusion

A travers ce chapitre, nous avons vu les étapes de la conception et la réalisation de notre système biométrique, sa représentation modulaire et aussi les outils de développements utilisés pour l'implémenter, dans le chapitre suivant nous allons voir les tests et les résultats obtenus par ce système.

Chapitre 6

Test et évaluation des résultats

6.1 Introduction

Dans le but d'atteindre notre objectif qui est la réalisation d'un système biométrique fiable, l'obtention d'une bonne classification est essentielle. Nous évaluerons dans ce chapitre les résultats et tests obtenus sur la base de données ORL sous différents paramètres des méthodes décrites précédemment à savoir (LBP uniforme et les réseaux de neurones).

On exposera l'influence de ces dernières sur la performance de notre système à travers un ensemble de tests effectués pour les deux modes de reconnaissance : identification et vérification.

6.2 La base de données ORL

Pour évaluer l'efficacité des méthodes décrites dans les chapitres précédents , nous avons opté pour une validation sur des bases de données standard ORL (Olivetti Research Laboratory). La base de données ORL est constituée de 40 individus, chaque individu possède 10 poses, donc la base contient 400 images. Les poses ont été prises sur des intervalles de temps différents pouvant aller jusqu'à trois mois. Les images sont de dimensions (112×92) pixels.

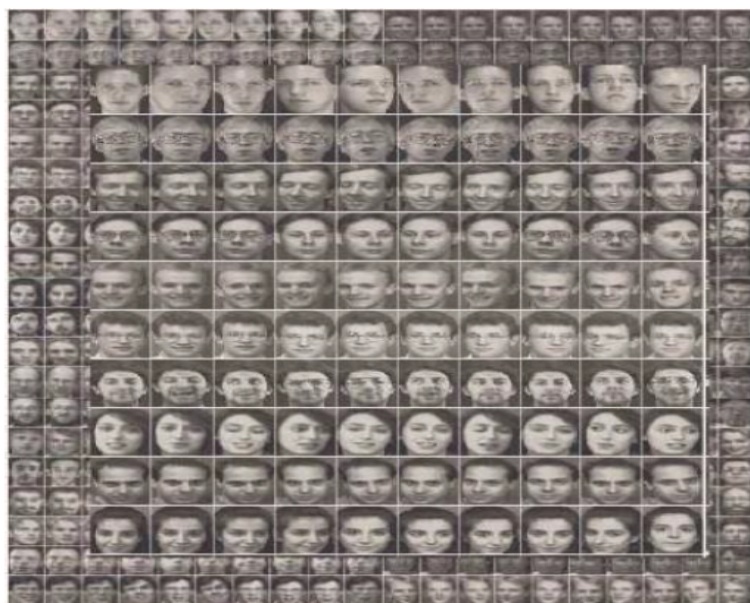


FIGURE 6.2.1 – Base de données ORL[Ahmed 15]

Les images ont été collectées à des dates différentes, avec des variations dans les conditions d'éclairage, les expressions faciales (expression neutre, sourire et yeux fermés) et des occultations partielles par les lunettes.

Voici un exemple où l'acquisition se fait sous différentes orientations du visage :



FIGURE 6.2.2 – Exemple de changements d'orientations du visage

Voici un exemple où l'acquisition se fait sous différents éclairages :



FIGURE 6.2.3 – Exemple de changements d'éclairage

La base de données ORL prend aussi en considération les expressions faciales, telles que les grimaces. En voici un exemple :



FIGURE 6.2.4 – Exemple de changements des expressions faciales

La Base ORL prend en compte le fait qu'un individu peut porter ou ne pas porter des lunettes. Cet exemple en est l'illustration :

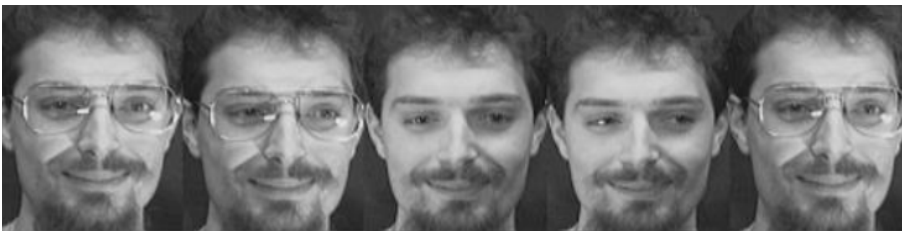


FIGURE 6.2.5 – Exemple de port de lunettes

Un individu peut aussi porter une barbe ou changer de coiffure, la base ORL prend en considérations ces particularités :



FIGURE 6.2.6 – Exemple de changements de coiffure et de port de barbe

Nous avons partitionnée notre base donnée en deux sous bases de 200 images chacune l'une pour l'apprentissage et l'autre 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 ces deux modes.

6.3 Evaluation du système

Dans cette section on présentera l'influence des différents paramètres d'extraction et de classification par métriques de distance et réseau de neurone sur la performance du système.

Le système a été soumis à une série de tests en ses deux modes (identification et vérification) avec différents paramètres de configurations suivant l'approche d'extraction de paramètre « LBP » et ses variantes. Ceci avec les différentes distances de classification à savoir (Euclidienne, Mahalcos, Cosine, Chi-carrée X2 et la norme l_1) ainsi avec un réseau neuronal MLP 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 LBP** : On a utilisé comme indiqué précédemment les 5 premières images de chaque personne pour générer leurs modèles suivant l'algorithme LBP uniforme (avec le choix de variante à appliquer et le rayon à appliquer) défini dans le chapitre 3, il en résulte au final 200 modèles représentatifs de ces personnes.
- **Classification par les réseaux de neurones** : Ceci avec les différents paramètres du réseau neuronal à savoir : nombre de neurones dans la couche cachée, nombre d'itérations et taux d'apprentissage, dans le but de faire une étude comparative des différentes configurations. Pour tester un paramètre du réseau neuronal, nous fixons le reste des paramètres à des valeurs jugées raisonnables, nous faisons ensuite varier ce paramètre et nous réexécutons le programme. Afin de comparer les résultats, nous relevons à chaque fois les mesures suivantes :

Taux d'identification (TID) : le pourcentage des personnes bien reconnues.

Taux Faux rejet (FRR) : le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.

Taux Fausse acceptation (FAR) : le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

6.3.1 Évaluation de la première approche en utilisant le classifieur basé sur les métriques de distances

1. Paramètres fixes :

- le nombre d'image pour l'apprentissage :5 images pour chaque personne.
- le nombre d'image test :5 images pour chaque personne.
- Base de donnée ORL.
- Nombre de sujets pour l'apprentissage : de 1 à 40.

2. Paramètres variables :

- LBP uniforme et ses variantes : " LBP^U_4 ", " LBP^U_8 ", " LBP^U_{16} ", " $CLBP^U_8$ ".
- Le rayon : deux rayons (rayon 1, rayon 2).
- Nombre de blocs : 1 bloc(112*92), 4 blocs(52*46), 16 blocs(28*23).

Dans ce qui suit, on exposera les différents tests effectués sur la base de données ORL. Dans les deux modes identification et authentification (vérification) avec les métriques distances ;

6.3.1.1 Mode identification

1. Mode identification pour 1 bloc(112*92)

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP^U	Rayon1	Voisinage 4	69	68	68.5	68.5	68
		Voisinage 8	72	79	74.5	74.5	72
		Voisinage 16	67	80.5	75.5	75.5	69
$CLBP^U$		Voisinage 8	71	80	71	71	71
LBP^U	Rayon2	Voisinage 4	77	78	77.5	77.5	77
		Voisinage 8	79	82.5	82	82	79
		Voisinage 16	67.5	84.5	81.5	81.5	66.5
$CLBP^U$		Voisinage 8	80.5	80	80	80	80.5

TABLE 6.1 – Variation du taux d'identification TID (%) en fonction des variantes LBP uniforme et les distances pour un bloc

A travers ce tableau, on s'aperçoit que l'on atteint les meilleures performances en terme de taux d'identification (TID) avec la méthode de classification par métrique de distance Ctb par rapport aux autres méthodes, et cela quelque soit le type de LBP uniforme utilisée notamment $LBP^U(2,16)$ ou on a trouvé le TID le plus élevé (84.5%) lorsque le nombre de points P de voisinage augmente de 4 à 16 points et le rayon augmente de 1 à 2 , on explique ce résultat par la meilleur représentation de la texture à mesure que P augmente.

2. Mode identification pour 4 blocs (56*46)

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	84.5	85	85	85	82
		Voisinage 8	85.5	89.5	85.5	85.5	87
		Voisinage 16	83	90	87	87	83.5
CLBP ^U		Voisinage 8	85.5	91	85.5	85.5	85.5
LBP ^U	Rayon2	Voisinage 4	88	89.5	88.5	88.5	89
		Voisinage 8	89	92	92.5	92.5	91.5
		Voisinage 16	82.5	91.5	87	87	82
CLBP ^U		Voisinage 8	89.5	94.5	90	90	89.5

TABLE 6.2 – Variation du taux d'identification TID (%) en fonction des variantes LBP uniforme et les distances pour quatre blocs

A travers ce tableau, on s'aperçoit que l'on atteint les meilleures performances en terme de taux d'identification (TID) après la division en 4 blocs de taille (56*46) pixels avec la méthode de classification par la norme Ctb par rapport aux autres méthodes, et cela quelque soit le type de LBP uniforme utilisée notamment CLBP^U(2,8) ou on a trouvé le TID le plus élevé (94.5%).

Le découpage en blocs de taille (56*46) donne les meilleurs valeurs du TID par rapport au bloc de taille(112*92). Nous expliquons les bon résultats des blocs de tailles (56*46) qui correspondent à un découpage de l'image en blocs[2x2], par le fait que cette configuration correspond à un bon compromis pour le découpage des blocs.

En terme de type de LBP on a constaté à chaque fois le rayon passe de 1 à 2 plus les résultats sont plus satisfaisants on explique ce résultat par l'incorporation de données dans la bordure de l'image. En terme de type de variante on remarque que CLBP^U est meilleur que LBP^U, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

3. Mode identification pour 16 blocs (28*23)

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	91.5	90.5	92	92	90.5
		Voisinage 8	92.5	93.5	92	92	88
		Voisinage 16	90.5	93	90	90	84.5
CLBP ^U		Voisinage 8	92	95.5	92	92	92.5
LBP ^U	Rayon2	Voisinage 4	90.5	92	91	91	90
		Voisinage 8	93	93	91	91	88.5
		Voisinage 16	86.5	94.5	88	88	87
CLBP ^U		Voisinage 8	96	97	96.5	96.5	95.5

TABLE 6.3 – Variation du taux d’identification TID (%) en fonction des variantes LBP uniforme et les distances pour seize bloc

A travers ce tableau, on s’aperçoit que l’on atteint les meilleures performances en terme de taux d’identification (TID) après la division en 16 blocs de taille(28*23) avec la méthode de classification par la norme Ctb par rapport aux autres méthodes, et cela quelque soit le type de LBP utilisée notamment CLBP^U(2,8) ou on a trouvé le TID le plus élevé (97%).

Le découpage en blocs de taille (28*23) donne les meilleurs valeurs du TID par rapport au bloc de taille(112*92) et de (56*46) . Nous expliquons les bon résultats des blocs de tailles (28*23) qui correspondent à un découpage de l’image en blocs[4x4], par le fait que cette configuration correspond à un bon compromis pour le découpage des blocs, en effet les images ORL présente un grande variabilité de posture, aucune normalisation géométriques n’est appliqué pour pallier à ce problème. Des blocs de grandes tailles permettent de diminuer la sensibilité de la méthode LBP uniforme à la posture, mais dégrade la structures texturale de régions hautement discriminantes du visage tel que le nez, les yeux et les narines. Par contre, des blocs de petites tailles, préservent mieux ces informations faciales, mais dégrade la sensibilité de la méthode LBP uniforme à la posture.

En terme de type de LBP uniforme on a constaté à chaque fois le rayon passe de 1 à 2 plus les résultats sont plus satisfaisants on explique ce résultat par l’incorporation de données dans la bordure de l’image. En terme de type de variante on remarque que CLBP^U est meilleur que LBP^U, on explique ceci par le complément d’information contenue dans la CLBP_Magnétude.

6.3.1.2 Mode authentification

1. Mode authentification pour 1 bloc(112*92)

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	24.74	25.64	26.54	26.54	25.83
		Voisinage 8	25.19	24.35	26.35	26.35	28.08
		Voisinage 16	26.99	23.27	25.56	25.56	28.78
CLBP ^U		Voisinage 8	26.79	22.17	28.65	28.65	26.15
LBP ^U	Rayon2	Voisinage 4	24.68	24.87	25.58	25.58	24.23
		Voisinage 8	27	24.49	29.68	29.68	29.36
		Voisinage 16	29.20	25	33.05	33.05	30.96
CLBP ^U		Voisinage 8	23.21	20	28.65	28.65	24.49

TABLE 6.4 – Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage pour un bloc.

A travers les résultats des tests voir (tableau 6.4) ci-dessus on remarque qu'on atteint le taux de fausse acceptation (FAR) le plus bas (20%) avec la méthode de classification par distance de la norme Ctb avec CLBP^U(2,8), 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.

En terme de type de LBP on a constaté que plus le rayon passe de 1 à 2 plus les résultats sont plus satisfaisants on explique ce résultat par l'incorporation de données dans la bordure de l'image. En terme de type de variante on remarque que CLBP uniforme est meilleur que LBP uniforme, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	24.90	25.70	23.70	23.70	25.90
		Voisinage 8	25.20	24.40	26.70	26.70	28.20
		Voisinage 16	27	23.30	29.30	29.30	28.80
CLBP ^U		Voisinage 8	27	22.10	25.90	25.90	27.50
LBP ^U	Rayon2	Voisinage 4	24.70	25	23.80	23.80	25.60
		Voisinage 8	27.10	24.50	27.40	27.40	25.60
		Voisinage 16	27.10	24.50	27.40	27.40	30.30
CLBP ^U		Voisinage 8	23.20	19.80	20.40	20.40	23.40

TABLE 6.5 – Variation du taux des faux rejets FRR (%) en fonction du rayon et voisinage pour un bloc.

A travers les résultats des tests voir (tableau 6.5) ci-dessus on remarque qu'on atteint le taux de faux rejet (FRR) le plus bas (19.80%) avec la méthode de classification par distance de la norme Ctb avec $CLBP^U(2,8)$, d'où elle confirme aussi ses performances en mode authentification.

En terme de type de LBP uniforme on a constaté à chaque fois que le rayon passe de 1 à 2 plus les résultats sont plus satisfaisants on explique ce résultat par l'incorporation de données dans la bordure de l'image. En terme de type de variante on remarque que CLBP uniforme est meilleur que LBP uniforme, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

2. Mode authentification pour 4 blocs(56*46)

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP^U	Rayon1	Voisinage 4	20.38	19.42	19.94	19.94	18.14
		Voisinage 8	21.41	19.62	22.88	22.88	25.96
		Voisinage 16	24.68	19.68	29.10	29.10	28.65
$CLBP^U$		Voisinage 8	18.91	15.45	20.70	20.70	18.56
LBP^U	Rayon2	Voisinage 4	20.06	18.97	18.84	18.84	18.78
		Voisinage 8	21.35	18.01	23.20	23.20	25.13
		Voisinage 16	25.50	19.74	32.37	32.37	29.04
$CLBP^U$		Voisinage 8	17.48	14.42	17.82	17.82	17.31

TABLE 6.6 – Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage pour quatre blocs.

A travers les résultats des tests voir (tableau 6.6) ci-dessus on remarque qu'on atteint le taux de fausse acceptation (FAR) le plus bas (14.42%) après la division en 4 blocs de taille (56*46) avec la méthode de classification par distance de la norme Ctb avec $CLBP^U(2,8)$, d'où elle confirme aussi ses performances en mode authentification.

Le découpage en blocs de taille (56*46) donne les meilleurs valeurs du FAR par rapport au bloc de taille(112*92). Nous expliquons les bon résultats des blocs de tailles (56*46) qui correspondent à un découpage de l'image en blocs[2x2], par le fait que cette configuration correspond à un bon compromis pour le découpage des blocs.

En terme de type de LBP uniforme on a constaté à chaque fois le rayon passe de 1 à 2 plus les résultats sont plus satisfaisants on explique ce résultat par l'incorporation de données dans la bordure de l'image. Par contre une augmentation de FAR dans la majorité des cas à chaque augmentation du voisinage P , ceci peut être du

a une mauvaise représentation de la texture. En terme de type de variante on remarque que CLBP uniforme donne de meilleurs résultats que LBP uniforme, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	20.30	19.30	19.94	19.94	18.20
		Voisinage 8	21.40	19.50	24.60	24.60	26.10
		Voisinage 16	24.60	19.90	28.20	28.20	28.80
CLBP ^U		Voisinage 8	18.90	15.40	18.30	18.30	18.90
LBP ^U	Rayon2	Voisinage 4	20	18.80	19.20	19.20	18.60
		Voisinage 8	21.30	18	23.70	23.70	25.20
		Voisinage 16	25.58	19.80	30.70	30.70	29.10
CLBP ^U		Voisinage 8	17.40	14.50	16.70	16.70	16.90

TABLE 6.7 – Variation du taux des faux rejets FRR (%) en fonction du rayon et voisinage pour quatre blocs.

A travers les résultats des tests voir (tableau 6.7) ci-dessus on remarque qu'on atteint le taux de faux rejet (FRR) le plus bas (14.50%) après la division en 4 blocs de taille (56*46) avec la méthode de classification par distance de la norme Ctb avec CLBP^U(2,8).

Le découpage en blocs[2x2] donne les meilleurs valeurs du FRR par rapport au bloc [1x1]. Nous expliquons les bon résultats des blocs de tailles (56*46) qui correspondent à un découpage de l'image en blocs[2x2], par le fait que cette configuration correspond à un bon compromis pour le découpage des blocs.

En terme de type de LBP uniforme on a constaté à chaque fois le rayon passe de 1 à 2 plus les résultats sont plus satisfaisants on explique ce résultat par l'incorporation de données dans la bordure de l'image. Par contre une augmentation de FAR dans la majorité des cas à chaque augmentation du voisinage P , ceci peut être du a une mauvaise représentation de la texture. En terme de type de variante on remarque que CLBP uniforme est meilleur que LBP uniforme, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

3. Mode authentification pour 16 blocs(28*23)

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	20.96	18.72	19.74	19.74	18.97
		Voisinage 8	19.29	18.08	20.26	20.26	24.04
		Voisinage 16	20.58	18.46	24.42	24.42	26.60
CLBP ^U		Voisinage 8	16.53	14.64	16.28	16.28	15.83
LBP ^U	Rayon2	Voisinage 4	21.41	19.36	19.68	19.68	20.45
		Voisinage 8	20.83	18.91	22.05	22.05	25.06
		Voisinage 16	22.18	22.77	25.83	25.83	25.64
CLBP ^U		Voisinage 8	16.15	14.68	16.47	16.47	16.86

TABLE 6.8 – Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage pour seize blocs.

A travers les résultats des tests voir (tableau 6.8) ci-dessus on remarque qu'on atteint le taux de fausse acceptation (FAR) le plus bas (14.64%) après la division en 16 blocs de taille (28*23) avec la méthode de classification par la norme Ctb avec CLBP^U(2,8).

Le découpage en blocs de taille (28*23) donne des résultats moins meilleurs que celle de bloc de taille (56*46). En terme de type de LBP uniforme on a constaté que à chaque fois que le rayon passe de 1 à 2 le FAR augmente d'un pourcentage allant jusqu'à 7.63% on explique ce résultat par la perte de donnée dans la bordure de l'image. En terme de type de variante on remarque que CLBP uniforme est meilleur que LBP uniforme, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

		Type	Euclidienne	Ctb	Cosine	Mahcos	X2
LBP ^U	Rayon1	Voisinage 4	20.90	18.80	19.20	19.20	18.90
		Voisinage 8	19.30	18	20.40	20.40	23.90
		Voisinage 16	20.50	18.4	24.50	24.50	26.4
CLBP ^U		Voisinage 8	16.50	14.5	16.90	16.90	16
LBP ^U	Rayon2	Voisinage 4	21.40	19.30	19.40	19.40	20.20
		Voisinage 8	20.80	18.70	22.30	22.30	25.20
		Voisinage 16	22.10	20.60	26.90	26.90	25.7
CLBP ^U		Voisinage 8	16.10	14.60	16.90	16.90	16.5

TABLE 6.9 – Variation du taux des faux rejets FRR (%) en fonction du rayon et voisinage pour seize blocs.

A travers les résultats des tests voir (tableau 6.9) ci-dessus on remarque qu'on

atteint le taux de faux rejet (FRR) le plus bas (14.5%) avec la méthode de classification par distance de la norme Ctb avec $CLBP^U(2,8)$.

Le découpage en blocs de taille (28*23) donne des résultats moins meilleurs que celle de bloc de taille (56*46). En terme de type de LBP uniforme on a constaté que à chaque fois que le rayon passe de 1 à 2 le FRR augmente d'un pourcentage allant jusqu'à 7.5% on explique ce résultat par la perte de donnée dans la bordure de l'image. En terme de type de variante on remarque que CLBP uniforme est meilleur que LBP uniforme, on explique ceci par le complément d'information contenue dans la CLBP_Magnétude.

. Synthèse 1

On peut résumer les principaux résultats obtenus sur les tests effectués sur L'ORL :

- Le nombre de point du voisinage P et le rayon R influent sur les performances du système, le voisinage P = 8 et le rayon R = 2 sont un bon compromis entre précision et lourdeur de calcul.
- La métrique de distance Ctb donne de meilleurs résultats par rapport aux autres mesures de distance utilisées.
- La taille des blocs détermine grandement les performances du système, la taille de [28*23] pour la base ORL à donner les meilleurs résultats TID = 97% et la taille de [56*46] à donner les meilleurs résultats FAR = 14,42% et FRR = 14.50.
- Le découpage en blocs de [4x4] gagne en terme d'identification et perd en terme d'authentification.
- La valeur la plus faible obtenue pour le TID (67%) correspond à un découpage de l'image ORL en un seul bloc, l'intégralité de l'image est alors utilisée dans cette configuration pour former le modèle, cette approche correspond aux méthodes globale, ce résultat valide l'appartenance de LBP uniforme aux méthodes locale.
- L'extension uniforme réduit les calculs tout en gardant un pouvoir discriminant élevé.
- La CLBP uniforme complète l'information contenue dans la LBP uniforme.

6.3.2 Évaluation de la deuxième approche en utilisant la classification par réseau de neurone

1. Paramètres fixes :

- le nombre d'image pour l'apprentissage :5 images pour chaque personne.
- le nombre d'image test :5 images pour chaque personne.
- Base de donnée ORL.

-Nombre de sujets pour l'apprentissage : de 1 à 40.

2. Paramètres variables :

- LBP et ses variantes : "LBP^U₄", "LBP^U₈", "LBP^U₁₆", "CLBP^U₈".

-Le rayon : deux rayons (rayon 1, rayon 2).

- nombre de blocs : 1 bloc(112*92), 4 blocs(52*46), 16 blocs(28*23).

-Fonction de transfert (activation) : tansig, logsig, purelin.

-Fonction d'entraînement : traingdx, traingda, trainrp, trainoss, traincgb.

-Nombres de neurones .

- Nombre d'itérations.

- Taux d'apprentissage.

Suivant différentes combinaisons des configurations de paramètres décrits plus haut, les résultats de ces tests en mode identification et authentification sont détaillés comme suit :

6.3.2.1 Variation du paramètre « fonction d'activation »

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Fonction d'entraînement : traingda

Nombre d'itérations = 50

Nombre de neurones de la couche cachée = 50

Ensemble d'apprentissage = 0.01

Voici les résultats jugés meilleurs obtenus en variant les fonctions d'activation avec LBP^U(2,4) :

	Nombre d'itérations=50 Taux d'apprentissage = 0.01 Nombre de neurone=50 Fonction d'apprentissage= traingda											
	Fct transfert= 'tansig' 'tansig'				Fct transfert= 'logsig' 'purelin'				Fct transfert= 'purelin' 'purelin'			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
LBP ^U (2,4)	42.60	42.63	0.9530	14	35.73	35.70	0.9998	37	37.56	37.50	0.9360	30.5

TABLE 6.10 – Résultats du FAR, FRR et TID (%) en variant les fonction d'activation

Afin de fixer les paramètres de notre réseau on a joué sur la variation de la « fonction d'activation » tel qu'on a testé toutes les combinaisons possibles entre tansig, logsig et purelin, tout en laissant les valeurs de la fonction d'entraînement, taux d'apprentissage, nombre d'itérations et le nombre de neurones fixes.

Le tableau ci-dessus montre les meilleurs résultats obtenus. On constate que l'utilisation du couple « logsig, purelin » donne des performances plus acceptable par rapport aux autres ceci en utilisant $LBP^U(2,4)$.

6.3.2.2 Variation du paramètre « fonction d'entrainement »

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Fonction d'activation : logsig, purelin

Nombre d'itérations = 50

Nombre de neurones de la couche cachée = 50

Ensemble d'apprentissage = 0.01

Voici les résultats jugés meilleurs obtenus en variant les fonctions d'entrainement avec $LBP^U(2,4)$:

	Nombre d'itérations=50 Taux d'apprentissage = 0.01 Nombre de neurone=50 Fonction de transfert= 'logsig', et 'purelin'											
	Fct apprentissage= traingda				Fct apprentissage= trainrp				Fct apprentissage= traingcb			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
$LBP^U(2,4)$	42.37	42	0.9999	5	42.88	42.80	0.8765	58	37.90	37.80	0.9370	59.5

TABLE 6.11 – Résultats du FAR, FRR et TID (%) en variant les fonction de transfert

Selon les résultats obtenus dans le tableau (6.10) on a fixé la fonction d'activation à « logsig, purelin » et on a laissé les autres paramètres par défaut tout en variant la fonction d'entrainement. Le tableau(6.11) montre que la fonction d'apprentissage « traingcb » nous permet d'avoir de meilleurs performance par rapport a traingda qui est la fonction fixe de notre réseau ainsi que les autres « trainrp, trainoss, traingdx ».

6.3.2.3 Variation du nombre de neurones dans la couche cachée avec LBP uniforme :

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Fonction d'activation : logsig, purelin

Fonction d'entrainement : traingcb

Nombre d'itérations = 50

Taux d'apprentissage = 0.01

Nombre de neurones= 59/48/500

Voici les résultats obtenus en variant le nombre de neurones et le type de LBP uniforme :

	Nombre d'itérations=50 Taux d'apprentissage = 0.01 Fonction de transfert= 'logsig' et 'purelin' Fonction d'apprentissage= traincgb											
	Nombre de neurone=59				Nombre de neurone=48				Nombre de neurone=500			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
LBP ^U (2,4)	45.51	43.70	0.9999	70	42.97	42	0.9999	68.5	35.70	36	0.9999	75
LBP ^U (2,8)	42.56	42.30	0.9999	81.5	36.60	36.20	0.9999	78	30.25	30.10	0.9999	91
LBP ^U (2,16)	37.17	37	0.9999	58	32.50	32.20	0.9999	61	25.90	26.08	0.9999	82
CLBP ^U (2,8)	40.96	40.60	0.9999	83.5	40	36.28	35.50	71	28.52	27.90	0.9999	94

TABLE 6.12 – Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre neurone

On sait qu'il n'existe pas de règle générale mais des règles empiriques pour choisir la taille de la couche cachée. La taille de cette dernière doit être égale : soit à celle de la couche d'entrée, soit à 75% de celle-ci, soit à la racine carrée du produit des nombres dans la couche d'entrée et de sortie. Donc dans notre cas égale 59, 44 ou 48 respectivement et 500 qu'on a choisi après avoir augmenté le nombre de neurones d'une manière aléatoire. On constate effectivement pour cette valeur on obtient de meilleurs résultats par rapport à celle de l'état de l'art. On remarque ainsi qu'avec 500 neurones et CLBP^U(2,8) on atteint les meilleures performances pour le TID, mais pour FAR, FRR les résultats restent peu satisfaisants.

6.3.2.4 Variation du taux d'apprentissage avec LBP uniforme :

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Fonction d'activation : logsig, purelin

Fonction d'entraînement : traincgb

Nombre d'itérations = 50

Nombre de neurones de la couche cachée = 500

Ensemble d'apprentissage = 0.01/0.30/0.90

Voici les résultats obtenus en variant taux d'apprentissage et types de LBP uniforme :

Nombre d'itérations=50 Nombre de neurone=500 Fonction de transfert= 'logsig' et 'purelin' Fonction d'apprentissage= traincgb												
	Taux d'apprentissage = 0.01				Taux d'apprentissage = 0.30				Taux d'apprentissage = 0.90			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
LBP ^U (2,4)	36	35.70	0.9999	75	35.83	3580	0.9976	73	35.96	35.80	0.9730	54.5
LBP ^U (2,8)	30.25	30.10	0.9999	91	30.19	30.10	0.9762	83.5	29.23	29.20	0.7619	14.5
LBP ^U (2,16)	26.08	25.90	0.9999	82	24.35	24.30	0.8517	22	21.60	21.50	0.1254	6.5
CLBP ^U (2,8)	28.52	27.90	0.9999	94	28.26	28	0.9875	72	26.98	26.90	0.9268	8

TABLE 6.13 – Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et taux d'apprentissage

En terme de paramètre de réseau, le taux d'apprentissage est compris entre 0 et 1. Si les poids corrects sont loin des poids initiaux il est bien de choisir un taux d'apprentissage proche de 1 pour qu'ils convergent assez rapidement . Si ces derniers sont proches des poids initiaux il est bien de choisir un taux d'apprentissage proche de 0 pour ne pas les rater. A travers les résultats des tests (tableau 6.13) on constate que le meilleur taux d'apprentissage est 0.01.

En terme de type de LBP uniforme les meilleures performances de FAR, FRR et TID, on les obtient avec CLBP^U(2,8).

6.3.2.5 Variation du nombre d'itérations avec LBP uniforme

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Fonction d'activation : logsig, purelin

Fonction d'entraînement : traincgb

Taux d'apprentissage = 0.01

Nombre de neurones de la couche cachée = 500

Nombre d'itérations =50/100/500

Voici les résultats obtenus en variant le nombre d'itération et le type de LBP uniforme :

	Nombre de neurone=500 Taux d'apprentissage = 0.01 Fonction de transfert= 'logsig' et 'purelin' Fonction d'apprentissage= traincgb											
	Nombre d'itérations=50				Nombre d'itérations = 100				Nombre d'itérations = 500			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
$LBP^U(2,4)$	35.70	36	0.9999	75	35.70	36	0.9999	77	35.70	36	0.9999	75
$LBP^U(2,8)$	30.25	30.10	0.9999	91	30.25	30.10	0.9999	93	30.25	30.10	0.9999	91
$LBP^U(2,16)$	25.90	26.08	0.9999	82	25.90	26.08	0.9999	80.5	25.90	26.08	0.9999	82
$CLBP^U(2,8)$	28.52	27.90	0.9999	94	28.52	27.90	0.9999	90	28.52	27.90	0.9999	89.5

TABLE 6.14 – Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre d'itération

A travers les résultats des tests (tableau 6.14), on remarque en terme de paramètre de réseau, le nombre d'itérations n'influence pas sur les performances FAR et FRR, pour TID on remarque une légère amélioration quand le nombre d'itérations égal a 50. En terme de type LBP uniforme, $CLBP^U(2,8)$ atteint le FAR et FRR les plus bas 28,52, 27.90 respectivement, et un excellent TID de 94%.

Après un ensemble important de tests sur ce protocole qui dépend de l'approche LBP uniforme et ses variantes, les meilleurs résultats obtenus sont : FAR=28.52, FRR=27.90 et TID=94. Cela avec les paramètre qui suit :

-La méthode LBP :

" $LBP^U(2,4)$ ", " $LBP^U(2,8)$ ", " $LBP^U(2,16)$ " et " $CLBP^U(2,8)$ "

Paramètre de reseau de neurone :

- Taux d'apprentissage :0.01

- Nombre de neurone : 500 neurones

- Nombre d'itération : 50 itérations

Mais les résultats de FAR et FRR obtenus restent peu satisfaisants, pour cela on a opté pour une deuxième phase de test tel que on a essayer de fixer nos paramètres d'une autre manière afin d'améliorer nos résultats.

6.3.3 Amélioration des résultats obtenus en terme d'authentification

6.3.3.1 Variation du nombre de neurones dans la couche cachée :

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Nombre d'itérations = 50

Taux d'apprentissage = 0.01

Voici les résultats obtenus en variant le nombre de neurones et le type de LBP uniforme

	Fonction d'apprentissage = 'traingda' Fonction de transfert= 'tansig' 'tansig' Nombre d'itérations=50 Taux d'apprentissage = 0.01											
	Nombre de neurones=50				Nombre de neurones=500				Nombre de neurones=2000			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
LBP ^U (1,4)	43.14	43.10	0.95718	14	45.19	42	0.9572	31	43.40	43.20	0.9573	49.5
LBP ^U (2,4)	42.63	42.60	0.95302	14	43.33	42.30	0.95303	34	42.24	43	0.9531	60.5
LBP ^U (1,8)	26.86	26.79	0.9568	6	26.47	26.40	0.9566	32	26.54	26.50	0.9567	70.5
LBP ^U (2,8)	26.93	26.95	0.9524	11.5	26.82	26.79	0.9523	35.5	25.71	25.60	0.9524	84.5
LBP ^U (1,16)	22.18	22.03	0.8918	10.5	21.89	21.85	0.8919	12.5	21.60	21.60	0.8921	72.5
LBP ^U (2,16)	26.88	26.87	0.8960	8	26.74	26.62	0.8961	23	21.47	21.40	0.8963	88
CLBP ^U (1,8)	26.65	26.64	0.9598	10.5	26.68	26.63	0.9598	33	26.40	26.40	0.9599	79
CLBP ^U (2,8)	24.84	24.73	0.9551	12.5	24.39	24.30	0.9551	46.5	24.42	24	0.9552	87

TABLE 6.15 – Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre neurone

On sait qu'il n'existe pas de règle générale mais des règles empiriques pour choisir la taille de la couche cachée. Dans notre cas on a opté pour 50, 500 ou 2000 respectivement. On constate effectivement que pour ces valeurs on obtient de meilleurs résultats par rapport à d'autre valeurs. On remarque ainsi qu'avec 2000 neurones et le type de LBP (2,16) on atteint les meilleures performances pour FAR, FRR et TID.

6.3.3.2 Variation du taux d'apprentissage avec LBP uniforme :

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Nombre d'itérations = 50

Nombre de neurones de la couche cachée = 2000

Ensemble d'apprentissage = 0.01/0.30/0.90

Voici les résultats obtenus en variant taux d'apprentissage et types de LBP uniforme :

	Fonction d'apprentissage = 'traingda' Fonction de transfert= 'tansig' 'tansig' Nombre d'itération =50 Nombre de neurone = 2000											
	Taux d'apprentissage=0.01				Taux d'apprentissage=0.30				Taux d'apprentissage=0.90			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
LBP ^U (1,4)	43.40	43.20	0.9573	49.5	35.77	35.7	0.9785	43	35.45	35.30	0.9829	32.5
LBP ^U (2,4)	42.24	43	0.9531	60.5	35	34.40	0.9756	56.5	35.96	34.10	0.9799	36.5
LBP ^U (1,8)	26.54	26.50	0.9567	70.5	26.60	26.60	0.9501	66	26.93	26.85	0.9493	38
LBP ^U (2,8)	25.71	25.60	0.9524	84.5	26.06	26.10	0.9335	86	26.15	26.10	0.9249	43
LBP ^U (1,16)	21.60	21.60	0.8921	72.5	21.46	21.40	0.7683	60.5	21.12	21.10	0.7435	47
LBP ^U (2,16)	21.47	21.40	0.8963	88	20.93	20.90	0.7930	78.5	20.95	20.90	0.7782	51
CLBP ^U (1,8)	26.40	26.40	0.9599	79	26.09	25.98	0.9605	74.5	25.89	25.90	0.9613	30.5
CLBP ^U (2,8)	24.42	24	0.9552	87	25.11	25.10	0.9466	87	25.01	24.80	0.9449	34.5

TABLE 6.16 – Variation du FAR, FRR et TID (%) en fonction de type LBP et taux d'apprentissage

En termes de paramètres du réseau, le taux d'apprentissage est compris entre 0 et 1. Si les poids corrects sont loin des poids initiaux il est bien de choisir un taux d'apprentissage proche de 1 pour qu'ils convergent assez rapidement. Si ces derniers sont proches des poids initiaux il est bien de choisir un taux d'apprentissage proche de 0 pour ne pas les rater. A travers les résultats des tests (tableau 6.10) on constate que le meilleur taux d'apprentissage est 0.01. En termes de type de LBP uniforme les meilleures performances de FAR, FRR et TID, on les obtient avec LBP^U (2,16).

6.3.3.3 variation du nombre d'itérations avec LBP uniforme

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Taux d'apprentissage = 0.01

Nombre de neurones de la couche cachée = 2000

Nombre d'itérations =50/100/500

Voici les résultats obtenus en variant le nombre d'itération et le type de LBP uniforme :

	Fonction d'apprentissage = 'traingda' Fonction de transfert= 'tansig' 'tansig' Nombre de neurone =2000 Taux d'apprentissage = 0.01											
	Nombre d'itération=50				Nombre d'itération=100				Nombre d'itération =500			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
LBP ^U (1,4)	43.40	43.20	0.9573	49.5	43.40	43.20	0.9573	49.5	43.40	43.20	0.9573	49.5
LBP ^U (2,4)	42.24	43	0.9573	60.5	42.24	43	0.9531	60.5	42.24	43	0.9531	60.5
LBP ^U (1,8)	26.54	26.50	0.9567	70.5	26.54	26.50	0.9567	70.5	26.54	26.50	0.9567	70.5
LBP ^U (2,8)	25.71	25.60	0.9524	84.5	25.71	25.60	0.9524	84.5	25.71	25.60	0.9524	84.5
LBP ^U (1,16)	21.60	21.60	0.8921	72	21.60	21.60	0.8921	72	21.60	21.60	0.8921	72
LBP (2,16)	21.47	21.40	0.8963	88	21.47	21.40	0.8963	88	21.47	21.40	0.8963	88
CLBP ^U (1,8)	26.40	26.40	0.9599	79	26.40	26.40	0.9599	79	26.40	26.40	0.9599	79
CLBP ^U (2,8)	24.42	24	0.9552	87	24.42	24	0.9552	87	24.42	24	0.9552	87

TABLE 6.17 – Variation du FAR, FRR et TID (%) en fonction de type LBP uniforme et nombre d'itération

A travers les résultats des tests (tableau 6.12), on remarque en terme de paramètres du réseau que l'augmentation de nombre d'itérations n'influence pas sur les taux de performances. En termes de type de LBP uniforme, LBP^U (2,16) atteint le FAR et le FRR les plus bas 21.47, 21.40 respectivement et atteint le TID le plus élevé où on a trouvé 88%.

6.3.4 Amélioration des performances de notre système en utilisant la division en 16 blocs(28*23)

6.3.4.1 Variation du nombre de neurones dans la couche cachée avec LBP uniforme :

1. Avec fonction d'apprentissage 'traincgb' et la fonction de transfert 'logsig,purelin'

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Taux d'apprentissage = 0.01

Nombre de neurones de la couche cachée = 100, 500, 2000

Nombre d'itérations =50

Voici les résultatsobtenus en variant les fonctions d'activation avec CLBP^U (2,8) :

	Nombre d'itérations=50 Taux d'apprentissage =0.01 Fonction de transfert= 'logsig' et 'purelin' Fonction d'apprentissage= traingcb											
	Nombre de neurone=100				Nombre de neurone=500				Nombre de neurone=2000			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
CLBP ^U (2,8)	19.61	19.40	0.9995	89	20	19.40	0.9992	97.5	20.29	20.10	0.9992	98

TABLE 6.18 – Variation du FAR, FRR et TID (%) en fonction du nombre de neurones

Le tableau (6.18) représente les taux de performance en utilisant un découpage en 16 blocs de taille (28*23) dans

On sait qu'il n'existe pas de règle générale mais des règles empiriques pour choisir la taille de la couche cachée. Dans notre cas on a opté pour un nombre de neurones égale à 100, 500 et 2000 respectivement qu'on a choisi d'une manière aléatoire car l'utilisation des valeurs de l'état de l'art (944, 708 et 194) n'ont pas donnés de bonnes performances. On constate effectivement pour les valeurs utiliser en dessous on obtient de meilleurs résultats par rapport à celle de l'état de l'art. On remarque ainsi qu'avec 2000 neurones et CLBP^U(2,8) on atteint les meilleures performances pour le TID voire 98%, mais pour FAR, FRR les résultats restent peu satisfaisants. Donc on opte pour d'autres variations de paramètres afin d'améliorer les performance en terme d'authentification.

2. Avec fonction d'apprentissage 'traingda' et la fonction de transfert 'tansig,tansig'

Pour tester ce paramètre, nous avons fixé les autres paramètres comme suit :

Taux d'apprentissage = 0.01

Nombre de neurones de la couche cachée = 100, 500, 2000

Nombre d'itérations =50

Voici les résultats obtenus en variant le nombre d'itération et le type de LBP uniforme :

	Nombre d'itérations=50 Taux d'apprentissage =0.01 Fonction de transfert= 'tansig' et 'tansig' Fonction d'apprentissage= traingda											
	Nombre de neurone=100				Nombre de neurone=500				Nombre de neurone=2000			
	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID	FAR	FRR	Seuil	TID
CLBP ^U (2,8)	19.55	19.30	0.9323	20	19.23	19.10	0.9330	68.5	19.23	19.20	0.9297	65

TABLE 6.19 – Variation du FAR, FRR et TID (%) en fonction du nombre de neurones

A travers le tableau (6.19) on remarque une légère amélioration de FAR=19.23 et FRR=19,10 après avoir changer la fonction d'apprentissage en 'traingda' et la fonction de transfert en 'tansig,tansig' en utilisant la variante CLBP^U(2,8) et le découpage en [4x4] blocs.

Synthèse 2

Après ces tests expérimentaux, les meilleurs résultats sont obtenus pour 16 blocs de taille (28*23) :

TID=98, FAR=19.23 FRR=19.10 Cela avec les paramètre qui suit :

Type : CLBP^U(2,8) ,

Paramètre de réseau de neurone :

- Taux d'apprentissage :0.01
- Nombre de neurone : 500 neurone
- Nombre d'itération : 50 itération

1. pour FAR et FRR on a utilisé :

- Fonction d'apprentissage : 'traingda'
- Fonction de transfert : 'tansig,tansig'

2. pour TID on a utilisé :

- Fonction d'apprentissage : 'traincgb'
- Fonction de transfert : 'logsig,purelin'

- Les résultats obtenus dans cette partie montrent que la division en blocs apporte une amélioration de performance en terme d'authentification et d'identification.
- La CLBP uniforme complète l'information contenue dans la LBP uniforme.

6.3.5 Comparaison des résultats :

À travers ces tests effectués dans les deux modes (Identification et vérification), on peut résumer l'effet du choix de LBP uniforme, le choix de nombre de blocs, la classification selon la norme de distance, les paramètres de réseau de neurone à appliquer comme suit :

En utilisant une décomposition de LBP uniforme en blocs les performances augmentent à chaque augmentation de nombre de blocs. Ceci quelque soit le type de LBP uniforme à appliquer et l'approche de classification à utiliser, cela peut être due à l'utilisation seulement de l'information pertinente (concentration d'énergie) c-à-d en se focalisant juste sur les détails de l'image issu de l'application de LBP uniforme.

L'approche de classification par mesure de distance de la norme « Ctb » est particulièrement plus robuste et on a vu à travers les différents tests effectués qu'elle donne de bons résultats. En termes de type de LBP uniforme, $CLBP^U(2,8)$ est le mieux adapté dans le cas d'identification, il nous donne d'excellents performances, voire un TID=97% avec une division en 16 blocs [4x4]. Par contre dans le cas d'authentifications les meilleurs résultats sont obtenus en utilisant $CLBP^U(2,8)$, voire un FAR=14.64 et FRR=14.50 avec une division en 4 blocs [2x2].

En ce qui concerne la classification selon le réseau de neurone, l'utilisation des valeurs d'état de l'art nous a donné de bonnes performances en terme d'identification voire un TID de 94% mais, la variation de paramètres avec un taux d'apprentissage de 0.01, un nombre d'itérations de 50 et 2000 neurones dans la couche cachée, nous a permis d'atteindre de performances plus satisfaisantes en authentification, voire un FAR de 21.47% et un FRR de 21.40% qu'on peut juger assez bons, et ceci en utilisant un bloc. Par contre l'application du réseau neuronal sur une image découpée en 16 blocs de taille (28*23) nous a permis d'atteindre les meilleurs résultats voire un TID de 98% qui est très satisfaisant, FAR=19.23 et un FRR=19.10.

L'utilisation de l'approche 1 basée sur les métriques de distances nous a permis de gagner en terme d'authentification avec un FAR=14.42 et FRR=14.50, en revanche l'utilisation de l'approche 2 basée sur le réseau neuronal nous a permis d'atteindre la meilleure performance en terme d'identification avec un TID de 98%.

Pour conclure, on constate que l'application des réseaux de neurones sur l'approche LBP uniforme apporte une amélioration des performances du système surtout après la division en blocs.

6.3.6 Conclusion

Tout au long de ce chapitre, nous avons effectué des tests expérimentaux sur les différents paramètres constituant notre système. Et enfin, on a utilisé les para-

mètres jugés bons dans la conception du système de reconnaissance de visages.

Conclusion générale et perspectives

Dans ce mémoire, nous avons pu aborder le domaine de la biométrie en étudiant les systèmes biométriques en général, et ceux basés sur le visage en particulier.

En effet, nous avons conçu et réalisé un système de reconnaissance de visages dans ces deux modes (identification et vérification) basé sur l'approche LBP pour l'extraction et la modélisation de paramètres qu'on a choisi parmi toutes les approches existantes et qui reste l'une des approches les plus fiables pour la reconnaissance de visage vu son invariance aux influences des éléments externes, ensuite vient l'étape de la classification où on a opté pour deux méthodes l'une est la méthode de classification dite par mesure de similarité associée à cinq distance (Euclidienne, "Mahalcos", "Cosine", "Chi-carrée X^2 " et la "norme C_{tb} "), dont nous avons constaté la puissance, la robustesse et la simplicité. Et l'autre en utilisant un réseau de neurone MLP (Multi-Layer Perceptron, Perceptron multicouche) tout en variant ses paramètres tel que nombre de neurone dans la couche cachée, taux d'apprentissage et nombre d'itérations qui influencent beaucoup sur les performances du système.

Dans le but d'évoluer et d'améliorer la performance de notre système nous avons opté pour une division de nos images en un nombre différents de blocs.

Dans notre système de reconnaissance, on a fait appel à des tests expérimentaux effectués sur la base de données ORL basés sur l'approche LBP uniforme et CLBP uniforme, pour mesurer sa performance à savoir le taux d'identification (TID) en mode identification et le taux de fausse acceptation (FAR) et le taux de faux rejet (FRR) en mode vérification. A cet effet, les résultats de CLBP uniforme ont été

A travers ce projet nous avons assimilé les concepts principaux de l'opérateur LBP et les distances utilisées pour la classification, les réseaux neuronaux et mieux s'adapter à l'outil Matlab ainsi que ses différentes bibliothèques.

Comme perspective d'améliorations nous proposons :

- Effectuer plusieurs prétraitements afin d'améliorer la qualité de nos images.
- Diviser les images en nombre de blocs plus grand.
- Utilisation d'autres types de réseaux de neurones.
- Lancer d'autres tests sur d'autres variantes de l'approche LBP en augmentant plus le voisinage et le rayon et le nombre de régions.

- Recourir à la multi modalité, en fusionnant la modalité visage avec une autre modalité comme la voix, dans le but d'améliorer la performance de notre système.

Bibliographie

- [A. Houamed 15] A.Hariz A. Houamed. *"Application des Réseaux artificiels des Neurones pour contrôler la tension d'un système photovoltaïque connecté à un Réseau Local"*. 2015.
- [A. Schmitt 01] M.-M. Corsini C. Lafond et J. Bruzek A. Schmitt B. Le Blanc. *"Artificial neural network. A relevant data processing tool for anthropology"*. 2001.
- [abdelhamid] djeflal abdelhamid. *"Réseaux de neurones"*. [www](http://www.abdelhamid.net)
- [Ahmed 15] Ghali Ahmed. *"Amélioration de la reconnaissance par le visage"*. 2015.
- [Amina 16] Medjadji Omar Amina Ben Hamed. *"Reconnaissance des Empreintes Digitales"*. 2016.
- [Antitza] Jean-Luc DUGELAY (EURECOM) Sophia Antipolis Antitza Dantcheva (Inria). *"(en ligne) L'histoire de la biométrie"*. CAFE TECHNO, doctorante EURECOM de 2008 à 2011.
- [Antoine] Cornuéjols Antoine. *"Les réseaux de neurones"*. I.I.E. L.R.I., Université d'Orsay.
- [Attalah 12] Bilal Attalah. *"Conception d'un système de Reconnaissance des empreintes digitales par apprentissage"*. 2012.
- [Bedia 12] cherfi Nadjat Bedia Fatima. *"La vérification automatique de parenté basée sur le visage"*. 2012.
- [Bettahar Abdessettar 14] SABER Fathi Bettahar Abdessettar. *"Extraction des caractéristiques pour l'analyse biométrique d'un visage"*. 2014.
- [Bishop.C 95] Bishop.C. 1995.
- [Bouchra 13] Khelif Bouchra. *"Mise au point d'une application de reconnaissance faciale"*. 2013.

- [C. Fredoville 00] C. Jaboulet J. Hennebert J. F. Bonastre C. Mokbel F. Bimbot C. Fredoville J. Marie thoz. *"Behavior of a Bayesian adaptation method for incremental enrollment in speaker verification"*. 2000.
- [C.Fredouille 06] C.Jaboulet J.Hennebert J.F.Bonastre F.Bimpot C.Fredouille J.Mariethoz. *"adaptation method for incremental enrollment in speaker verification"*. 2006.
- [CHeraa 16] Saadeddine Boucetta Samir CHeraa. *"Etude comparative de quelques mesures de similarité, et leur application à la recherche d'images"*. 2016.
- [Claude 92a] Touzet Claude. *"Les réseaux de neurones artificiels"*. 1992.
- [Claude 92b] Touzet Claude. *"Les réseaux de neurones artificiels, introduction au connexionisme"*. 1992.
- [Céline 13] Briod et Yann Ehmann Céline. *"La biométrie sur Internet"*. 2013.
- [David 08] Panzol David. *"Proposition de l'architecture « Cortexionist » pour l'intelligence comportementale de créations artificielles"*. 2008.
- [Day 09] D Day. *Biometric applications overview*. "Encyclopedia of biometrics", 2009.
- [Deluzarche 06] Céline Deluzarche. *"la biométrie :l'identité par le corp"*. 2006.
- [Douib 16] Oualid Douib. 2016. [www](#)
- [Estelle] Benoit Burg et Lucas Lang Estelle Kiedaisch. *"TPE :Les Empreintes Digitales"*. [www](#)
- [F. Perronnin 03] J. L. Dugelay F. Perronnin & K. Rose. *"Deformable face mapping for person identification"*. 2003.
- [Fiche 12] Cécile Fiche. *"Repousser les limites de l'identification faciale en contexte de vidéo surveillance"*. 2012.
- [Fouad 18] Helal Fouad. *"Identification des personnes par les empreintes digitales"*. 2018.
- [Francis 88] Galton Francis. *"Personnal Identification and Description"*. 1888.
- [Ghoulia 17] Kouidri Ghoulia. *"Etude comparative d'ensemble des descripteurs de texture pour la reconnaissance de visages"*. 2017.

- [Hanane 12] Ouamane Hanane. *"Identification de reconnaissance faciale avec des expressions"*. 2012.
- [Hizem] Walid Hizem. *"Capteur intelligent pour la reconnaissance de visage"*.
- [Ibtissam 16] Benchennane Ibtissam. *"Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus"*. 2016.
- [Isabelle 97] Claude Isabelle. *"The Local Binary Pattern Approach to texture analysis"*. 1997.
- [Ismail 11] Belkhouché Ismail. *"Planification du trajectoire et évitement d'obstacle par les réseaux de neurones pour les robots mobile autonome"*. 2011.
- [Jain 08] A. K. Jain & Ross. A. *"Introduction to biometrics"*. 2008.
- [James G 17] Fujimoto James G. *"Integrated Local Binary Pattern Texture Features for Classification of Breast Tissue Imaged by Optical Coherence Microscopy"*. 2017.
- [John D. 03] Jr. Christopher Horn Julius Gatune John D. Woodward & Aryn Thomas. *"Biometrics A Look at Facial Recognition"*. 2003.
- [Juslin 16] Tshiamua Mudikolele Juslin. *"Mise en oeuvre d'un système distribué pour l'identification et le suivi du casier judiciaire"*. 2016.
- [K. Etemad 97] R. Chellappa K. Etemad. *"Discriminant Analysis for Recognition of Human Face images"*. 1997.
- [Kanade 73] T Kanade. *"Computer recognition of human faces"*. 1973.
- [Karine 09] Volpi Karine. *"Les réseaux de neurones"*. 2009.
- [Kary 13] Främpling Kary. *"Modélisation et apprentissage des préférences par réseaux de neurones pour l'aide à la décision multicritère"*. 2013.
- [Lazarick 08] R. Lazarick & J. L Cambier. *"Biometrics in the government sector"*. 2008.
- [Lynda 09] Selami Lynda. *"Approche Data Mining pour la Détection d'Intrusions"*. 2009.
- [Marc 14] Zaffagni Marc. *"L'odeur corporelle, nouvel outil biométrique ?"*. 2014.

- [Matti 10] Pietikäinen Matti. *"Local Binary Patterns"*. 2010.
- [Mekkani 84] Samia Mekkani. *"Description statistique de la texture"*. 1984.
- [Merzouka 09] Nouressadat Merzouka. *"Les Réseaux de Neurones Artificiels"*. 2009.
- [Mickaël 14] Garnier Mickaël. *"Modèles descriptifs de relations spatiales pour l'aide au diagnostic d'images biomédicales"*. 2014.
- [Midhula 17] Vijayan Midhula. *"Moving Object Detection Using Local Binary Pattern and Gaussian Background Model"*. 2017.
- [MM.Zakaria 17] MM.Zakaria. *"Classification des images avec les réseaux de neurones convolutionnels"*. 2017.
- [Mohamed 07] Bouchaddak Mohamed. *"Conception et Développement d'une application de gestion de temps de travail d'employés dans un parc d'entreprise"*. 2007.
- [Mokri 01] Mohammed Zakaria Mokri. *"Etude prospective des applications possibles des réseaux de neurones formels dans le traitement des données psychométriques"*. 2001.
- [Mokri 17] Mohammed Zakaria Mokri. *"Classification des images avec les réseaux de neurones convolutionnels"*. 2017.
- [Muhammad 03] sarfraz Muhammad. *"The Local Binary Pattern Approach to texture analysis"*. 2003.
- [Nassima 12] Mezhoud Nassima. *"Une approche hybride pour la segmentation d'images Application aux images médicales"*. 2012.
- [Nawal 14] Nawal. *"Classifieurs SVM et Réseaux de Neurones"*. 2014.
- [Nicolas 01] Morizet Nicolas. *"Revue des algorithmes PCA, LDA et EBGM utilisées en reconnaissance 2D du visage pour la biométrie"*. 2001.
- [N.Morizet 09] N.Morizet. *"Reconnaissance biométrique par fusion multimodale du visage et de l'iris"*. 2009.
- [Philippe] André Thomas Philippe Thomas.
- [Philippe 10] Martin Philippe. *"UFLDL Tutorial ,Convolutional Neural Network "*. 2010.

- [Pierre 11] Buyssens Pierre. *"Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e-transactions"*. 2011.
- [P.Vickram 13] Dr. A. Sri Krishna P.Vickram & D.Swapna. *"Offline signature verification using support local binary pattern"*. 2013.
- [R.Djourani 06] R.Djourani. *"Reconnaissance de visages"*. 2006.
- [Rodriguez 06] Marcel S Rodriguez Y. *Face authentication using adapted local binary pattern histograms*. In : Leonardis, A., Bischof, H., Pinz, A. (eds.) *ECCV 2006. LNCS, vol. 3954*, pp. 321–332. Springer, Heidelberg (2006). 2006.
- [Romain 12] Giot Romain. *"Contributions à la dynamique de frappe au clavier : multibiométrie, biométrie douce et mise à jour de la référence"*. 2012.
- [S. Shigematsu 99] Y. Tanabe T. Adachi S. Shigematsu H. Morimura & Katsuyuki Machida. *"A Single-Chip Fingerprint Sensor and Identifier"*. 1999.
- [Serge 10] Komanda Basema Serge. *"Identification des personnes par reconnaissance de visage pour la sécurité d'une institution bancaire"*. 2010.
- [S.lui 01] msilveman S.lui. *"A pratical guide to biometric security technology"*. 2001.
- [Sofiane 12] Boudjellal Sofiane. *"Détection et identification De personne par méthode Biométrie"*. 2012.
- [Souhila 08] Guerfi ababsa Souhila. *"Authentication d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D"*. 2008.
- [Stephen 14] Mayhew Stephen. *"Biometrics market"*. 2014.
- [Timo Ahonen 06] Abdenour Hadid Timo Ahonen & Matti Pietikainen. *"Face description with local binary patterns : Application to face recognition"*. 2006.
- [Vermont 05] Fabrice Vermont. *"localisation de visage "*. 2005.
- [W. Ben Soltana 14] N. Vandenbroucke A. Ahmad et D. Hamad W. Ben Soltana A. Porebski. *"Contribution des descripteurs de texture LBP à la classication d'images de dentelles"*. 2014.
- [Wadihaji 03] Wadihaji. *"Les treillis de Galois et leurs applications dans la classification textuelle"*. 2003.

- [Y. Baohua 12] C. Honggen Y. Baohua & C. Jiuliang. *"Combining Local Binary Pattern and Local Phase Quantization for Face Recognition"*. 2012.
- [Y 98] Oussar Y. *"Réseaux d'ondelettes et réseaux de neurones pour la modélisation statique et dynamique de processus"*. 1998.
- [Yasmine 99] yactine Yasmine. *Topologie des réseaux de neurones*. 1999.
- [Youcef 17] Djeriri Youcef. *"Les Réseaux de Neurones Artificiels"*. 2017.
- [Younes 14] Bennani Younes. *"Apprentissage par réseaux de neurones artificiels"*. 2014.
- [Zahir 14] Asradj Zahir. *"Identification des systèmes non linéaires par les réseaux de neurones"*. 2014.
- [zakaria 14] Aouati zakaria. *"(en ligne)panorama sur les différentes techniques biométriques"*. 2014.
- [Zhenhua Guo] Member IEEE Zhenhua Guo Lei Zhang & David Zhang. *"A Completed Modeling of Local Binnry Pattern Operateur for Texture Classification »IEEE tran .on image Processing"*.