République **A**lgérienne **D**émocratique et **P**opulaire

Ministère de l'**E**nseignement **S**upérieur et de la **R**echerche **S**cientifique

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

Mémoire de Fin d'Etudes

De MASTER ACADEMIQUE

Domaine : **Mathématiques et Informatique**

Filière : **Informatique**

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

Thème :

Développement d'un système biométrique pour la reconnaissance de visage, basé sur L'opérateur binaire Local(LBP) et ses variantes.

Encadreur : Mme C. CHERIFI

Examinateur : Melle YESLI

Examinateur :

Président : Mr HABET

Présenté par :

-GOUMEZIANE Hayet

-LARIBI Djamila

Promotion :2017 /2018

Remerciements :

*Nous tenons tout d'abord a remercié **DIEU**, tout puissant, de nous avoir donné la force de réaliser ce projet tout au long de cette année. Nous adressons nos plus vifs remerciements à*

*Notre promotrice C.**FERHAOUI-CHERIFI** pour la confiance qu'elle nous a accordée en nous proposant ce sujet, pour ses précieux conseils, pour ses remarques pertinentes, ainsi que son encouragement sans lequel ce travail n'aurait jamais vu le jour.*

Nos remerciements vont également à tous les enseignants de l'université Mouloud

***Mammeri (département informatique)** pour le savoir qu'ils nous ont permis d'acquérir et pour l'esprit d'analyse qu'ils nous ont permis de développer. Nous présentons nos gratitudes au **président et aux membres du jury** qui nous font l'honneur de juger notre travail.*

Nous remercions tous ceux, qui de près ou de loin, nous ont apporté leur contribution pour

la réalisation de ce travail.

Dédicaces

Je dédié mon travail à :

A ceux que j'aime jusqu'à la frontière de l'imagination : ma très chère mère FATMA qu'ALLAH l'agrée près de lui dans son vaste paradis, et mon très cher père Boussad pour son aide et son soutien tout au long de mes études et à ma belle-mère.

A mon mari Sofiane qui m'a toujours soutenu dans tout ce que j'ai entrepris, qui m'a accompagné et encouragé tout au long de mon parcours universitaire et à mon futur bébé.

A mes chères sœurs Lila et Meriem et à mes très chers frère Mokrane, Hassane, Smail, et Salim.

A ma belle-mère Nadia et mon beau père Arezki et à toute ma famille conjugale

A mes belle sœurs Samira et Lila

A mes nièces Amel, Imane et Iline et mes neveux Amine et Massi

A tous mes oncles et tantes, cousins et cousines.

A mon binôme et a tous mes amies.

A tous ceux que je connais de près ou de loin et en particulier ceux qui ont contribué à la réalisation de ce travail.

A toute la promotion 2018.

Hayet.

Dédicaces

Je dédie ce modeste travail

A la mémoire de mes grands pères et ma grande mère et mon cousin « said ».

A mes chers parents

A ma chère grande mère

A mes sœurs et frères

A mes proches grands et petits

A tout tous mes amis

A cette personne qui compte déjà énormément pour moi, et pour qui je porte beaucoup de tendresse et respect.

A mon binôme

A tous ce qui ont participés de près ou de loin dans la réalisation de ce travail.

Djamila.

Résumé :

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

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

Dans le cadre de notre projet de fin d'étude nous avons réalisé un système de reconnaissance faciale basé sur motif binaire local (LBP) et ses variantes. Le processus de reconnaissance faciale est divisé en plusieurs étapes à savoir : la détection du visage de chaque image, la normalisation du visage, l'extraction des caractéristiques faciales, classification et décision. Nous avons utilisé les motifs binaires locaux (Local Binary Pattern) pour l'extraction des caractéristiques faciales qui a prouvé sa robustesse.

L'évaluation du système a été faite sur la base de données standards : **ORL** qui est une base d'images fixes, elle nous a permis de tester l'approche LBP ainsi que plusieurs de ses variantes en utilisant les méthodes de classification : la distance Euclidienne, Cos, Mahcos, la norme CTB et ainsi la distance Chi_carrée $X2$. L'ensemble des résultats a mis en évidence l'intérêt que cette approche apporte en termes d'efficacité et de robustesse face aux variations d'éclairage et les expressions du visage.

Les Mots Clés : La biométrie, les modalités biométriques, la reconnaissance faciale, motifs binaire locaux (LBP), distance (euclidienne, cosine, ctb, …).

SOMMAIRE

Chapitre II : Système de reconnaissance de visage.

Partie II : Extraction de caractéristique et classification

Chapitre III : Extraction de caractéristique et classification

Chapitre IV : Conception et Réalisation

Chapitre V : Tests et Evaluation des résultats

Liste des figures :

Liste des tableaux

Introduction Générale

Introduction générale :

Le besoin en sécurité de nos sociétés modernes s'est accru ces dernières années, avec la prolifération des menaces d'usurpation d'identité et de vol de données personnelles. Pour répondre à ces besoins les outils classiques tel que les mots de passes et les badges ne suffisent plus. Afin d'accroitre la fiabilité des systèmes de sécurité classique, la biométrie est une alternative de plus en plus employée.

La biométrie consiste à identifier une personne à partir des caractéristiques physiques ou comportementales, elle facilite l'accès pour les usagers tout en garantissant un niveau de sécurité élevé, elle pallie aux risques du vol des cartes d'accès ou d'oubli des mots de passes.

La reconnaissance faciale est une aptitude qui relie l'apparence d'une personne à son identité. Lors d'une rencontre, cette compétence permet de se rappeler des échanges précédents et ainsi de construire une relation à long terme ou les individus finissent par se connaître et savoir anticiper leurs comportements et besoins respectifs. En effet, elle est l'une des techniques biométriques les plus utilisées car elle présente un avantage d'être naturelle et sa mise en œuvre est facile.

Plusieurs méthodes de reconnaissance faciale ont été développées ces dernières années, parmi elles la Local Binary Pattern (LBP) caractérisée par sa simplicité et son invariance au changement d'illumination.

C'est dans ce cadre que se place notre projet de fin d'études, qui a pour objectif la proposition d'un système de reconnaissance de visage basé sur une technique locale LBP, qui se veut être fiable et adaptée à un environnement présentant des variabilités de luminance, de pose, expression de visage et présence ou absence des composants structurels. Il est nécessaire de travailler à tous les niveaux du système (détection, extraction des caractéristiques et reconnaissance) en apportant des contributions pertinentes à différents points de la chaîne de traitement.

Pour la partie reconnaissances on a opté pour plusieurs méthodes de classification par mesure de similarité à noter la distance euclidienne, cosine, mahcos, ctb et Chi-carrée X2.

Afin de bien mener à terme notre projet et de donner une démarche compréhensible, nous avons structuré le présent mémoire de la manière suivante :

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

Chapitre II : « SYSTEME DE RECONNAISSANCE DE VISAGES », 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 des différentes techniques développées au cours de ces dernières années dans la reconnaissance faciale.

Chapitre III : « EXTRACTION DES CARACTERISTIQUES ET CLASSIFICATION », décrit en particulier la méthode locale : LBP. Ces principes de fonctionnement et la présentation de quelques variantes de l'approche LBP.

Chapitre IV : « CONCEPTION ET REALISATION » présente la phase de conception et réalisation du système, les cas d'utilisation de notre système et les diagrammes de séquences l'exposition de différents algorithmes et méthodes utilisées pour l'extraction de caractéristiques du visage.

Chapitre VI : « TEST ET EVALUATION DES RESULTATS » donne les tests et les résultat obtenus après réalisation et exécution de notre système tout en donnant une synthèse de notre travail.

PARTIE I

BIOMETRIE ET RECONNAISSANCE DE VISAGES.

CHAPITRE I

BIOMETRIE : Concepts, Application et enjeux

Introduction :

Il existe traditionnellement deux manières d'identifier un individu. La première méthode est fondée sur une clef connue uniquement par l'utilisateur telle qu'un mot de passe utilisé au démarrage d'une application ou un code qui permet d'activer un téléphone portable. La seconde méthode est fondée sur la possession d'un objet tel qu'une pièce d'identité, une clef, ou un badge. Ces deux méthodes peuvent être utilisées de manière complémentaire afin d'obtenir une sécurité accrue. Cependant, elles présentent un double inconvénient ; en effet, l'utilisation d'un mot de passe nécessite sa mémorisation et le fait d'en avoir plusieurs rend la tâche plus difficile, le noter engendre le risque de perte ou de vol. De même, l'utilisation de cartes magnétiques, de clefs ou de badges n'échappe pas au risque de vol par des imposteurs qui sont capables de falsifier leur identité.

Comme chaque individu possède des caractéristiques qui lui sont propres : sa voix, ses empreintes digitales, les traits de son visage, la forme de sa main, sa signature et jusqu'à son ADN (données biométriques). Toutes les difficultés des deux méthodes ont donné naissance à l'idée d'utiliser ces caractéristiques biométriques comme moyen d'identification et de reconnaissance.

Dans ce chapitre, Nous introduisons la notion de la biométrie en commençant par sa définition, les différentes modalités biométriques, et le principe de fonctionnement des systèmes biométriques ainsi que les outils utilisés pour mesurer leurs performances.

I.1. Définition de la biométrie :

La biométrie est donnée par Roethenbaugh **[1]** : « La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables, permettant de reconnaître ou de vérifier automatiquement l'identité ».

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques : comportementales physiques ou physiologiques

Le mot biométrie est une traduction du mot anglais « biométrics » qui correspond en français à l'anthropométrie. Il désigne dans un sens très large l'étude quantitative des êtres vivants, mais dans le contexte de la reconnaissance d'individus il est défini par **[2] :**

1. Selon le CLUSIF (Club de la Sécurité des systèmes d'Information Français) La biométrie est la science qui étudie à l'aide des mathématiques, les variations biologiques à l'intérieur d'un groupe déterminé.

2. Selon la RAND (Public Safety and Justice), la biométrie est définie comme toute caractéristique physique ou trait personnel automatiquement mesurable, robuste et distinctif qui peut être employé pour identifier un individu ou pour vérifier son identité.

I.2. Historique de la biométrie :

Dans la Chine des dynasties, les documents étaient signés à l'aide d'empreintes digitales. Selon le rapport de l'explorateur Joao de Barros **[3].** Il a écrit que les marchands chinois relevaient les empreintes des mains et des pieds des enfants de jeune âge sur du papier en utilisant de l'encre afin de les distinguer les uns des autres. C'est une des méthodes les plus anciennes de la biométrie en pratique et elle est toujours utilisée de nos jours. Dans les échanges commerciaux de Babylone, 3000 ans avant-J.-C., le même système était utilisé. En Amérique précolombienne, nombre d'architectes laissèrent également la trace de leurs mains colorées sur les parois de grottes aménagées.

Mais ce n'est qu'au début du XVIIIème siècle que le Docteur Henri Faulds développe l'utilisation de traces de doigt pour l'identification des personnes **[2].** A la même époque, l'anglais Francis Galton réalise des travaux de mesures de corps humains et crée une table de statistiques basée sur les tailles et les poids des personnes. Il met au point la méthode "Fingerprints" qui établit l'unicité et la permanence des figures cutanées. En 1881, le médecin italien Cesare Lombroso tente de prouver que l'humain criminel présente des caractéristiques repérables et stables. Ainsi, le poids du cerveau des honnêtes gens pèserait entre 1475 et 1550 grammes tandis que celui des criminels serait d'à peu près 1455 grammes. Ces théories, non fondées scientifiquement, sont vite abandonnées. En 1885, Alphonse Bertillon ne laisse cependant pas de côté cette hypothèse, responsable de l'identité judiciaire en France, il construit "le Bertillonage" qui s'appuie sur les mensurations des criminels. Le principe connaît un vif succès jusqu'au jour où une erreur judiciaire grave vient détruire le rêve de ségrégation.

Après l'échec du Bertillonage, la police a commencé à utiliser la technique des empreintes digitales, qui a été développée par Richard Edward Henry de Scotland Yard, ressemblant essentiellement aux mêmes méthodes employées par les Chinois durant des années. Au XIXème siècle, la police criminelle fait considérablement avancer la recherche du fait de la multiplication des Analyses d'Indices Biologiques (ADN)

Dans les trois dernières décennies, la biométrie a évolué d'une seule méthode simple (empreintes digitales) vers plus de dix méthodes discrètes. Les sociétés de biométrie comptent des centaines de nouvelles méthodes appliquées et continuent à améliorer leurs méthodes de

sécurité tant que la technologie répond à leurs exigences. Les prix du hardware requis continuent à baisser rendant des systèmes faisables pour de faibles et moyens budgets.

Cependant le développement de l'industrie, fait ainsi le souci du public concernant les libertés et l'intimité. Des lois et des règlements continuent à être rédigés et des normes commencent à être mises en place. Tandis qu'aucune autre technique biométrique n'a encore atteint le succès de l'utilisation de l'empreinte digitale, certaines commencent à être employées dans des secteurs d'activité judiciaire et commerciale.

I.3. Système biométrique :

I.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 **[4],** extrayant un ensemble de caractéristiques à partir des données acquises, et comparant ces caractéristiques contre 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.

I.3.2. Modules d'un système biométrique :

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

1. **Module de capture :** 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.)

2. **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.

3. **Module de correspondance :** Il compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.

4. 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).

I.3.3. L'architecture d'un système biométrique :

Les techniques biométriques sont employées pour assurer plusieurs services concernant les contrôles d'accès virtuels ou physiques dans différents domaines **[5].**

Elles comportent deux processus importants : l'enregistrement des personnes pour le service (Apprentissage), et à un stade ultérieur, la reconnaissance de ces individus. Cette dernière consiste en une tache d'identification ou d'authentification.

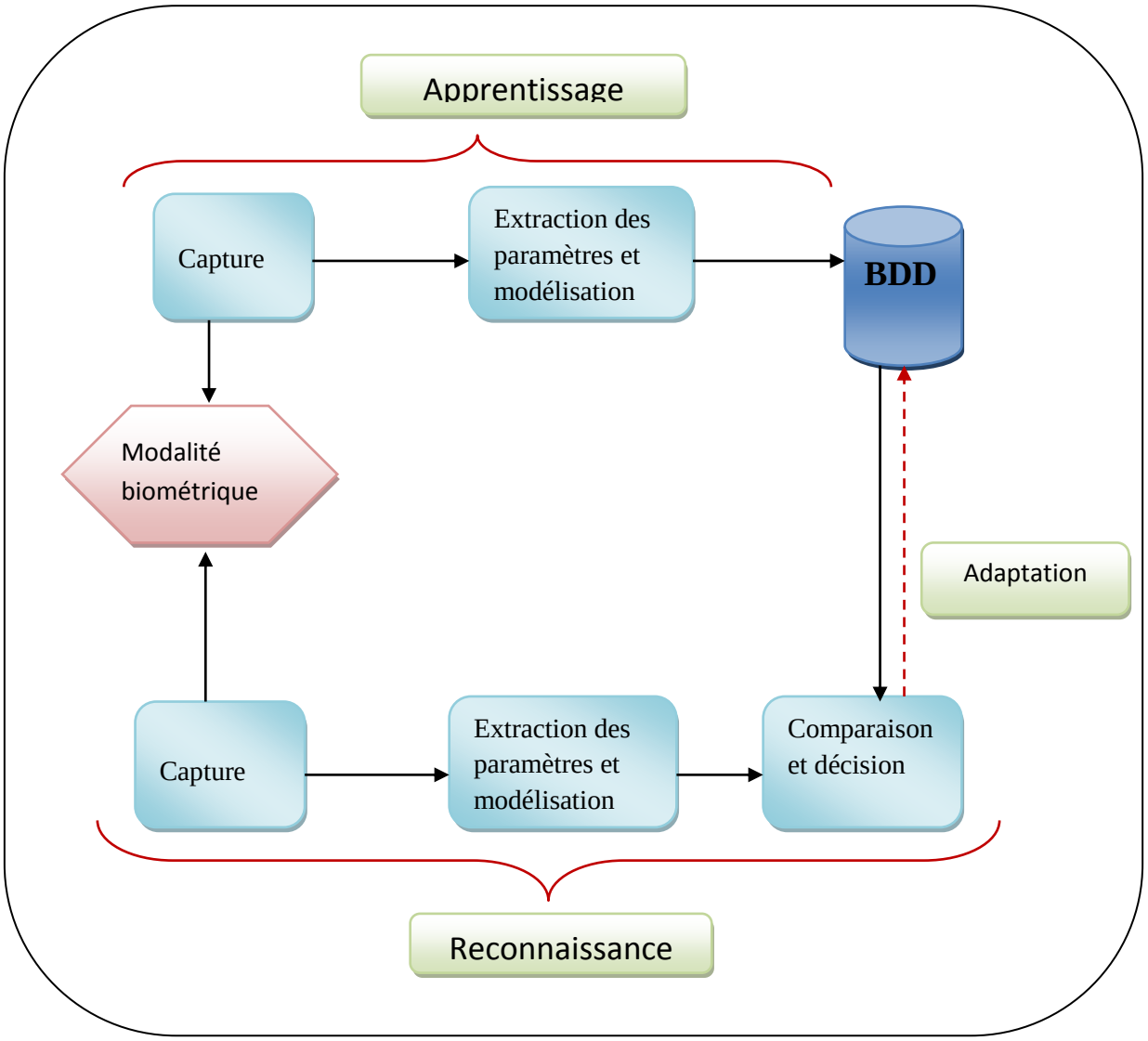

Figure I.1: architecture d'un système biométrique **[5]**

I.3.3.1 Apprentissage (enrôlement)

Dans le cas où quelqu'un se présente devant le système pour une demande d'identification ou d'authentification, une modalité biométrique de la personne en question (voix, visage, iris, rétine, empreinte digitale…etc.) est captée par un dispositif approprié, puis digitalisée. L'information essentielle est par la suite extraite à partir des données acquises pour être modélisée à l'aide de fonctions mathématiques. Le modèle obtenu va être sauvegardé dans une base de données des utilisateurs du système, qui servira à leur reconnaissance.

Cette phase comporte deux principaux modules :

1. Le module de capture
2. Le module d'extraction de paramètres et modélisation

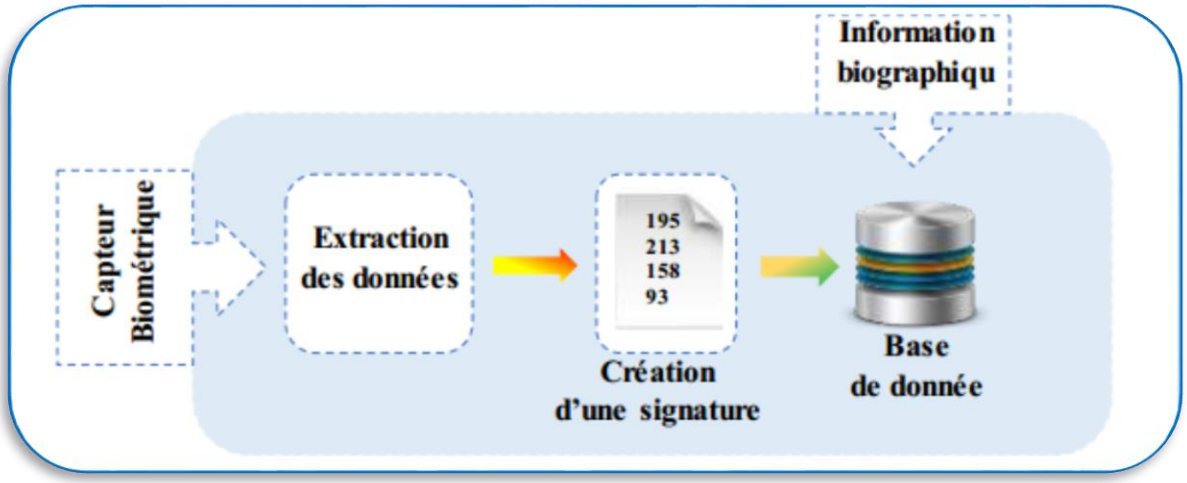

Figure I.2. Processus d'apprentissage dans un système biométrique.

I.3.3.2 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

- **Identification :**

Dans le cas d'identification, le système mesure le degré de similitude entre les caractéristiques extraites et l'ensemble des modèles de la base de données référence. Ce mode de test est appelé un test «1 contre N » **[6],**

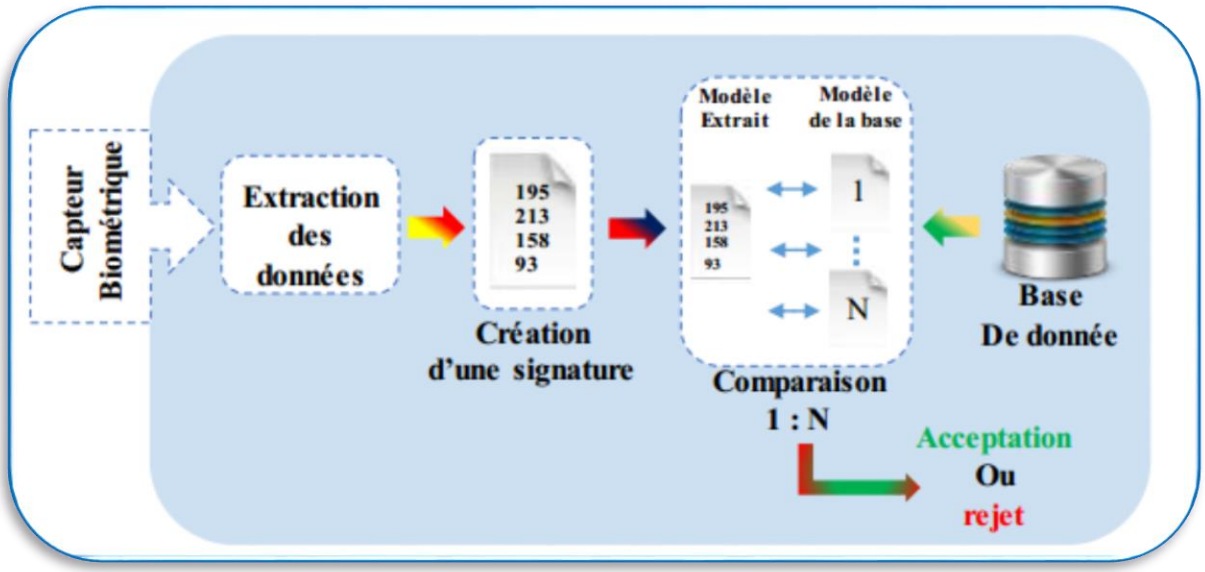

Figure I.3. Processus d'identification dans un système biométrique.

- **Vérification (authentification) :**

Contrairement au mode d'identification, une personne qui désire être authentifiée réclame une identité par l'intermédiaire d'un numéro d'identification personnelle (PIN), d'un nom d'utilisateur ou d'une carte futée… etc. Ensuite, le système fait une comparaison (module de correspondance) « un à un » entre les données biométriques extraites et le modèle préenregistré. Cela, afin de déterminer si l'identité proclamée par la personne est vraie ou fausse (module de décision).

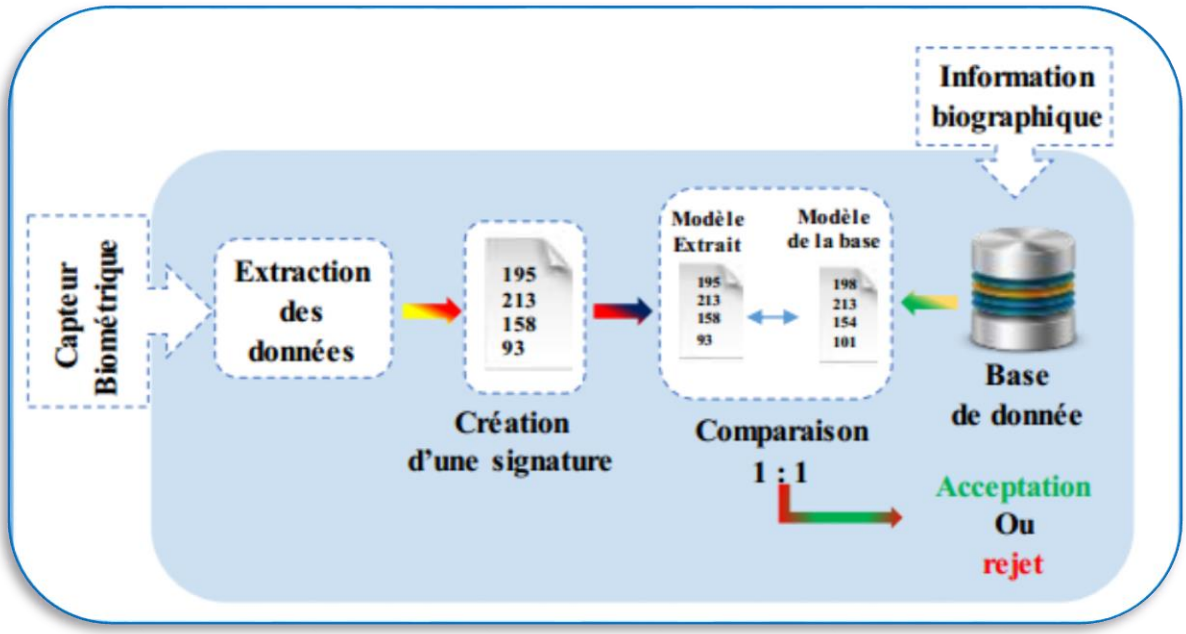

Figure I.4. Processus de vérification dans un système biométrique.

I.3.4. Mesure de performance d'un système biométrique :

Afin de mesurer la performance d'un système biométrique en modes de vérification et/ou d'identification, deux principaux tests sont utilisés **[7] :**

I.3.4.1. Test de vérification :

Dans la tâche de vérification, un utilisateur final doit faire une demande d'authentification de son identité. Par exemple : il proclame "je suis Mr XY", alors le système biométrique doit déterminer si l'identité proclamée par l'utilisateur est acceptée ou rejetée.

Deux taux sont alors calculés :

- ***Le Taux de Faux Rejets*** **ou False-Rejection Rate (FRR) :** il exprime le pourcentage d'utilisateurs rejetés alors qu'ils devraient être acceptés par le système.

$$\boldsymbol{FRR} = \frac{Nombre\ de\ clients\ rejetés(FR)}{Nombre\ de\ clients\ totale}$$

- ***Le Taux de Fausses Acceptations*** **ou False-Acceptance Rate (FAR) :** il exprime le pourcentage d'utilisateurs acceptés par le système alors qu'ils devraient être rejetés.

$$\boldsymbol{FAR} = \frac{Nombre\ d'imposteur\ acceptés(FA)}{nombre\ d'imposteur\ totale}$$

On peut formuler le test de vérification de la façon suivante :

Soient X_Q le vecteur de caractéristiques de la personne proclamée *I*, *Xt* le vecteur de caractéristiques de la personne *I* stockée dans la base de données, *S* (X_Q, Xt) la fonction de similarité entre le vecteur X_Q et *Xt.* 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, XQ),* telle que :

$$(I, X_Q) = \begin{cases} w1 & si \quad S(X_{Q,}\, X_t) > \theta \\ w2 & sinon \end{cases}$$

Où w1 indique que la personne proclamée est vraie et w2 qu'elle est un imposteur.

Le choix du seuil de similarité θ est important car il influe directement sur les performances du système. Un seuil θ trop petit entraîne l'apparition d'un grand nombre de faux rejets, tandis qu'un seuil θ trop grand engendre un taux important de fausses acceptations.

La statistique la plus simple pour mesurer la performance d'un algorithme dans **le contexte de la vérification** est de calculer le *point d'équivalence des erreurs (Equal Error Rate - EER).*

Le point d'équivalence des erreurs, ou taux d'exactitude croisée, est déterminé par le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets FAR=FRR.

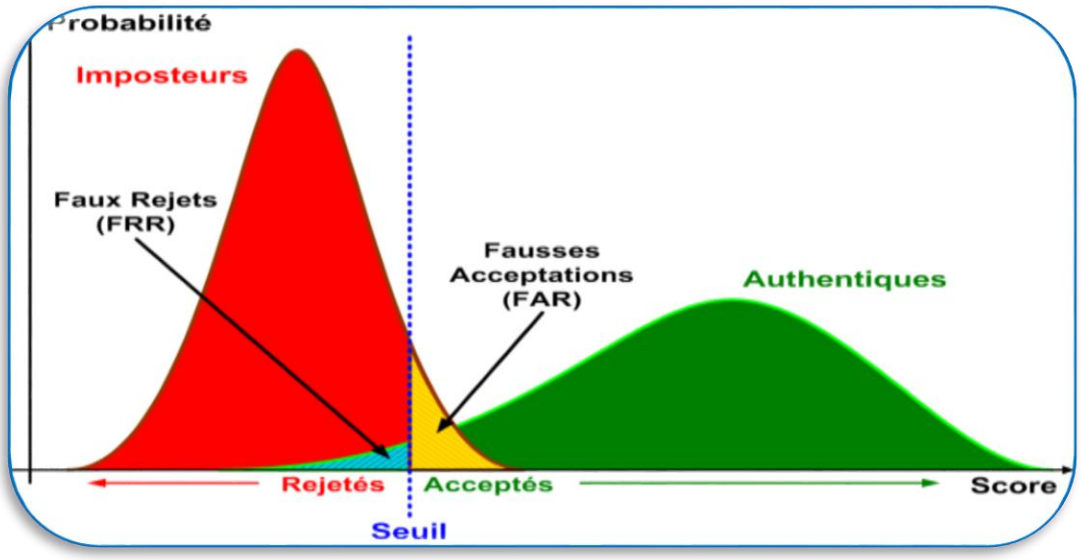

Figure I.5. Distributions des taux de vraisemblance des utilisateurs authentiques et des imposteurs d'un système biométrique.

La figure suivante montre l'influence du seuil de décision sur les erreurs du système biométrique :

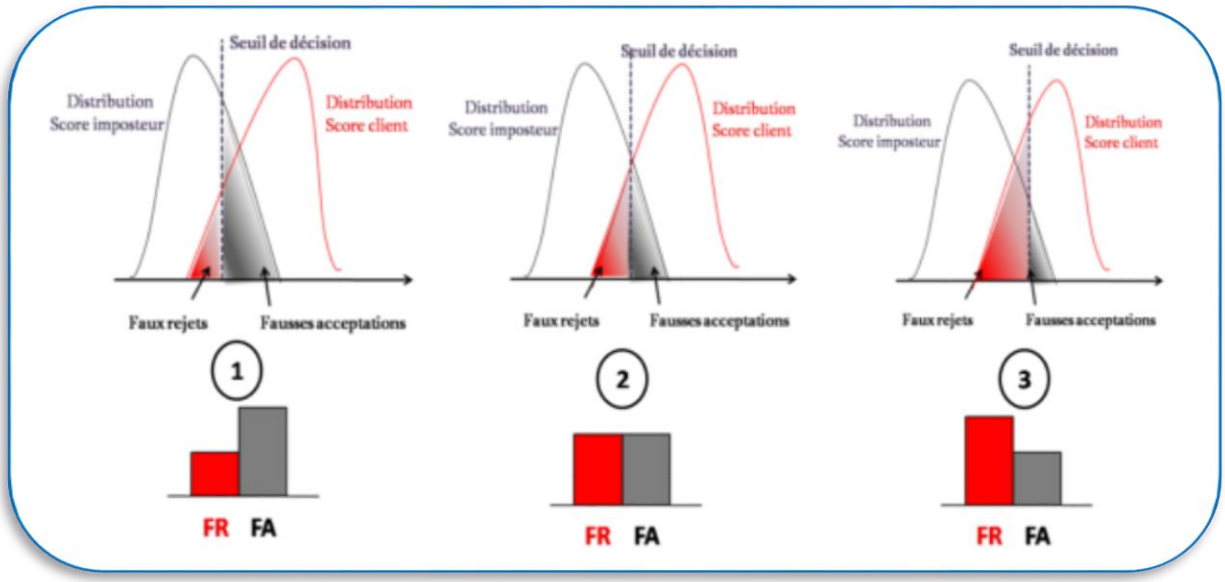

Figure I.6.Influence du seuil de décision sur les erreurs d'un système biométrique **[5].**

1- Seuil de décision choisi dans le but de réduire le nombre de faux rejets

2- Seuil de décision choisi pour obtenir autant de faux rejets que de fausses acceptations (EER).

3- Seuil de décision choisi dans le but de réduire le nombre de faux rejets.

L'évaluation passe également par le tracé de statistiques complexes, comme la courbe « Receiver Operating Characteristic ROC ». Cette courbe donne le FRR en fonction du FAR. Elle est tracée de manière paramétrique en fonction des valeurs du seuil θ.

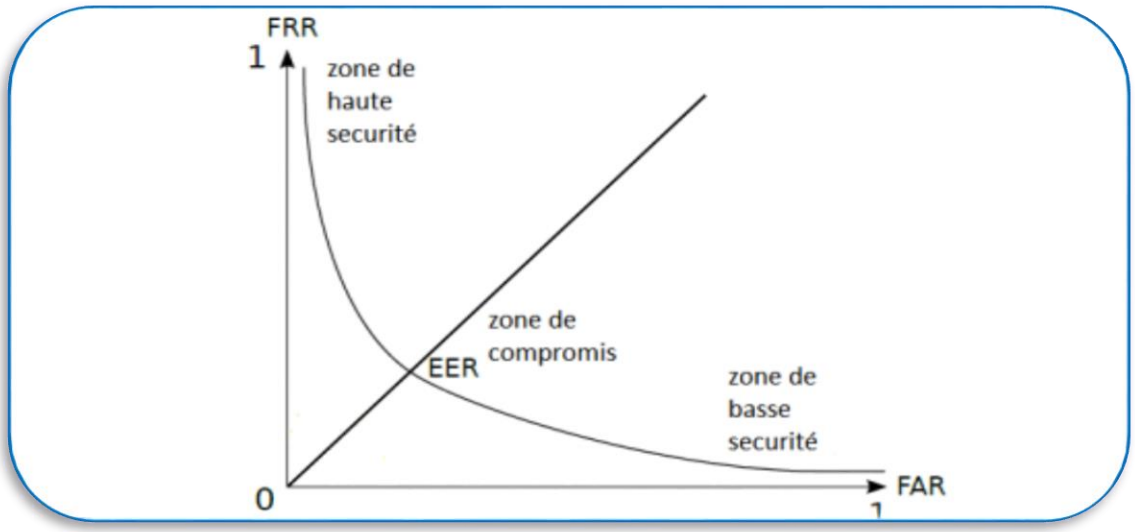

Figure I.7. Courbe ROC

1.3.4.2. Test d'identification :

A ce niveau les performances sont mesurées par le pourcentage des personnes bien reconnues par rapport au nombre de tests, appelé le Taux d'Identification (TID) qui est définie par la formule suivante :

$$\boldsymbol{TID} = \frac{\text{Nombre de tests qui ont conduit à une bonne identification}}{\text{Nombre totale de tests}}$$

On peut formuler le test d'identification de la façon suivante:

Soient X_Q le vecteur de caractéristiques, pour déterminer l'identité I_K, $K \in \{1, 2,..,.N, N+1\}$, on calcule la fonction (I, X_Q) définie par :

$$(I, X_Q) = \begin{cases} I_K & , si\ max_K \quad \{S(X_Q, X_{I_K})\} \geq \theta,\ K = 1 \ldots . N \\ I_{N+1} & , sinon \end{cases}$$

Où I_1,.., I_N sont les identités enrôlées, I_{N+1} une identité rejetée, X_{IK} la signature biométriques qui correspond à l'identité I_K, et θ le seuil.

Le *test d'identification* représente la mesure la plus couramment utilisée, mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve parmi les *N premières réponses du système*. On trace alors la courbe *Cumulative Match Characteristics* (CMC) qui représente la probabilité que le bon choix se trouve parmi les *N premiers* [Phi00].Comme l'illustre la figure I-8

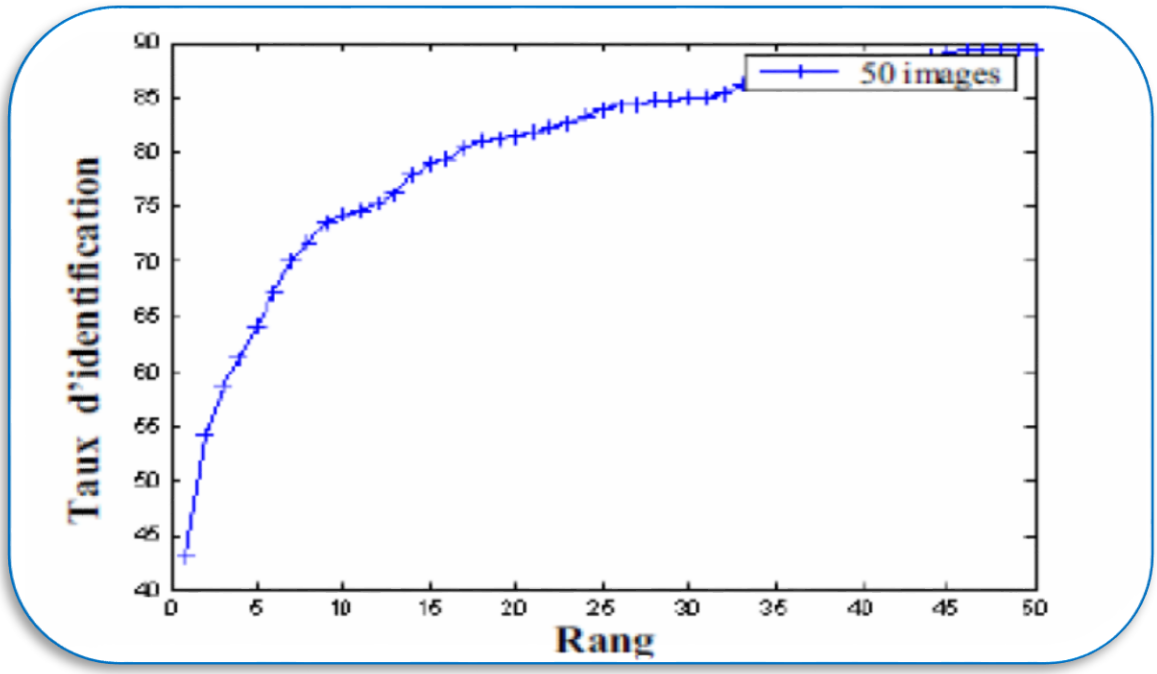

Figure I.8.courbe CMC

I.4. Modalités biométriques :

La multitude des caractères biométriques de l'être humain a donné naissance à plusieurs systèmes d'authentification, chacun repose sur un caractère morphologique ou comportemental, parmi ces systèmes il y a ceux qui ont prouvé leur fiabilité et leurs performances et d'autre sont toujours en cours d'évolution.

I.4.1. Les modalités morphologiques:

Ce type de système est basé sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine, et de l'iris de l'œil.

a- Les Empreintes digitales :

A l'heure actuelle la reconnaissance des empreintes digitales est la méthode biométrique la plus utilisée **[8].** Les empreintes digitales sont composées de lignes localement parallèles présentant des points singuliers (minuties) et constituent un motif unique, universel et permanent.

Pour obtenir une image de l'empreinte d'un doigt, les avancées technologiques ont permis d'automatiser la tâche au moyen de capteurs intégrés, remplaçant ainsi l'utilisation classique

de l'encre et du papier. Ces capteurs fonctionnant selon différents mécanismes de mesure (pression, champ électrique, température) permettent de mesurer l'empreinte d'un doigt fixe positionné sur ce dernier (capteur matriciel) ou en mouvement (capteurs à balayage).

L'image d'empreinte d'un individu est capturée à l'aide d'un lecteur d'empreinte digitale puis les caractéristiques sont extraites de l'image puis un modèle est créé. Si des précautions appropriées sont suivies, le résultat est un moyen très précis d'authentification.

Les techniques d'appariement des empreintes digitales peuvent être classées en deux catégories **:** Les techniques basées sur la *détection locale des minuties* et les techniques basées sur la *corrélation*.

L'approche basée sur les minuties : consiste à trouver d'abord les points de minuties puis trace leurs emplacements sur l'image du doigt

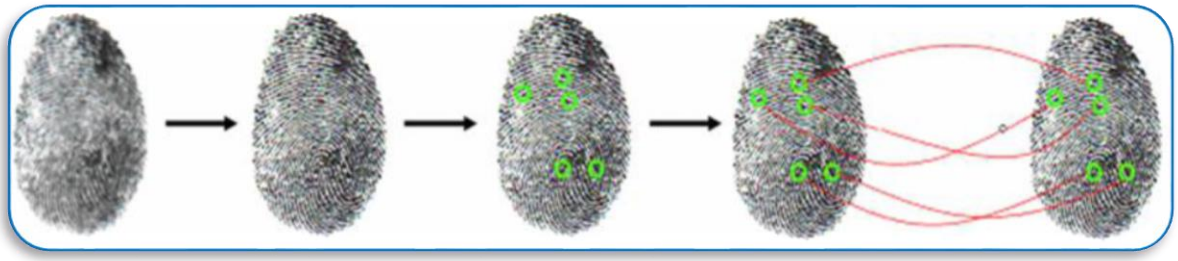

Figure I.9. Empreinte digitale **[8]**

Cependant, il y a quelques difficultés avec cette approche lorsque l'image d'empreinte digitale est d'une qualité médiocre, car l'extraction précise des points de minutie est difficile. Cette méthode ne tiens pas en compte la structure globale de crêtes et de sillons.

Les méthodes basées sur la corrélation **:** sont capables de surmonter les problèmes de l'approche fondée sur les minuties. Ces méthodes utilisent la structure globale de l'empreinte, mais les résultats sont moins précis qu'avec les minuties. De plus, les techniques de corrélation sont affectées par la translation et rotation de l'image de l'empreinte. C'est pour cela que les deux approches sont en général combinées pour augmenter les performances du système

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

Avantages	Inconvénients
- La technologie la plus éprouvée techniquement et la plus connue du grand public. - Caractéristique difficile à dupliquer. - La petite taille du lecteur facilite son intégration dans la majorité des applications (téléphones portables, PC). - Faible coût des lecteurs grâce aux nouveaux capteurs de type "Chip silicium". - Bon compromis entre le taux de faux rejet et le taux de fausse acceptation.	- Acceptabilité moyenne de la part du grand publique. - Besoin de la coopération de l'utilisateur (pose correcte du doigt sur le lecteur). - Certains systèmes peuvent accepter un moulage de doigt ou un doigt coupé (la détection du doigt vivant permet d'éviter ce type d'usurpation).

b- Géométrie de la main :

La géométrie de la main est une technologie biométrique récente **[8].** Comme son nom l'indique, elle consiste à analyser et à mesurer la forme de la main, c'est-à-dire mesurer la longueur, la largeur et la hauteur de la main d'un utilisateur et de créer une image 3-D. Des LEDs infrarouges et un appareil-photo numérique sont utilisés pour acquérir les données de la main.

Cette technologie offre un niveau raisonnable de précision et est relativement facile à utiliser. Cependant elle peut être facilement trompée par des jumeaux ou par des personnes ayant des formes de la main proche. Les utilisations les plus populaires de la géométrie de la main comprennent l'enregistrement de présence et le contrôle d'accès. Par contre, les systèmes de capture de la géométrie de la main sont relativement grands et lourds, ce qui limite leur utilisation dans d'autres applications comme l'authentification dans les systèmes embarqués : téléphones portables, voitures, ordinateurs portables, etc.

Figure I.10. Géométrie de la main **[8]**

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

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.	- 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

c- L'iris :

L'utilisation de l'iris comme caractéristique biométrique unique de l'homme a donné lieu à une technologie d'identification fiable et extrêmement précise. L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il est unique. L'iris a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu. Les algorithmes utilisés dans la reconnaissance de l'iris sont si précis que la planète toute entière pourrait être inscrite dans une base de données de l'iris avec peu d'erreurs d'identification.

L'image de l'iris est généralement capturée à l'aide d'une caméra standard. Cependant, cette étape de capture implique une coopération de l'individu. De plus, il existe plusieurs contraintes liées à l'utilisation de cette technologie. Par exemple, il faut s'assurer que l'iris de

l'individu est à une distance fixe et proche du dispositif de capture, ce qui limite l'utilisation de cette technologie

Figure I.11. L'iris **[16]**

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

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

d- La rétine :

La rétine est la « pellicule photographique » de l'œil **[9].** Elle est constituée de 4 couches de cellules et est située au fond de l'œil.

Les éléments qui permettent de distinguer deux rétines sont les veines qui les tapissent. La disposition de ces veines est stable et unique.

La biométrie par la rétine procure également, un haut niveau en matière de reconnaissance. Cette technologie est bien adaptée pour des applications de haute sécurité (sites militaires et nucléaires, salles de coffres forts, etc.).

La disposition des veines de la rétine assure une bonne fiabilité et une haute barrière contre la fraude. L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. A ce moment, un faisceau lumineux traverse l'œil jusqu' aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence. Après la capture d'une image de la rétine, le logiciel du dispositif de lecture découpe un

anneau autour de la fovéa. Il repère l'emplacement des veines et leur orientation. Puis il les codifie dans un gabarit. Les algorithmes de l'opération restent relativement complexes.

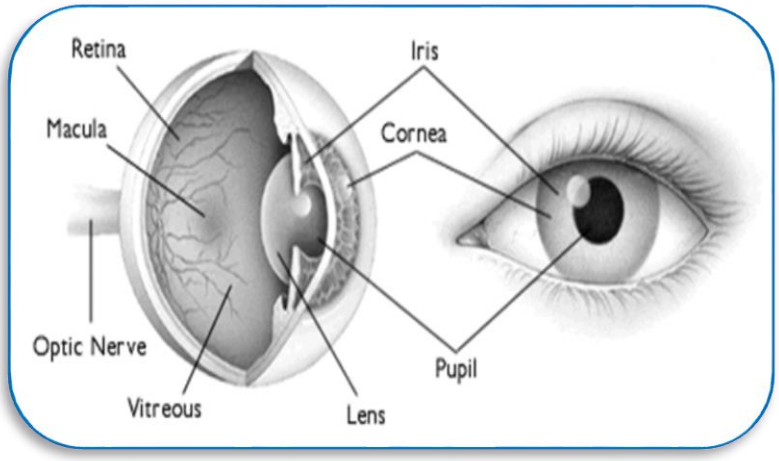

Figure I.12. La rétine **[9]**.

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

Avantages	Inconvénients
- L'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure,…). - Très difficile, voire impossible, de l'imiter. - Les taux de faux rejet et de fausse acceptation sont faibles. - Stable durant la vie d'un individu.	- Système intrusif et mal accepté par le public ; il faut placer l'œil près du capteur. - Coût plus important que le coût des autres technologies. - Modalité non adapté pour un flux de passage important.

e- Le visage :

Il s'agit de capter la forme du visage d'un individu et d'en extraire certaines informations jugées évidentes pour l'authentification. Selon le système utilisé, l'individu doit être positionné devant l'appareil où peut être en mouvement à une certaine distance. Les données biométriques qui sont obtenues sont par la suite comparées au fichier référence. Au début des années 1970, la reconnaissance par le visage était principalement basée sur des attributs faciaux mesurables comme l'écartement des yeux, des sourcils, des lèvres, la position du menton, la forme, &etc. Depuis les années 1990, les différentes technologies utilisées

exploitent toutes les découvertes effectuées dans le domaine du traitement d'image et de l'analyse de données.

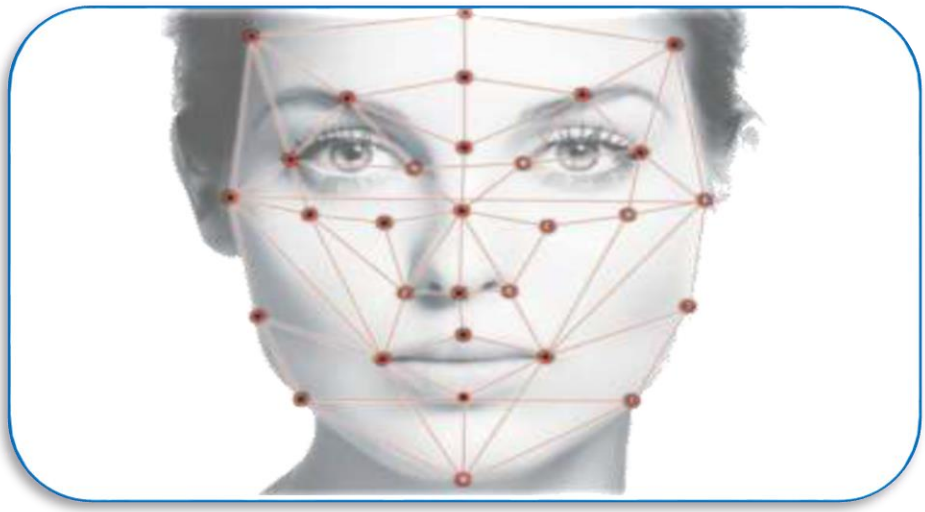

Figure I.13.reconnaissance du visage **[16].**

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

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

I.4.2 Les modalités comportementales :

Ce type de système se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, sa démarche et sa façon de taper sur un clavier.

a- L'écriture (la signature) :

Chaque personne possède une signature qui lui est propre et qui peut donc servir à l'identifier. Il existe deux modes de reconnaissance **[10]:** le mode *statique* et le mode *dynamique*.

Le mode statique n'utilise que l'information géométrique de la signature. Le mode dynamique utilise à la fois l'information géométrique et dynamique, c'est à dire les mesures de vitesse, d'accélération, etc. Le mode dynamique est plus riche en information que le mode statique et donc plus discriminant.

De plus, si un imposteur veut dupliquer une signature à partir d'un exemple, il n'a pas accès à l'information dynamique. La capture se fait à l'aide d'une tablette graphique. La signature a l'avantage par rapport aux autres mesures biométriques d'être couramment utilisée pour les transactions. Pour cette raison, la signature comme moyen d'identification est en général bien acceptée. Le problème de la reconnaissance par signature provient de la très grande variabilité qui existe entre deux occurrences de la signature d'un même individu. De plus, la signature peut être affectée par l'état de santé ou émotionnel de l'individu.

Figure I.14. La signature **[10].**

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

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

b- Dynamique de frappe au clavier :

Un système basé sur la dynamique de frappe au clavier ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier **[11].** 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 mille 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.

Ce dispositif biométrique est utilisé comme méthode de vérification pour le commerce électronique et comme mécanisme de contrôle d'accès à des bases de données.

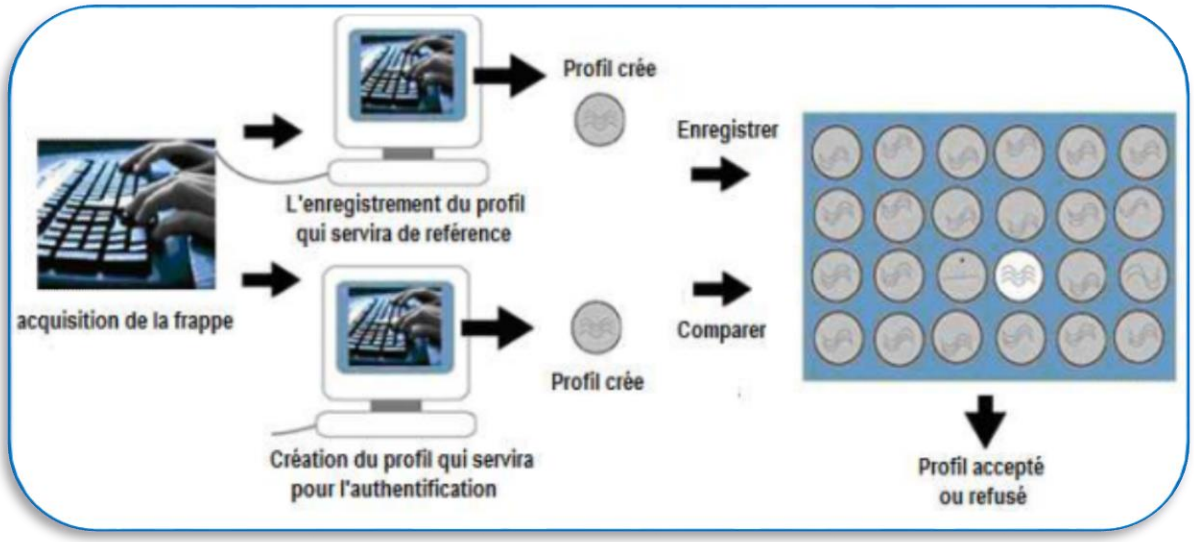

Figure I.15. Dynamique de frappe au clavier **[11].**

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

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

c- Analyse de la démarche :

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps…), en analysant des séquences d'images. 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.

Figure I.16. La démarche

d- La voix :

De tous les traits humains utilisés dans la biométrie, la voix est celle que les humains apprennent à reconnaître dès le plus jeune âge. Les systèmes de reconnaissance de locuteur peuvent être divisés en deux catégories : les systèmes dépendant du texte prononcé et les systèmes indépendants du texte. Dans le premier cas, l'utilisateur est tenu d'utiliser un texte (un mot ou une phrase) fixe prédéterminé au cours des séances d'apprentissage et de reconnaissance. Alors que, pour un système indépendant du texte le locuteur parle librement sans texte prédéfini.

Cette dernière catégorie est plus difficile, mais elle est utile dans le cas où l'on a besoin de reconnaître un locuteur sans sa coopération. La recherche sur la reconnaissance de locuteur est en pleine croissance, car elle ne nécessite pas de matériel cher, puisque la plupart des ordinateurs personnels de nos jours sont équipés d'un microphone. Toutefois, la mauvaise qualité et le bruit ambiant peuvent influencer la vérification et par suite réduire son utilisation dans les systèmes biométriques. Dans un système de reconnaissance de locuteur le signal est premièrement mesuré puis décomposé en plusieurs canaux de fréquences passe-bande. Ensuite, les caractéristiques importantes du signal vocal sont extraites de chaque bande. Parmi les caractéristiques les plus communément utilisées sont les coefficients Cepstraux. Ils sont obtenus par le logarithme de la transformée de Fourier du signal vocal dans chaque bande. Finalement, la mise en correspondance des coefficients Cepstraux permet de reconnaître la voix. Dans cette étape, généralement on fait appel à des approches fondées sur les modèles de Markov cachés, la quantification vectorielle, ou la déformation temps dynamique.

Figure I.17. Spectre d'un signal de voix **[16].**

Les avantages et les inconvénients de cette technique sont cités ci-dessous :

Avantages	Inconvénients
- Il est plus facile de protéger le lecteur que dans les autres technologies. - Impossible d'imiter la voix. - Non intrusif	- Sensible à l'état physique et émotionnel de l'individu. - Fraude possible par enregistrement. - Sensible aux bruits ambiants. - Taux de faux rejets et fausses acceptations élevés.

I.4.3 Les modalités biologiques :

Ce type de biométrie est basé sur l'identification de traits biologique particuliers

a- **ADN :**

L'analyse des empreintes génétiques est une méthode extrêmement précise d'identification, issue directement de l'évolution de la biologie moléculaire. L'information génétique d'un individu est unique car aucun membre de l'espèce ne possède la même combinaison de gènes codes dans l'Acide Désoxyribonucléique (ADN), constituant essentiel des chromosomes du noyau cellulaire. Le profil génétique, aujourd'hui couramment utilise pour des identifications judiciaires, fut introduit officiellement pour la première fois dans une affaire criminelle en 1986 par l'universitaire anglais Alec Jefreys **[12], [13].**

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

un prélèvement d'échantillon (sang, salive, sperme, cheveux, urine, peau, dents, etc.) qui rend cette technique très intrusive.

Figure I.17. l'ADN **[16]**

b- Odeur corporelle :

Chaque personne dégage une odeur qui lui est particulière **[14].** Les systèmes biométriques qui exploitent cette technologie analysent les composantes chimiques contenues dans l'odeur pour ensuite les transformer en données comparatives.

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

c. La reconnaissance de la thermographie faciale :

La quantité de chaleur émise par les différentes parti es du visage caractérise chaque individu. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc. contrairement à la reconnaissance de visage, la chirurgie plastique n'a que peu d'influence sur les thermo grammes faciaux.

Pour capturer l'image, il est possible d'utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge [29]. La capture peut se faire dans n'importe quelle condition d'éclairage et même dans le noir complet ce qui est un avantage

Supplémentaire sur la reconnaissance de visage classique.

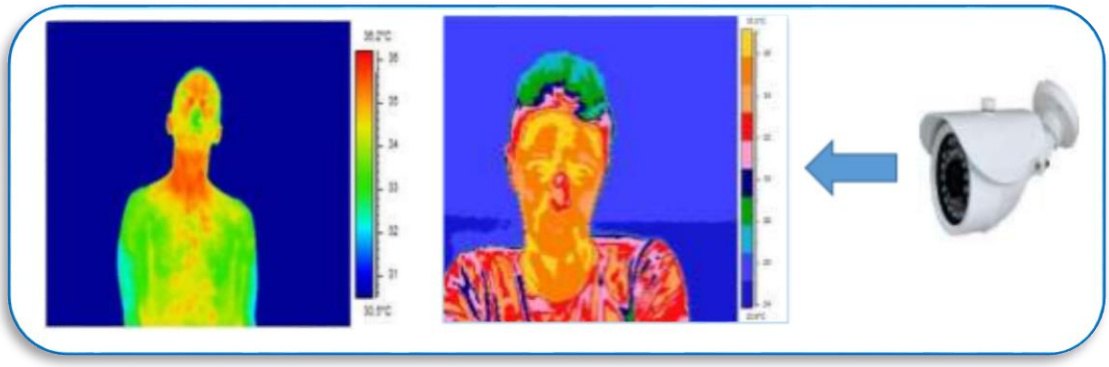

Figure I.18. La thermographie faciale [29].

I.4.4.Les multimodalités :

Les modalités biométriques cités précédemment peuvent être utilisées indépendamment comme elles peuvent être fusionnées, on peut définir la multimodalité comme la fusion de plusieurs systèmes biométriques en une seule, dans le but d'améliorer les performances de reconnaissance grâce à l'augmentation de la quantité d'information discriminante de chaque personne.

Le fait d'utiliser plusieurs modalités biométriques réduit les risques d'impossibilité d'enregistrement ainsi que les robustesses aux fraudes.

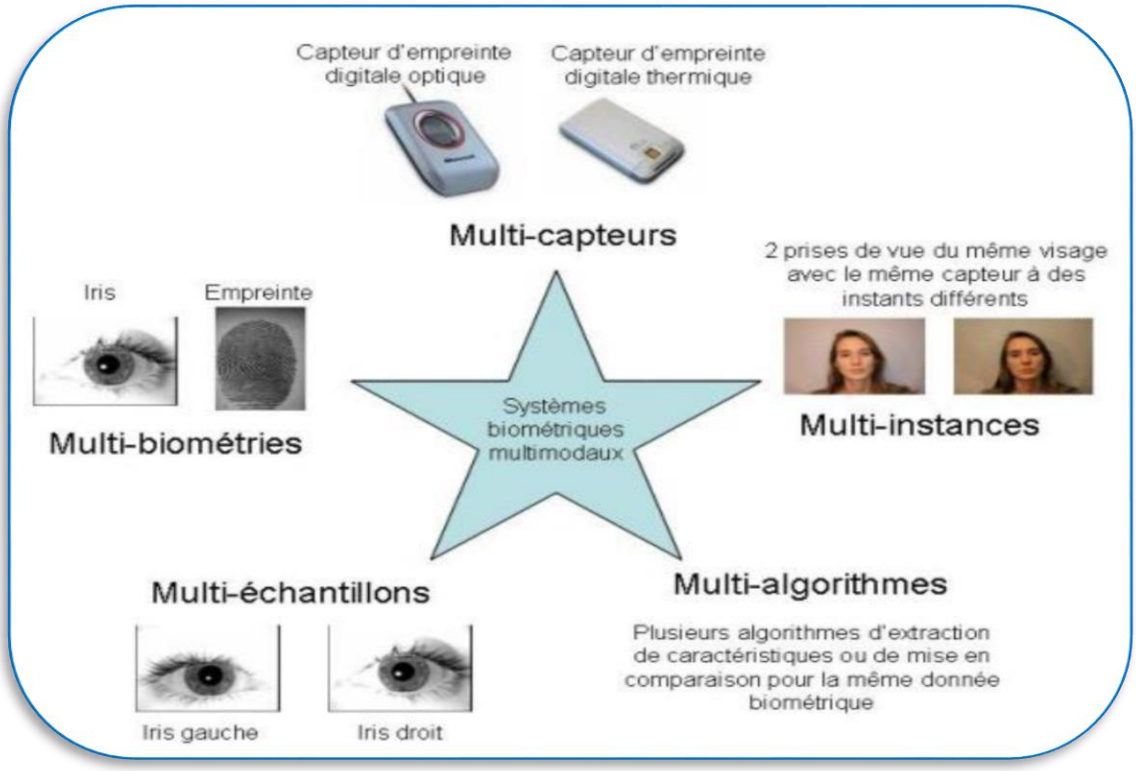

Figure I.19. La multimodalité **[16]**

I.5.Applications de la biométrie :

Les techniques biométriques sont appliquées dans plusieurs domaines et leur champ d'application couvre potentiellement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes. Les applications peuvent être divisées en trois groupes principaux :

- **Application commerciales :** telles que l'accès au réseau informatique, la sécurité de données électroniques, le commerce électronique, l'accès d'internet, l'ATM, la carte de crédit, le contrôle d'accès physique, le téléphone portable, le PDA, la gestion des registres médicales, l'étude de distances, etc.…
- **Applications de gouvernement :** telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc.…
- **Applications juridiques :** telles que l'identification de cadavre, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc.

On utilise aussi la biométrie dans le :

Contrôle d'accès aux locaux:

- Salles informatiques.
- Sites sensibles (service de recherche, site nucléaire).

Equipements de communication :

- Terminaux d'accès.
- Téléphones portables.

Systèmes d'informations :

- Lancement du système d'exploitation,
- Accès au réseau.
- Transaction (financière pour les banques, données entre entreprises).

Machines & Equipements divers :

- Lieu sensible (club de tir, police).
- Contrôle des adhérents dans les clubs privés.
- Contrôle des temps de présence.

Etat/Administration :

- Services sociaux (sécurisation des règlements).
- Système de vote électronique.

I.6.Caractéristiques biométriques :

Pratiquement, n'importe quelle caractéristique morphologique ou comportementale peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes **[15] :**

- **Universalité :** toutes les personnes à identifier doivent la posséder ;
- **Unicité :** l'information doit être aussi dissimilaire que possible entre les différentes personnes ;
- **Permanence :** l'information collectée doit être présente pendant toute la vie d'un individu ;
- **Collectabilité :** l'information doit être collectable et mesurable afin d'être utilisée pour les comparaisons ;
- **Acceptabilité :** le système doit respecter certains critères (facilité d'acquisition, rapidité, etc.) afin d'être employé.

Les caractéristiques biométriques ne possèdent pas toutes ces propriétés, ou les possèdent mais à des degrés différents. Le tableau 1.1, extrait de, compare les principales modalités biométriques selon les propriétés suivantes : Universalité (U), unicité (N), permanence (P), Collectabilité (C), acceptabilité (A) et performance (E).

Information	U	N	P	C	A	E
ADN	Oui	Oui	Oui	Faible	Faible	*****
Sang	Oui	Non	Oui	Faible	Non	*
Démarche	Oui	Non	Oui	Oui	Oui	***
Dynamique de frappe	Oui	Oui	Faible	Oui	Oui	****
Voix	Oui	Oui	Faible	Oui	Oui	****
Rétine	Oui	Oui	Faible	Oui	Faible	*****
Iris	Oui	Oui	Oui	Oui	Faible	*****
Visage	Oui	Non	Faible	Oui	Oui	****
Géométrie de la main	Oui	Non	Oui	Oui	Oui	****
Oreille	Oui	Oui	Oui	Oui	Oui	*****
Empreinte digitale	Oui	Oui	Oui	Oui	Moyen	****

Tableau I.1.comparaison des modalités biométriques selon les propriétés U, N, P, A, E

Ce tableau montre qu'aucune caractéristique n'est donc idéale et qu'elles peuvent être plus ou moins adaptées à des applications particulières. Par exemple, l'analyse basée sur l'ADN est une des techniques les plus efficaces pour vérifier l'identité d'un individu ou l'identifier. Néanmoins, elle ne peut pas être utilisée pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi, parce que personne ne serait prêt à donner un peu de sang pour faire la vérification. Le choix de la modalité est ainsi effectué selon un compromis entre la présence ou l'absence de certaines de ces propriétés selon les besoins de chaque application. A noter que le choix de la modalité biométrique peut aussi dépendre de la culture locale des usagers. En Asie, les méthodes nécessitant un contact physique comme les empreintes digitales sont rejetées pour des raisons d'hygiène alors que les méthodes sans contact sont plus répandues et acceptées telle que la reconnaissance de visage.

I.7.La part du marché :

I.7.1. Le marché mondial de la biométrie :

Régulièrement, un rapport sur le marché de la biométrie est édité par IBG (International Biometric Group) **[8].**Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance, et des développements industriels pour le marché de la biométrie actuel et futur.

La lecture de ce rapport est essentielle pour des établissements déployant la technologie biométrique, les investisseurs dans les entreprises biométriques, ou les développeurs de solutions biométriques. Le chiffre d'affaires de l'industrie biométrique incluant les applications judiciaires et celles du secteur public, se développe rapidement. Une grande partie de la croissance sera attribuable au contrôle d'accès aux systèmes d'information (ordinateur / réseau) et au commerce électronique, bien que les applications du secteur public continuent à être une partie essentielle de l'industrie.

On ne prévoit que le chiffre d'affaires des marchés émergents (accès aux systèmes d'information, commerce électronique et téléphonie, accès physique et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens).

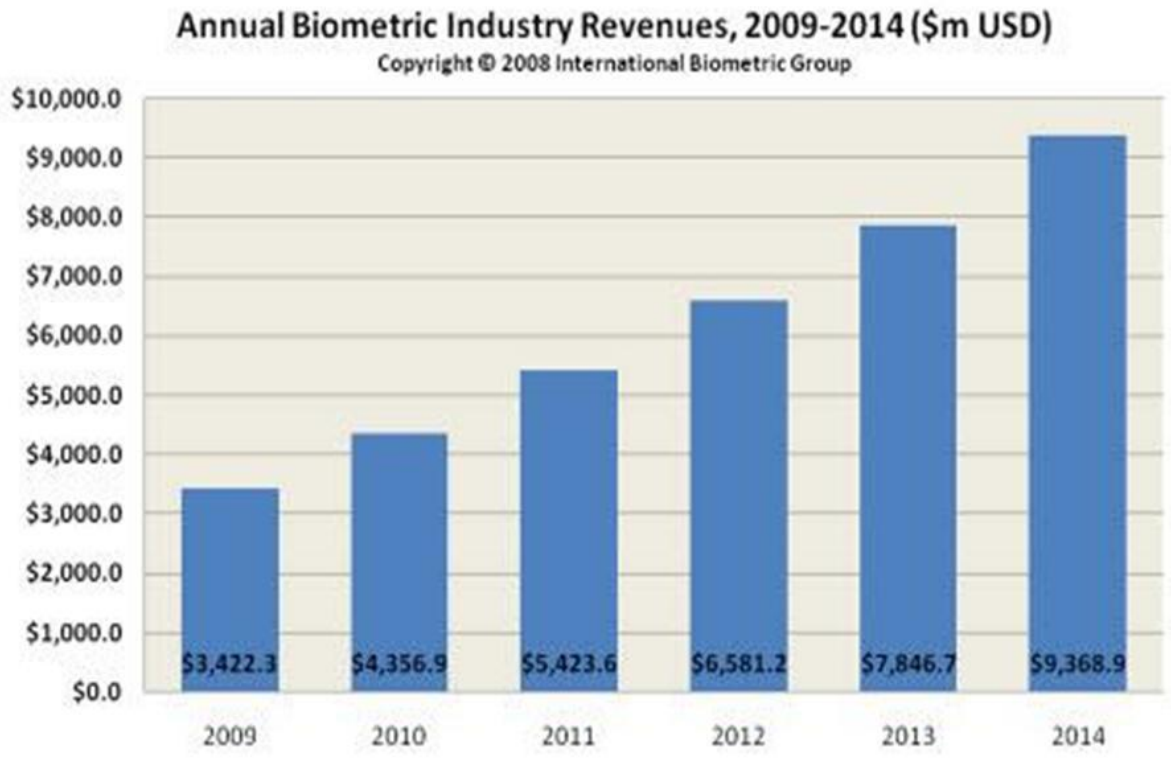

Figure I.20: Evolution du marché international de la biométrie **[8].**

I.7.2. Les parts de marché par technologie :

Les empreintes digitales continuent à être la principale technologie biométrique en termes de part de marché, près de 50% du chiffre d'affaires total (hors applications judiciaires).

La reconnaissance du visage, avec 12% du marché (hors applications judiciaires), dépasse la reconnaissance de la main, qui avait avant la deuxième place en termes de source de revenus après les empreintes digitales.

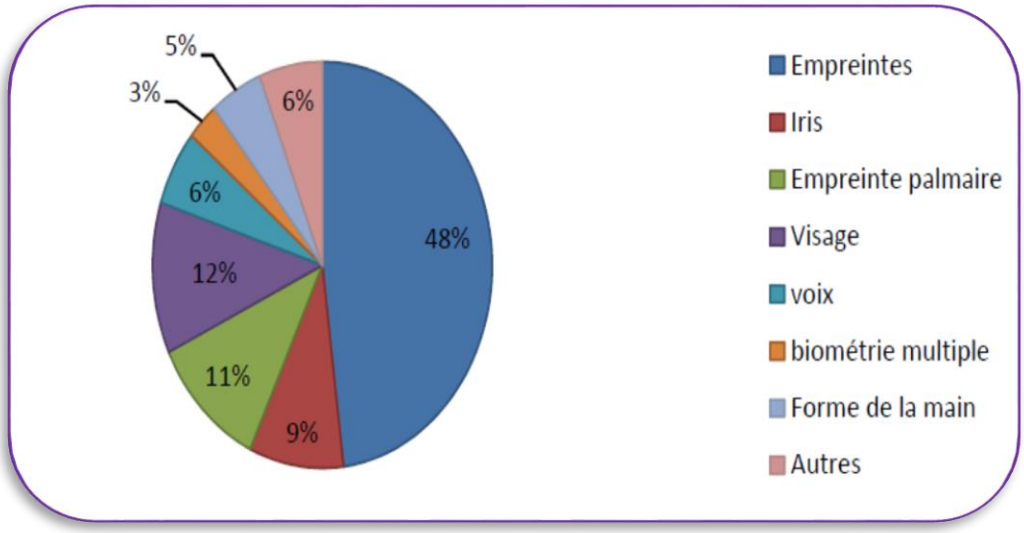

Figure I.21.Parts de marché des différentes méthodes biométriques **[8].**

Conclusion :

Nous avons introduit dans ce premier chapitre la notion de la biométrie et les systèmes biométriques. Après une introduction sur la biométrie, nous avons exposé les différentes modalités d'un système biométrique. Nous avons ensuite présenté l'architecture et le principe de fonctionnement des systèmes biométriques, ainsi que l'évaluation et la Mesure de performance.

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

CHAPITRE II

Système de Reconnaissance Faciale

Introduction :

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

Dès lors, la reconnaissance des visages a connu un fort développement et reste un domaine qui suscite toujours des interrogations et un engouement par les chercheurs.

Dans ce chapitre, nous expliquons la reconnaissance de visage, ces applications et nous donnons un aperçu sur les méthodes de reconnaissance de visage qui existent.

II .1. Pourquoi le visage ?

Les principaux critères d'évaluation des techniques biométriques (coût, intrusivité, précision, effort) nous permettent de comparer les différentes modalités biométriques, et ainsi déduire la place de la reconnaissance du visage parmi les autres techniques.

la reconnaissance du visage s'avère plus avantageuse, d'une part c'est une méthode non intrusive, c'est-à-dire elle n'exige pas la Coopération du sujet (en observant les individus à distance), et d'une autre part les capteurs utilisés sont peu coûteux (une simple caméra) contrairement à l'empreinte digitale et l'iris où le sujet devra être très proche du capteur et devra coopérer pour l'acquisition de l'image sans oublier le coût de l'équipement nécessaire pour l'acquisition (équipement spécial coûteux).[32]

En conséquence, La reconnaissance du visage représente la modalité la plus commune, populaire et reste la plus acceptable par rapport aux autres méthodes.

II.2. Système de reconnaissance faciale :

Les systèmes de reconnaissance faciale sont des systèmes automatisés capables d'identifier des individus en fonction des caractéristiques de leur visage telles que l'écartement des yeux, des arêtes du nez, des commissures des lèvres, des oreilles, menton, etc. Ces caractéristiques

sont analysées puis comparées à une base de données existante afin d'identifier une personne ou de vérifier son identité.

Dans un système de reconnaissance de visages, depuis son acquisition, l'image suit un processus bien précis pour arriver à déterminer ou à vérifier l'identité du porteur de visage.

Les deux premières étapes s'effectuent en amont du système (détection [39] et normalisation [40]) et les deux dernières représentent la reconnaissance à proprement dit (extraction et comparaison des caractéristiques).

Ce processus peut être présenté par le diagramme suivant :

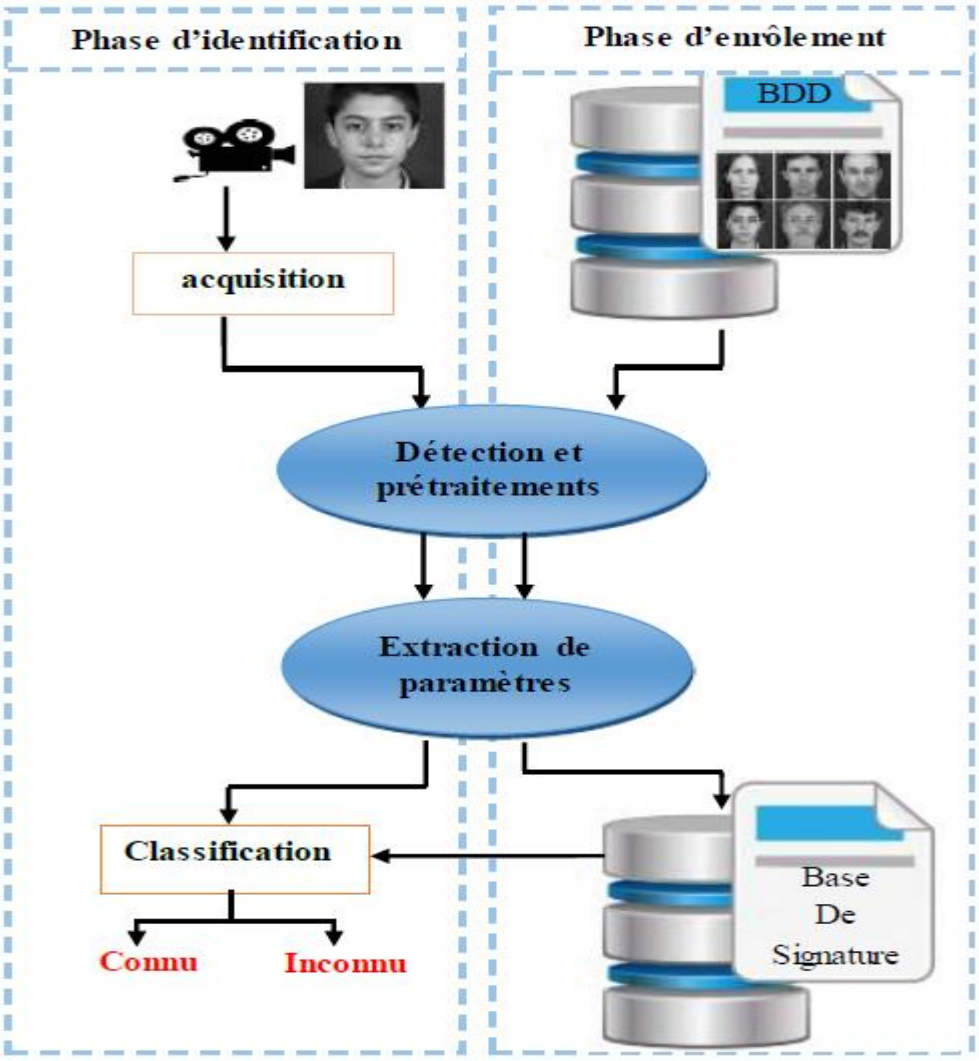

Figure II.1. Le processus de reconnaissance de visage.

En général, l'image d'une personne dans un système de biométrie faciale suit les étapes suivantes :

II.2.1. Acquisition :

Cette étape consiste [17] 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. L'image dans cette étape est dans un état brut ce qui engendre un risque de bruit qui peut dégrader les performances du système.

II.2.2. Détection de visages :

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. 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 [33].

II.2.3. 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. 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 de l'histogramme 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. [11]

II.2.4. Extraction de paramètres et classification :

- **Extraction des paramètres** :

On doit extraire les informations utiles qui reviennent à établir un modèle du visage (vecteur de caractéristiques). Ces informations nécessaires pour que le visage d'une personne ne ressemble pas à celui d'un autre, en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition. [34]

- **Classification des paramètres** :

Ces informations seront ensuite classées, autrement dit, affectés à la classe la plus proche, les individus ayant des similarités sont regroupés dans la même classe. Ces classes varient selon le type de décision.

L'efficacité de cette étape à une influence directe sur la performance du système de reconnaissance de visage [34].

II.2.5. L'apprentissage :

C'est l'étape où on fait apprendre les individus au système, elle consiste à mémoriser les paramètres, après extraction et classification, dans une base de données bien ordonnées pour faciliter la phase de reconnaissance et la prise d'une décision, elle est en quelque sorte la mémoire du système. [34]

II.2.6. La décision

C'est l'étape qui fait la différence entre un système d'identification d'individus et un autre de vérification. 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) [34].

II.3. Méthodes de reconnaissance faciale :

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

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

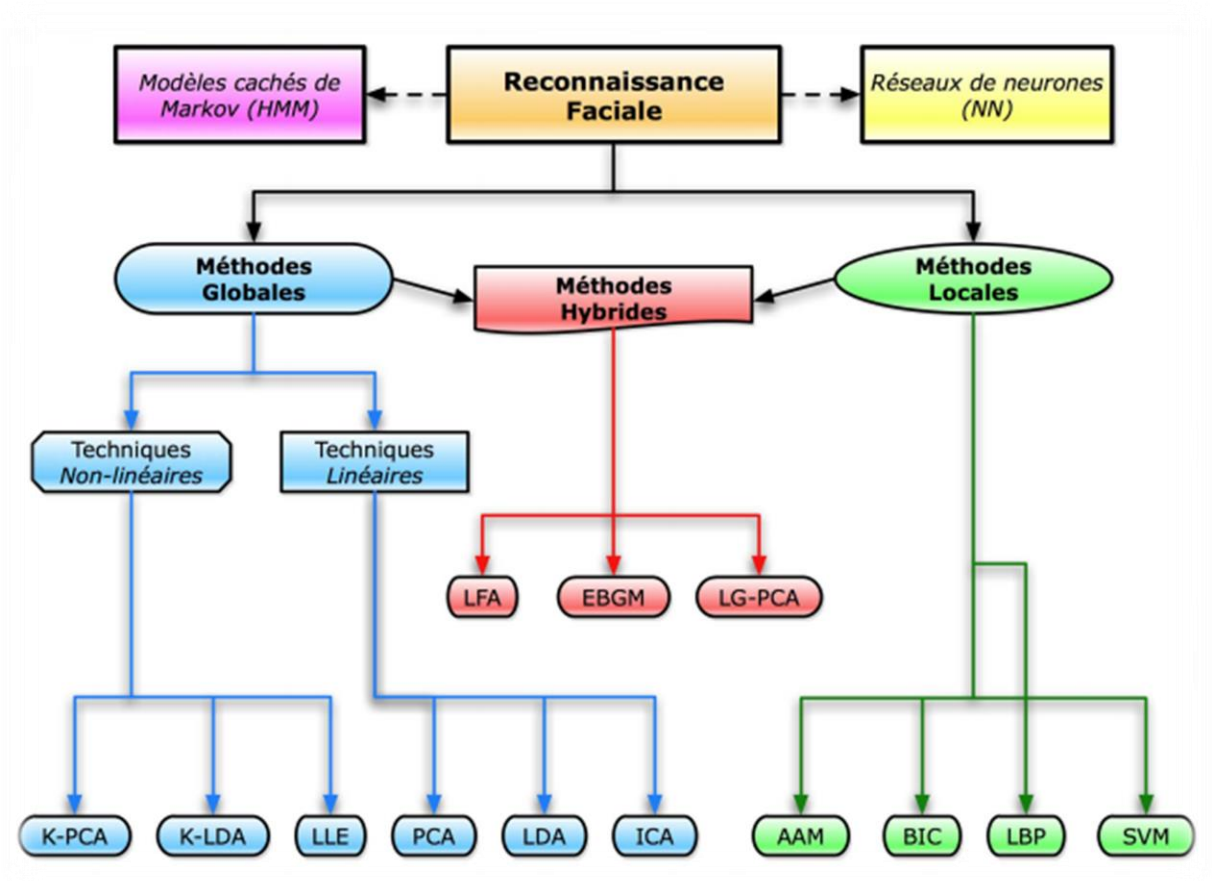

Figure II.2. Classification des méthodes principales utilisées dans la reconnaissance de visage [36].

II.3.1. Méthodes globales

Les méthodes globales sont basées sur des techniques d'analyse statistique bien connues. Il n'est pas nécessaire de repérer certains points caractéristiques du visage (comme les centres des yeux, le centre de la bouche, etc.) à part pour normaliser les images. Dans ces méthodes, les images de visage (qui peuvent être vues comme des matrices de valeurs de pixels) sont traitées de manière globale et sont généralement transformées en vecteurs, plus faciles à manipuler.

L'avantage principal des méthodes globales est qu'elles sont relativement rapides à mettre en œuvre et que les calculs de base sont d'une complexité moyenne. En revanche, elles sont très sensibles aux variations d'éclairement, de pose et d'expression faciale. Ceci se comprend aisément puisque la moindre variation des conditions de l'environnement entraîne des changements inéluctables dans les valeurs des pixels qui sont traités directement.

Ces méthodes utilisent principalement une analyse de sous-espaces de visages. [11] nous pouvons distinguer deux types de techniques parmi les méthodes globales : les techniques linéaires et les techniques non linéaires.

II.3.1.1. Techniques linéaires :

Les techniques linéaires réalisent une projection linéaire des données d'un espace de grande dimension (par exemple, l'espace de l'image originale) sur un sous -espace de dimension inférieure. Cependant, ces techniques linéaires sont sensibles aux conditions de luminosité notamment, et plus généralement aux variations non convexes [41]. Ainsi, l'utilisation de distances classiques dans l'espace projeté ne permet pas toujours de réaliser une bonne classification entre les classes « visages » et « non visages ». Ce facteur crucial limite le pouvoir des techniques linéaires pour obtenir une détection et une reconnaissance du visage très précises.

Parmi les méthodes globales les plus connues il y'a ACP (Analyse en Composante Principale), ADL (Analyse Discriminante Linéaire) et ACI (Analyse en Composante Indépendantes)

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

L'algorithme PCA est né des travaux de MA. Turk et AP. Pentaland au MIT Media Lab [35]. Aussi connu sous le nom Eigen faces car il utilise des vecteurs propres et des valeurs propres (respectivement Eigen vectors et Eigen values en anglais). L'idée principale consiste à exprimer les images de départ selon une base de vecteurs orthogonaux particuliers. Ces fameux vecteurs propres contenant des informations indépendantes d'un vecteur à l'autre. Ces nouvelles données sont donc exprimées d'une manière plus appropriée à la reconnaissance du visage [36]. Les images originales peuvent être reconstituées par combinaison linéaire de ces vecteurs propres. Les représentations graphiques de ces vecteurs rappellent un peu des images fantômes, chacune mettant en avant une partie du visage, on les appelle Eigen faces. (Figure II.3). Tout d'abord, l'algorithme PCA est une méthode globale utilisant en premier lieu les niveaux de gris des pixels d'une image. Sa simplicité à mettre en œuvre contraste avec une forte sensibilité aux changements d'éclairement, de pose et d'expression faciale. [36]

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

Le principe selon lequel on peut construire un sous-espace vectoriel en ne retenant que les

"meilleurs" vecteurs propres, tout en conservant beaucoup d'information utile, fait du PCA

Un algorithme efficace et couramment utilisé en réduction de dimensionnalité où il peut alors être utilisé en amont d'autres algorithmes (comme le ADL par exemple).

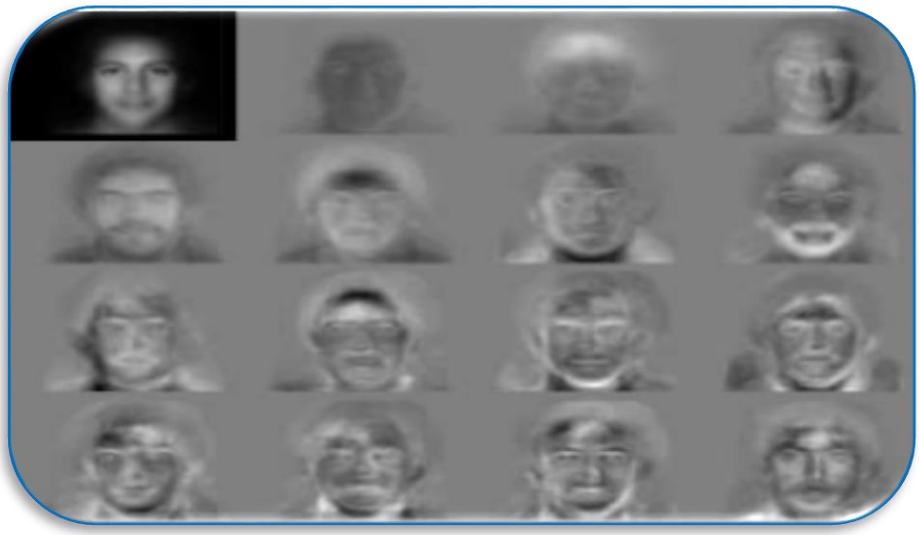

Figure II.3. Image moyenne et les 15ères Eigen faces.

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

L'algorithme LDA est né des travaux de Belhumeur et al. De la Yale University (USA), en 1997. Il est aussi connu sous le nom de Fisher faces. Contrairement à l'algorithme PCA, le LDA effectue une véritable séparation de classes Pour pouvoir l'utiliser, il faut donc au préalable organiser la base d'apprentissage d'images en plusieurs classes : une classe par personne et plusieurs images par classe. Le ADL analyse les vecteurs propres de la matrice de dispersion des données, avec pour objectif de maximiser les variations interclasses tout en minimisant les variations intra classes [36].

Tout d'abord, l'algorithme ADL permet d'effectuer une véritable séparation de classes, selon un critère mathématique qui minimise les variations entre les images d'un même individu (variations intra classe) tout en maximisant les variations entre les images d'individus différents (variations interclasses) (Figure. II.4). Cependant, pour des problèmes (sous échantillonnés) en reconnaissance du visage, c'est-`a-dire lorsque le nombre d'individus à traiter est plus faible que la résolution de l'image, il est difficile d'appliquer le ADL qui peut alors faire apparaitre des matrices de dispersions singulières (non inversibles).

Figure II.4. Exemple de six classes utilisant ADL.

- **L'analyse en composantes indépendantes ACI :**

ACI est une généralisation de l'algorithme ACP avec lequel il coïncide dans le cas de données gaussiennes. Elle a été introduite par les spécialistes du traitement de signal afin de trouver une solution au problème de séparation des sources lorsque la fonction de mélange F est inconnue [11]. Le traitement consiste à extraire les composantes linéaires d'une observation multi variée afin qu'elles soient aussi indépendantes que possible. Elle sert généralement à analyser les signaux issus de multiples capteurs pour lesquels la nature exacte des sources est inconnue, d'où vient son appellation de séparation aveugle de sources.

Par exemple on enregistre les conversations se tenant dans une salle où plusieurs personnes parlent simultanément, le signal perçu est une combinaison linéaire de ces différentes conversations [42]. La séparation de ces conversations peut alors se faire en extrayant leurs signaux individuels, que l'on suppose indépendants entre eux.

Bien que les méthodes globales linéaires soient efficaces, et aient eu beaucoup de succès, elles ne sont pas assez précises. Ceci est dû à des transformations non -linéaires, une simple modification de la luminosité déforme les images de visages de façon non linéaire.

II.3.1.2. Techniques non linéaires :

Afin de pouvoir traiter le problème de la non-linéarité, des techniques globales non linéaires ont été développées, souvent à partir des techniques linéaires. Ainsi l'Analyse en Composantes principales à Noyaux (ou « Kernel –PCA ») et l'Analyse Discriminante linéaire à Noyaux (ou « Kernel–LDA ») utilisent la notion mathématique des noyaux en étendant les techniques linéaires l'ACP et la LDA.

D'autres techniques non linéaires ont également été utilisées dans le contexte de la reconnaissance faciale :

– le MultiDimensional Scaling (MDS),
– l'Isomap,
– les diffusion maps,
– le Local Linear Embedding (LLE)
– les Laplacian ei genmaps
– le Hessian LLE
– le Local Tangent Space Analysis (LTSA)
– les approches neuronales

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 [32]. 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.

II.3.2. Méthodes locales :

Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l'on possède sur la morphologie du visage et s'appuient en général sur des points caractéristiques de celui-ci.

Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace de caractéristiques local et en utilisant des filtres d'images appropriés, de manière à ce que les distributions des visages soient moins affectées par divers changements.

Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Toutefois, elles sont plus lourdes à utiliser puisqu'il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection [11].

Dans cette catégorie, on trouve plusieurs méthodes comme : HMM (Hidden Markov Models), RNA (réseaux de neurones) et SVM (Machines à Vecteur de Support).

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

C'est une nouvelle technique qui a été proposée parV.Vapnik en 1995 [37]. Elle est utilisée dans plusieurs domaines statistiques (classement, régression, fusion, … etc.). Plusieurs travaux ont montré son efficacité et principalement en traitement d'images depuis son introduction dans le domaine de reconnaissance de formes.

L'idée essentielle de cette approche consiste à projeter les données de l'espace d'entrée (appartenant à des classes différentes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables [38]. Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la fonction de classement séparant les classes tels que : Les vecteurs appartenant aux différentes classes se trouvent de différents côtés de l'hyper plan. la plus petite distance entre les vecteurs et l'hyperplan (la marge) soit maximale.

- **Réseaux de neurones :**

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 [43]. 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. On note en particulier l'architecture MLP (Multi -Layer Perceptron, Perceptron Multicouches), l'architecture RBF (Radial Basis Function, Fonctions à base radiale) et l'architecture SOM (Self -Organizing Maps, Cartes auto Organisatrices de Kohonen) [11]. Dans le cas de la reconnaissance de 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.

- **Hidden Markov Modals (HMM) :**

Le modèle de Markov cachés HMM sont un ensemble de modèles statistiques utilisés pour caractériser les propriétés statistiques d'une image. L'image est divisée en N régions significatifs qui sont par exemple pour le visage : les cheveux, le front, les yeux, le nez et la bouche. Chacune de ces régions est ensuite assignée à un état Si (S1 : cheveux ; S2 : front ; S3 : yeux ; S4 : nez ; S5 : bouche).

Chaque état est caractérisé par une fonction de probabilité, estimée sur la base des images exemples. Le principe de HMM [43], lors de la localisation du visage, est de toujours extraire les mêmes régions de l'image d'entrée et de vérifier si les objets caractéristiques apparaissent dans le même ordre que défini dans le modèle HMM.

- **LBP (Local Binary Patterns) :**

Les motifs binaires locaux (LBP) sont des caractéristiques utilisées en vision par ordinateur pour la classification des textures, la détection et le suivi des objets mobiles dans une séquence d'image.
Ces descripteurs se basent sur la comparaison de niveau de luminance d'un pixel à analyser avec celles de ces proches voisins et la valeur qui le caractérise est calculé par leur somme pondérée par un certains poids (code binaire).
Selon l'échelle du voisinage utilise, certaines zones d'intérêts tels des coins ou des bords peuvent être détectées par ce descripteur.
Par la suite, nous présentons les principaux motifs binaires locaux (LBP), et nous élaborons deux versions qui s'adaptent mieux au suivi d'objet mobile.
Le concept du LBP consiste à générer un motif binaire pour chaque pixel P de l'image à analyser. En effet, tous les voisins dans une région de taille R (exemple 3x3) prendront alors une valeur "1" si leur valeur est supérieure ou égale au niveau de gris de pixel à analyser (central) et "0" autrement.
Les pixels de ce motif binaire sont alors multipliés par des poids (code binaire) et sommés afin d'obtenir un code LBP du pixel courant, par conséquent on obtient une image sur 8 bits.

II.3.3. Méthodes hybrides :

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction

de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales [11].

Parmi les algorithmes de reconnaissance de cette méthode nous citons l'EBGM.

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

A partir d'une image de visage, cette méthode localise des points caractéristiques comme les coins des yeux, de la bouche et le nez. Un treillis élastique virtuel est ensuite appliqué sur l'image du visage à partir de ces points. Chaque point représente un nœud étiqueté auquel nous associons un jeu de coefficients d'ondelettes complexes de Gabor, appelés Jet [36]. Dans cette approche, la reconnaissance se fait par la mesure de similarité entre les différents Jets et les longueurs des segments du treillis de deux images.

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

II.4. Principales difficultés de la reconnaissance faciale :

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 représentent 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 [11]. 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.

II.4.1 Changement d'illumination :

Les variations d'éclairage rendent la tache de reconnaissance de visages très difficile. En effet, le changement d'apparence d'un visage du a l'illumination, se révèle parfois plus critique que la différence physique entre les individus, et peut entrainer une mauvaise classification des images d'entrée [11].

Figure II.5. Exemple de variation d'éclairage [11].

II.4.2. Variation de pose :

Le taux de reconnaissance de visage baisse considérablement quand des variations de pose sont présentes dans les images. La variation de pose est considérée comme un problème majeur pour les systèmes de reconnaissance faciale. Quand le visage est de profil dans le plan image (orientation < 30°), il peut être normalisé en détectant au moins deux traits faciaux (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible [11].

Figure II.6. Exemple de variation de pose [11].

II.4.3 Expressions faciales

La déformation du visage qui est due aux expressions faciales est localisée 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 entraine forcement 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. [11]

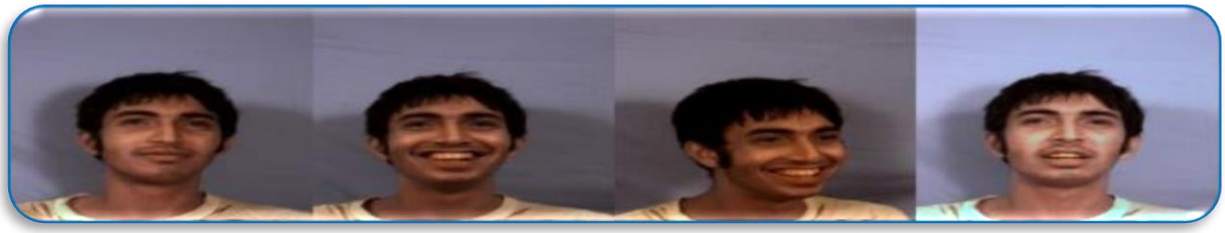

Figure II.7. Exemples de variation d'expressions [11].

II.4.4. Présence ou absence des composants structurels

La présence des composants structurels telle que la barbe, la moustache, ou bien les lunettes peut modifier énormément les caractéristiques faciales telles que la forme, la couleur, ou la taille du visage. De plus, ces composants peuvent cacher les caractéristiques faciales de base causant ainsi une défaillance du système de reconnaissance [11].

II.4.5. Les vrais jumeaux

Qui ont le même indicatif d'ADN, peuvent tromper les personnes qui ne les connaissent pas (les personnes familières avec les jumeaux ont reçu une grande quantité d'information sur ces derniers et sont donc beaucoup plus qualifies à distinguer les jumeaux.).

Il est peu probable que la vérification automatique de visage, ne pourra jamais détecter les différences très subtiles qui existent entre les jumeaux [11].

Conclusion :

Dans ce chapitre, nous avons présenté une technologie utilisée dans les systèmes biométriques pour l'identification de personnes qui est la reconnaissance faciale. Cette étude nous a permis de constater que la reconnaissance de visage suscite de plus en plus l'intérêt de la communauté scientifique, car elle présente plusieurs challenges et verrous technologiques. Enfin, nous avons mis en évidence les différentes difficultés inhérentes à la reconnaissance automatique de visages.

Dans le chapitre suivant, nous enchainerons avec l'étude d'une des méthodes de reconnaissance dite l'opérateur LBP qui sera utilisée plus tard dans la réalisation de notre système de reconnaissance de visages.

PARTIE II

EXTRACTION DES PARAMETRES ET CLASSIFICATION.

CHAPITRE III

Extraction des Caractéristiques et Classification

Introduction :

Après la détection et la normalisation du visage, les informations discriminantes du visage sont extraites pour constituer le modèle du visage, celui-ci sera utilisé par la suite dans la classification pour que le système décide de l'identité de la personne.

Plusieurs techniques d'extraction de caractéristiques faciale ont été proposées. Leur défaut majeur est leurs incapacités à répondre aux contraintes des applications temps réel, à cause de la complexité et la lourdeur des calculs, qui diminuent considérablement les performances des systèmes **[45]**.

Ces dernières années plusieurs méthodes discriminatives et efficaces en terme de calculs ont été proposées, dont les méthodes locales basées apparence qui utilisent le descripteur LBP (**Local binary pattern**) pour l'extraction de l'information pertinente, ce dernier a été développé spécialement pour accélérer les calculs et répondre aux contraintes des applications temps réels.

Ce chapitre se structure en deux parties : la première traite l'étude de l'opérateur LBP et ces variantes, puis leurs utilisations comme descripteur faciale, la seconde traite la reconnaissance faciale sur une image fixe basée sur l'approche LBP

III .1. Pourquoi le motif binaire local (LBP) :

Le succès de LBP **[48]** comme descripteur textural est dû à la simplicité de ses calculs qui lui permet d'analyser les images en un temps-réel, et à son invariance au changement mono-tonique de l'illumination, un changement global de la luminosité de l'image n'implique aucune variation dans l'image LBP correspondante.

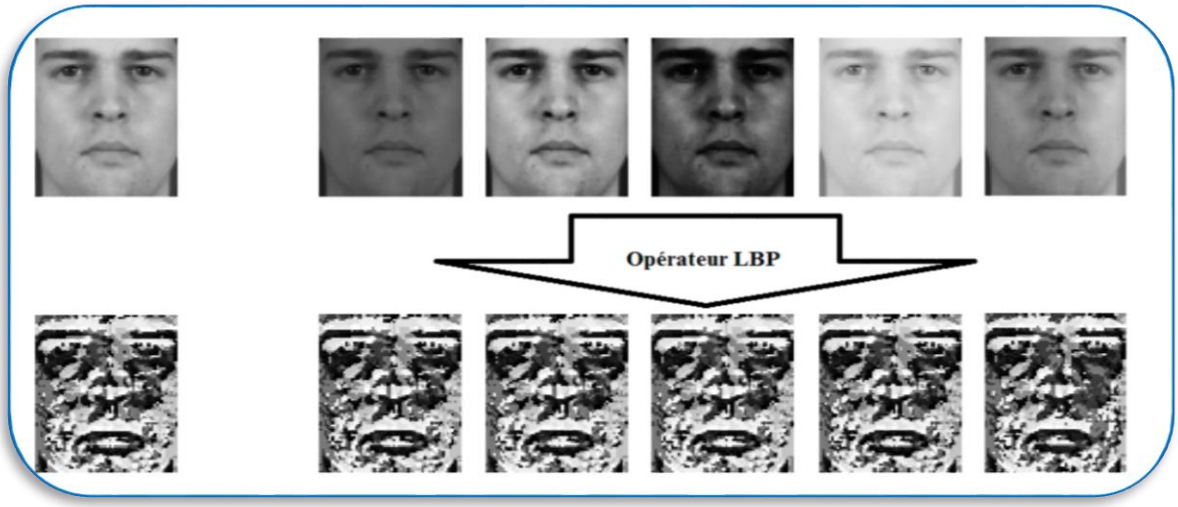

Figure III.1 : la stabilité de LBP au changement d'illumination **[48]**

III.2. Définition de la texture :

Dans le domaine du traitement de l'image et de la vision, il n'existe pas de définition satisfaisante de la texture. En effet, Les définitions mathématiques construites à partir de propriétés statistiques sont soit trop générales et imprécises, soit trop restrictives pour s'adapter à la diversité des cas rencontrés **[46].** De ce fait, il existe plusieurs définitions de la texture, chacune d'elles met en évidence certains aspects de cette dernière et qui permettent de mieux la cerner et l'appréhender. En voici quelques-unes des plus célèbres :

« Une région dans une image contient une texture constante si un ensemble de statistiques locales ou autres propriétés de la fonction image sont constantes, varient faiblement ou sont approximativement périodiques » **[51].**

« Une image texturée est décrite par le nombre et les types de ses primitives tonales ainsi que leurs orientations spatiales. Elle ne peut pas être analysée sans une vue de la primitive tonale de référence. Pour certaines surfaces ayant un ton de gris flouté, il existe une échelle telle que la texture est inexistante. Au fur et à mesure que la résolution augmente, on observe une texture fine puis une texture grossière » **[52].**

« 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 » **[53].**

III.3. Définition de LBP :

Les motifs binaires locaux ont initialement été proposés par *Ojala* en 1996 afin de caractériser les textures présentes dans des images en niveaux de gris **[54].** Ils consistent à attribuer 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 calculées en comparant le niveau de gris du pixel central *P* aux valeurs des niveaux de gris des pixels voisins.

Le concept du LBP est simple, il propose d'assigner un code binaire à un pixel en fonction de son voisinage. Ce code décrivant la texture locale d'une région est calculé par seuillage d'un voisinage avec le niveau de gris du pixel central. Afin de générer un motif binaire, tous les voisins prendront alors une valeur "1" si leur valeur est supérieure ou égale au pixel courant et "0" autrement. Les pixels de ce motif binaire sont alors multipliés par des poids et sommés afin d'obtenir un code LBP du pixel courant. On obtient donc pour toute l'image, des pixels dont l'intensité se situe entre 0 et 255 comme dans une image à 8 bits ordinaire. Plutôt que de décrire

l'image par la séquence des motifs LBP, on peut choisir comme descripteur de texture un histogramme de dimension 255.

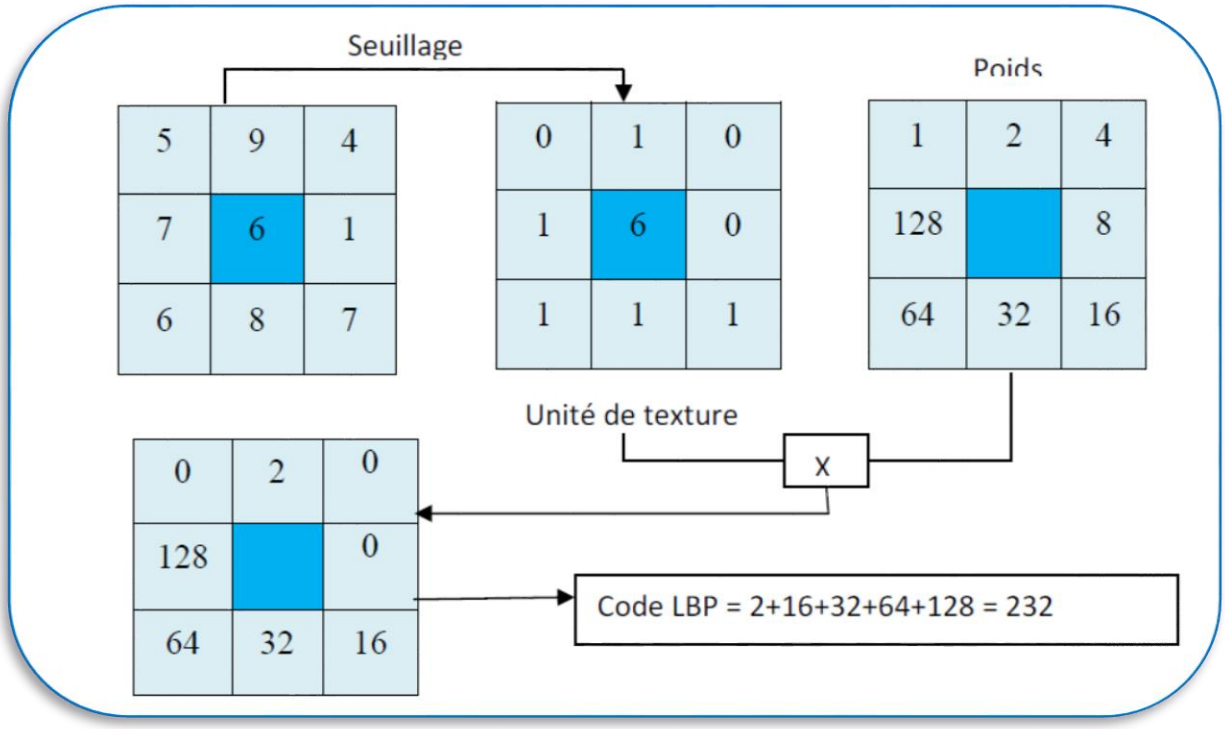

Figure III.2 : Calcul de l'opérateur LBP de base pour un pixel de l'image **[11].**

LBP (local Binary Pattern) **[11]** est une méthode mathématique dont son but consiste à caractériser la texture d'une image par calcule le code LBP pour tous les pixels d'image ensuite on calcule l'histogramme de cette image LBP pour former un vecteur de caractéristiques représentant l'image faciale.

III.4. LBP circulaire :

La technique LBP a été étendue ultérieurement en utilisant des voisinages de taille déférente **[11].** Dans ce cas, 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. Pour obtenir les valeurs des P points échantillonnés dans le voisinage pour tout rayon R, une interpolation est nécessaire. On adopte la notation (P, R) pour définir le voisinage de P points de rayon R d'un pixel. La *Figure III. 2* illustre trois voisinages pour des valeurs de R et P différentes.

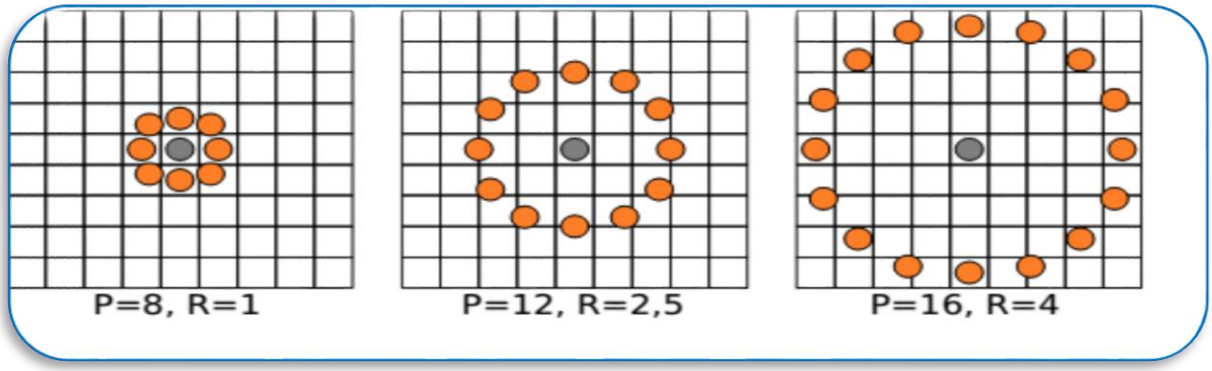

Figure III.3 : Exemples de différents voisinages circulaires pour les LBP **[60].**

Soient g_c le niveau de gris du pixel central, g_k (k = 1 ... P) les niveaux de gris de ses voisins **[47].** On note 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 :

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

Avec :

- $s(x) = \begin{cases} 1 & si \quad x \geq 0 \\ 0 & si \quad x < 0 \end{cases}$
- $g_c = I(x_c, y_c)$ valeur du pixel central
- $g_k = I(x_k, y_k)$ valeur du pixel voisin
- $(x_k, y_k) = (x_c + Cos(2\pi k/P), y_c - Sin(2\pi k/P))$

Où (x_c, y_c) sont les coordonnées du pixel courant, $LBP_{P,R}$ est le code LBP pour le rayon R et le nombre de voisins P. L'opérateur LBP obtenu avec P = 8 et R = 1 ($LBP_{8,1}$) est très proche de l'opérateur LBP d'origine. La principale déférence est que les pixels doivent d'abord être interpolés pour obtenir les valeurs des points sur le cercle (voisinage circulaire au lieu de rectangulaire).

III.5 LBP uniformes :

Une autre variante à l'opérateur original (LBP) emploie les dénommés motifs uniformes LBP invariant par rotation **[55]**. Pour ceci, une mesure d'uniformité d'un motif est employée : *U* ("motifs"). Celui-ci représente le nombre de transitions de bit de 0 à 1 ou vice versa lorsque la configuration binaire est considérée circulaire. De ce fait, un motif binaire local est appelé uniforme si sa mesure d'uniformité est au plus égale à 2.

Afin d'illustrer le principe des motifs uniformes, prenons les exemples suivants : les modèles 00000000 (transitions 0), 01110000 (2 transitions) et 11001111 (2 transitions) sont uniformes tandis que les modèles 11001001 (4 transitions) et 01010011 (6 transitions) ne le sont pas.

Par ailleurs, les modèles uniformes laissent voir la méthode de LBP comme approche d'unification des modèles statistiques et structuraux traditionnellement divergents de l'analyse de texture [55]. En effet, chaque Pixel est marqué avec le code du primitif de texture qui correspond le mieux au voisinage local, ainsi chaque code LBP peut être considéré comme un Micro-textons.

L'utilisation d'un code LBP uniforme, noté LBP^{u2} a deux avantages. Le premier est le gain en mémoire et en temps calcul. Le deuxième est que LBP^{u2} permet de détecter uniquement les textures locales importantes, comme les spots, les fins de ligne, les bords et les coins (figure 3.3 pour des exemples de ces textures particulières). Dans cette figure, les uns sont représentés comme des cercles sombres et les zéros comme des cercles clairs.

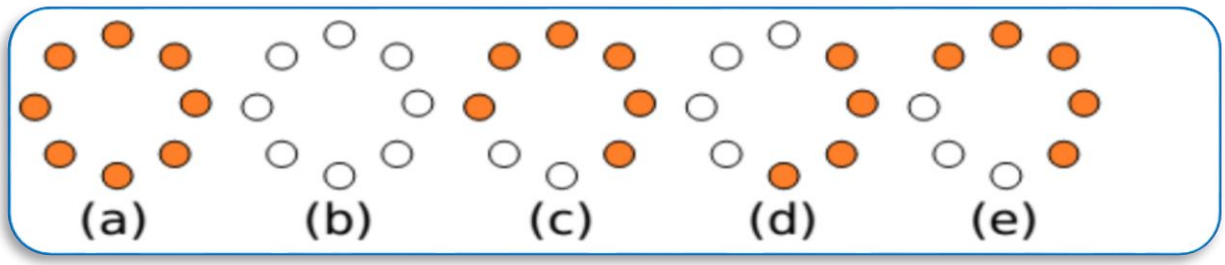

Figure III.4 : Primitives extraites par les motifs binaires locaux **[60].**

(a) et **(b)** correspondent à des tâches respectivement claires et sombres, **(c)** est une fin de ligne, **(d)** une bordure et **(e)** est un coin.

OJALA a constaté que seuls 58 des 256 motifs LBP sont uniformes mais expérimentalement, il a été constaté que 90% des patterns rencontrés dans les images sont uniformes **[56].**

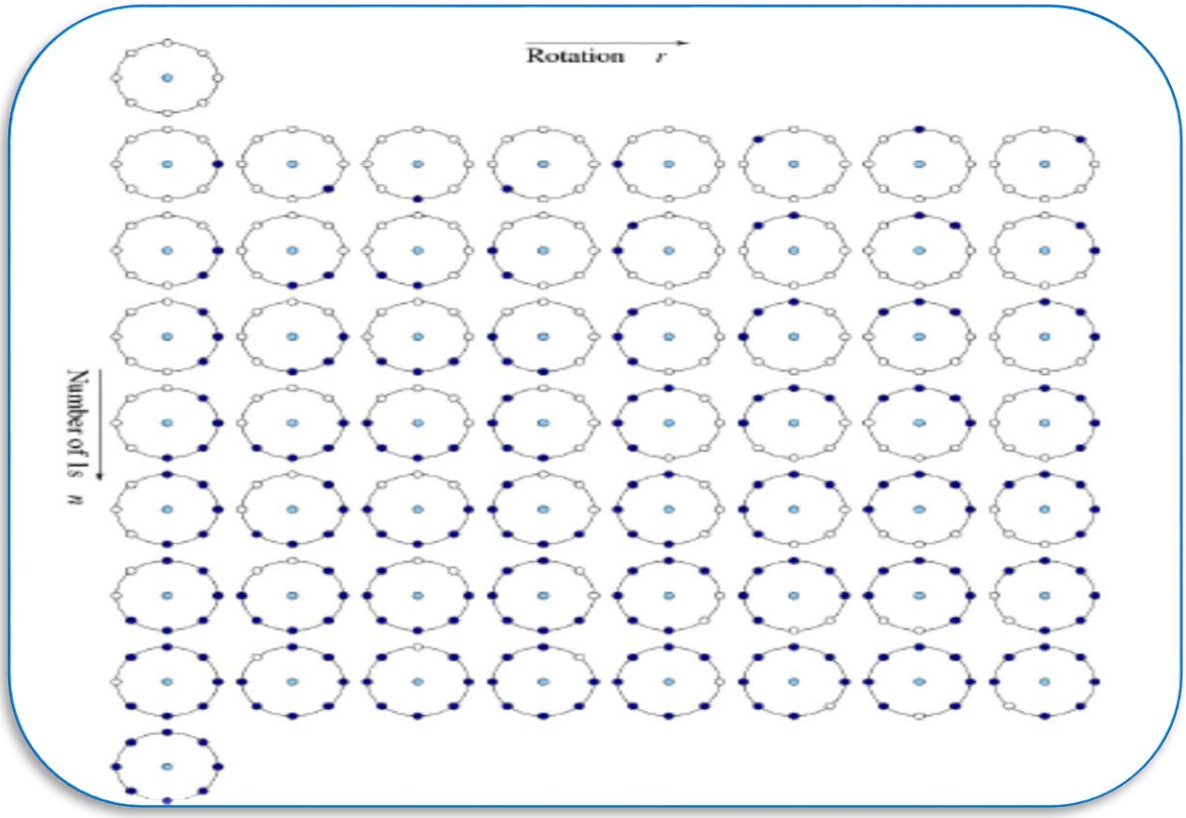

Figure III-5 : Les 58 différents motifs uniformes dans un voisinage (8, R) **[57]**

III.6. Histogramme LBP :

L'histogramme LBP est une mesure statistique permettant de représenter la distribution des codes LBP, cette représentation unidimensionnelle 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 H_{LBP} se fait à partir de l'image $LBP_{P,R}$ noté M_{LBP} par la formule suivante :

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

Où :

- I : fonction indicatrice

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

- W : largeur de l'image LBP
- H : longueur de l'image LBP
- P : nombre de pixels du voisinage
- i : code LBP

Figure III.6 : exemple d'histogramme LBP

III.7. Reconnaissance de visage avec la LBP :

Une fois le code LBP calculé pour tous les pixels de l'image **[11],** 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 et l'histogramme est construit pour chaque région. Finalement, on concatène tous les histogrammes des régions afin de former un grand histogramme représentant l'image des caractéristiques faciales.

L'efficacité du code LBP comme indice facial s'explique par le fait que le LBP permet 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.

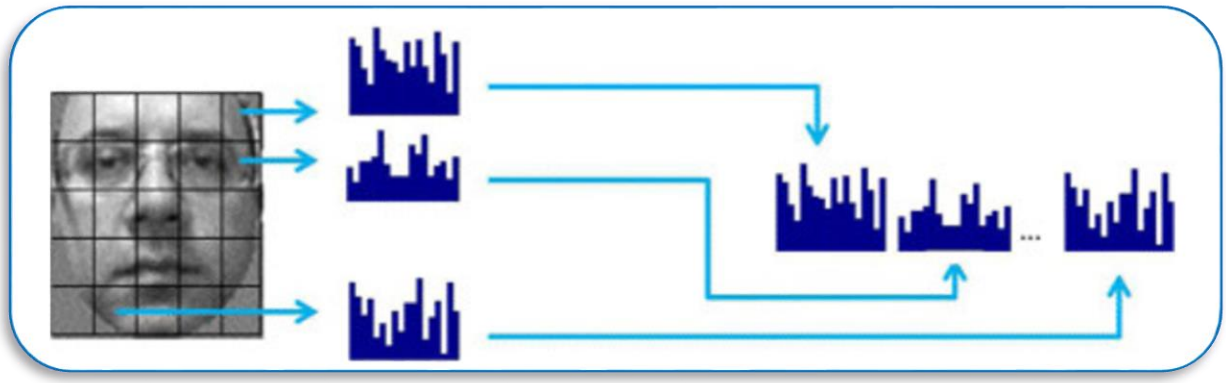

Figure III.7 : La représentation du visage par LBP

Etant donnés deux histogrammes de $LBP\ H1$, $H2$ de deux visages, l'étape suivante est d'utiliser une métrique pour calculer la similarité entre ces deux histogrammes. En testant les trois métriques $X2$, *Histogram intersection et Log-likelihood statistic,* Ahonen et al. **[18]** ont observé que la première métrique permet d'obtenir les meilleurs résultats :

$$\boldsymbol{X2}(\boldsymbol{H^1}, \boldsymbol{H^2}) = \sum_i \frac{(H_i^1 - H_i^2)}{H_i^1 + H_i^2}$$

III.8. Variantes de l'opérateur LBP :

Le calcul de l'opérateur LBP ne tient compte que du signe de la déférence entre les pixels, plusieurs variantes ont été proposé afin de complété l'information textural extraite par l'opérateur LBP.

III.8.1 complete local binary pattern (CLBP):

L'application de l'opérateur CLBP **[49]** sur une texture consiste à calculer pour chaque pixel de cette dernière deux différentes valeurs ($CLBP\_Signe$, $CLBP\_Magnitude$). Avec CLBP La région locale est représentée par un pixel centrale CLBP_C et une transformation de la différence locale Signe-magnitude, Tous les trois seuils CLBP_C, CLBP_S, CLBP_M ont un même format binaire, afin de les combinées à la fin pour former l'histogramme CLBP qui sera utilisé plus tard dans la classification.

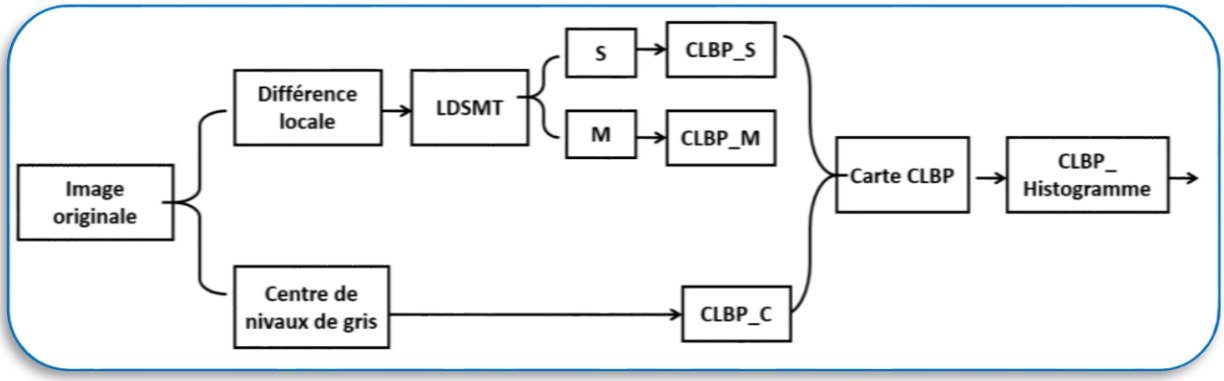

Figure III.8 : Méthodologie de CLBP **[49].**

Le schéma si dessous explique la méthodologie de CLBP :

Pour calculer les codes CLBP, il faut construire au premier lieu le vecteur de différences d'intensités entre le pixel central g_c. Et ses voisins g_p. Tel que $d_p = g_{p-} g_c$, ce vecteur local $[d0, d1..dp-1]$ caractérise la structure locale de l'image en pixel centrale g_c. Ensuite le vecteur d est décomposé en deux structures S, M :

$$d_p = s_p * m_p \; et \begin{cases} s_p = Sign(d_p) \\ m_p = |d_p| \end{cases}$$

Tel que :

- $s_p = \begin{cases} -1, & d_p < 0 \\ 1, & d_p \geq 0 \end{cases}$ est le signe de d_p et m_p c'est ça magnitude.

L'exemple ci-dessous illustre la décomposition de la matrice de différences locales de niveau de gris en deux matrices (magnitudes, signes).

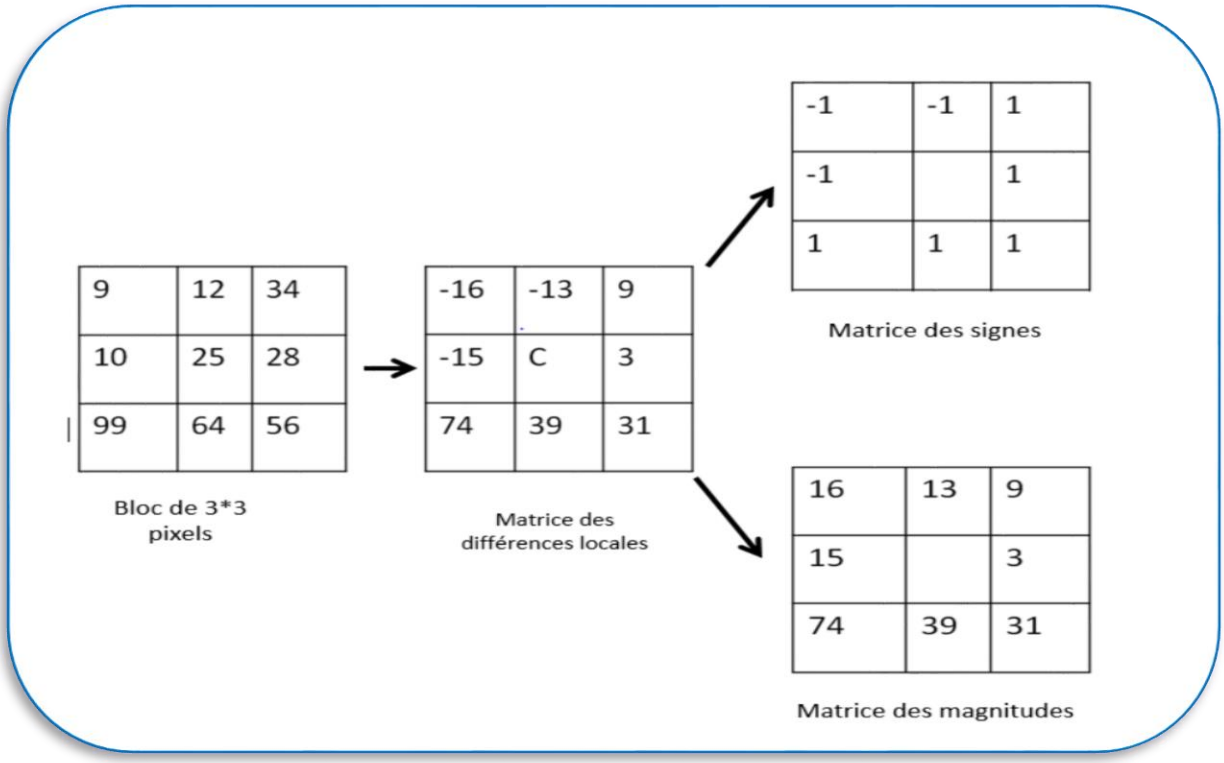

Figure III.9 : La séparation de matrice de signes et de magnitudes à partir de matrice de différence d'intensité locale **[49].**

Lorsque les vecteurs de signes et de magnitudes seront récupérés à partir des matrices (signes et magnitudes) comme il est expliqué dans la figure ci-dessus, on procède au calcul des codes LBP_S et LBP_M :

- L'opérateur LBP_S est typiquement le même que LBP, son équation est définie :

$$LBP_{S_{P,R}} = \sum_{K=1}^{P} s(g_K - g_c)2^{K-1}$$

- Le calcul de CLBP_M est basé sur l'équation suivante :

$$LBP_{M_{P,R}} = \sum_{K=0}^{P-1} t(M_K, c)2^K \ , t(x,c) = \begin{cases} 1, x \geq c \\ 0, x < c \end{cases}$$

Tel que :

- M_p : est la différence de niveaux de gris entre le pixel voisin k et le pixel central.

- c : est la moyenne des différences locales de niveaux M_p de toute l'image.

La figure ci-dessous illustre les résultats d'application des deux opérateurs CLBP_S et CLBP_M :

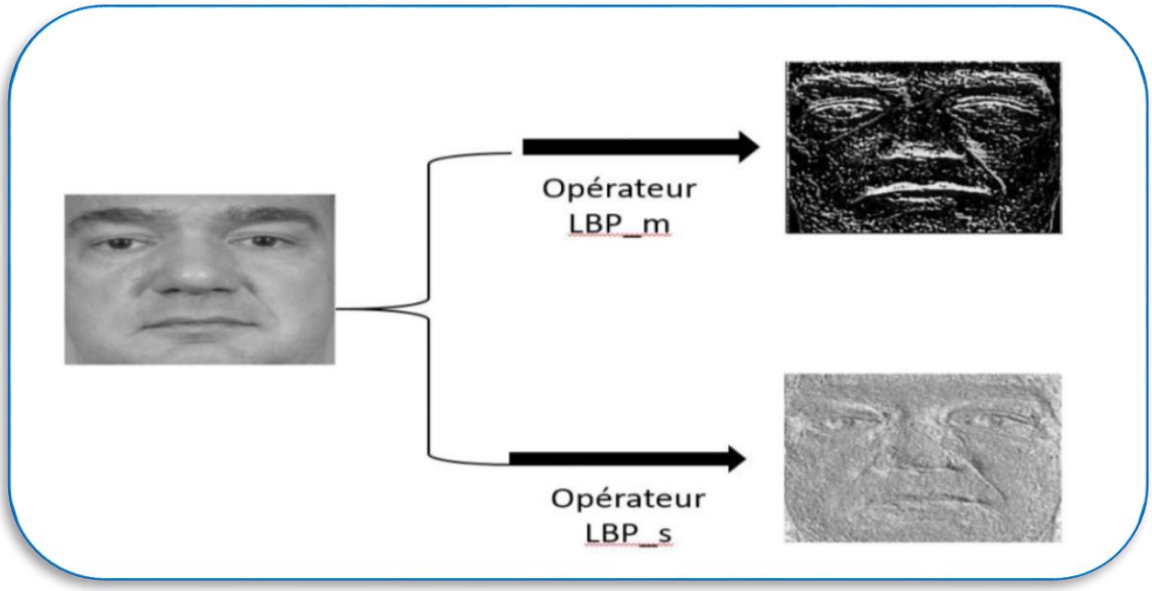

Figure III.10 : Résultats d'application de LBP_M et CLBP_C sur une image **[49].**

III.8.1.1 Extraction des caractéristiques avec la CLPB :

Une fois les codes CLBP_S et CLBP_M calculés pour tous les pixels de l'image, on possède au calcul l'histogramme pour former le vecteur caractéristique représentant l'image faciale CLBP. 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 **[49]**.

Nous présentons dans la figure ci-dessous les étapes de construction d'un histogramme CLBP :

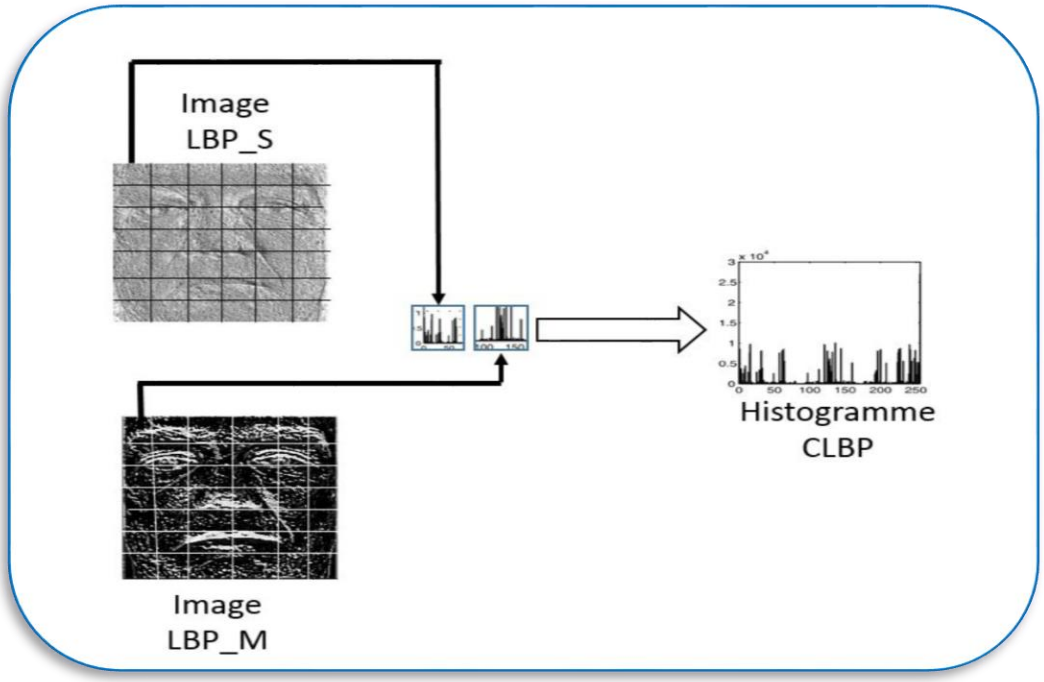

Figure III.11: La construction de l'histogramme CLBP **[49].**

III.8.1.2 Rapport entre CLBP et LBP

Plusieurs observations peuvent être faites pour la CLBP **[49]**

- LBP est un cas particulier de CLBP en utilisant seulement CLBP_S
- La classification de texture peut donner de meilleurs résultats avec CLBP grâce à la fusion d'histogrammes CLBP_S, CLBP_M
- CLBP_S conserve plus d'informations sur la structure locale de la texture que CLBP_M, ce qui explique pourquoi l'opérateur LBP simple peut extraire la textures d'une manière relativement bien.

III.8.2 Adaptation MAP :

- Après avoir appliqué avec succès l'opérateur LBP dans la reconnaissance faciale **[48],** beaucoup de chercheurs ont adopté ce descripteur avec d'autres fonctions de classification. Rodriguez et al ont proposé un modèle génératif pour l'authentification des visages basé sur LBP.
- Comme il est expliqué précédemment pour calculer le vecteur caractéristique, les images visages sont divisées en R blocs de même taille K, où l'histogramme LBP calculé pour chaque bloc. Au lieu de travailler avec ces histogrammes directement, Rodriguez et al les normalisent pour les employer en tant que distribution de probabilités.

$$\sum H_r\,(i) = 1 \quad r = \{1,2,\dots,R\}$$

Tel que :

$\boldsymbol{H}$ **:** L'histogramme normalisé de l'image.

$\boldsymbol{r}$ **:** Le numéro du Bloc.

I : Classe de l'histogramme

Pour déduire le modèle adapté d'un client, un modèle générique UBM est calculé à partir de la concaténation de tous les histogrammes apprentissage normalisés tel qu'il est illustré dans la figure ci-dessous :

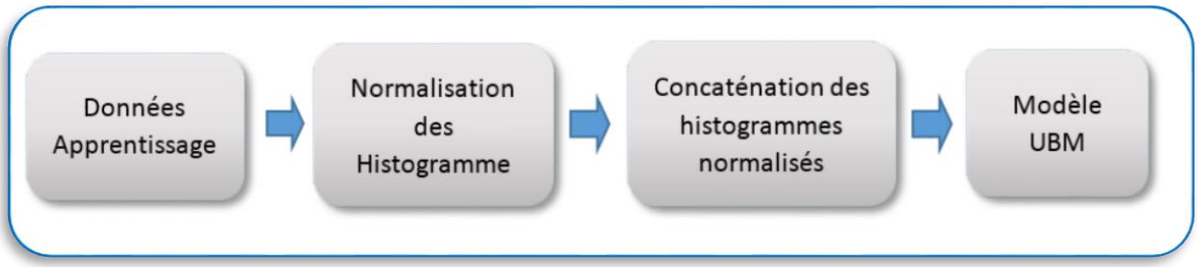

Figure III-12 : Le calcul du modèle UBM **[48]**

Dans l'étape de vérification, la proclamation X pour un Client est considérée comme un nombre fixe de R blocs de même taille et le score de vérification est obtenu comme suit :

$$\Lambda(X) = \log P(X|\,\theta_c) - \log P(X|\,\theta_w)$$

θc : Ensemble de paramètres du modèle Client C.

θw : Ensemble de paramètres de l'ensemble du monde UBM

$P\,(X\,|\theta c)$: La probabilité que la demande en provenance d'un véritable Client.

$(X\,|\theta w)$: La probabilité que la demande provient d'un imposteur.

III.8.2.1 Adaptation des histogrammes LBP :

Le principe de l'adaptation **[48]** a été appliqué avec succès sur la reconnaissance vocale, puis sur La reconnaissance faciale. L'adaptation MAP consiste à créer le modèle générique UBM (Universal Backgroud Model, modèle du monde) qui utilise tous les modèles d'apprentissage. Le modèle UBM contient les caractéristiques de tous les utilisateurs de l'ensemble d'apprentissage, il permet de déduire le modèle spécifique du client. à partir de ce dernier et une approche bayésienne appelée Maximum A Posteriori. Dans le contexte l'adaptation MAP,

le modèle client adapté est une somme pondérée du modèle client et du modèle du monde, il est défini par l'équation suivante :

$$\widehat{H}_c^r(L_k) = \alpha\, H_w^r(l_k) + (1-\alpha) H_c^r(L_k)$$

$H_w^r(l_k)$: L'histogramme normalisé pour le block R pour UBM.

$H_c^r(L_k)$: L'histogramme normalisé pour le block R pour le modèle client.

α : Le poids.

l_k : La k ème classe de l'histogramme.

La figure suivante illustre les étapes de génération du modèle client adapté.

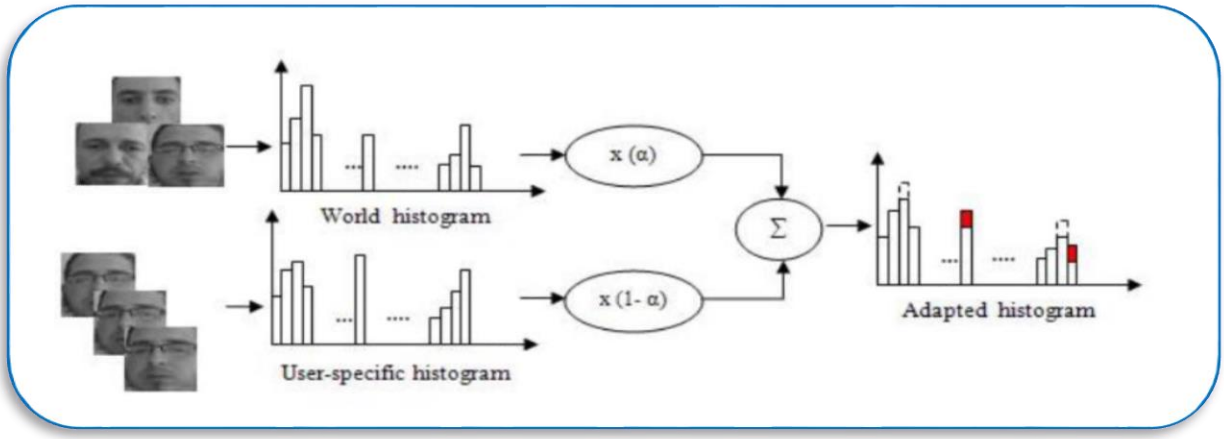

Figure III-13 : Adaptation du modèle Client **[48]**

III.9. Applications de LBP et de ces variantes :

Au cours de ces dernières années, la popularité de l'approche LBP ne fait qu'augmenter grâce à son application dans les divers problèmes de vision par ordinateur.

III.9.1. La détection et le suivi d'objets

Grace à sa simplicité de calcul et sa puissance discriminatoire, LBP est devenue très populaire dans les taches de détection et de suivi. Avec l'utilisation des histogrammes spatiaux, *Zhang et al*. **[58]** ont développés une méthode basée sur le choix automatique des motifs d'histogrammes spatiaux. Un classificateur hiérarchique est appris en combinant des d'histogramme en cascade avec une machine de support vectorielle afin de détecter des objets.

Les histogrammes spatiaux sont obtenus par le traitement des images avec un opérateur LBP 3×3, puis des modèles spatiaux sont employés pour coder les motifs d'histogrammes spatiaux sur l'échelle de l'espace.

III.9.2. La biométrie

En plus de la reconnaissance des expressions faciale, LBP a également été employée avec succès dans beaucoup d'autres applications de la biométrie, y compris, la reconnaissance de l'iris, la reconnaissance d'empreintes digitales **[59]** et palmaires ainsi que celles des de veine de doigt.

III.10. Classification :

Après l'extraction du vecteur caractéristique, arrive 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 tel que, réseau de neurones, SVM (Support Vector Machine), et dans notre cas on a utilisé le classificateur du plus proche voisin.

III-10.1 La méthode du plus proche voisin

C'est une méthode de classification simple, elle diffère des autres méthodes de classification supervisées par le fait qu'aucun modèle n'est déduit à partir d'exemples d'apprentissages ; ces derniers sont seulement enregistrés pour faire la comparaison avec le modèle en utilisant des mesures de distances, pour choisir à la fin le modèle le plus proche, formellement il retourne **[50]**

La complexité de la méthode du plus proche voisin en termes de temps de calcul est de l'ordre O (Nd) où N désigne le nombre de personnes présentes dans la base et d la dimensionnalité du modèles (taille histogramme), ceci doit être pris en compte lors du choix de la méthode d'extraction, surtout si le système doit opérer en temps réel et que le nombre de personne dans la base est grand.

III-10.2 Les distances

Afin de classer correctement l'image test, il est nécessaire de comparer son modèle avec différents modèles existants dans la base de données. Il existe plusieurs métriques de comparaison :

- **Euclidienne :**

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

- **Distance de Manhatan :**

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

- **Mesure Chi carré $\chi 2$:**

La mesure de dissimilarité du Chi carré est utilisée pour le calcul des intersections entre les histogrammes, car il a été prouvé qu'elle est plus fiable **[45]** que la distance euclidienne.

$$\chi 2\ (x,y) = \sum_{i} \frac{(x_i - y_i)^2}{(x_i + y_i)}$$

- **Statistique de log- vraisemblance :**

La distance du modèle de l'image test et le modèle le plus proche constitue son score de dissimilarité.

Conclusion :

Dans ce chapitre, nous avons présenté l'approche de modélisation *LBP*, ses principales variantes, ainsi qu'on a défini la phase de classification.

Ceci clôture l'étude des phases du processus de reconnaissance faciale, La chapitre suivant traitera la conception de notre système.

CHAPITRE IV

Conception et Réalisation

Introduction :

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

IV.1. Conception :

Dans la phase de conception, 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, ainsi que leurs implémentations en expliquant les interactions entre elles à travers plusieurs diagrammes.

IV.1.1. Les acteurs du système :

Chaque acteur du système, est amené à effectuer un certain nombre de tâches résumées dans ci-dessous :

1. L'Administrateur :

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

Effectuant plusieurs tâches :

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

2. L'individu Test :

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

IV.1.2. Diagramme du 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 :

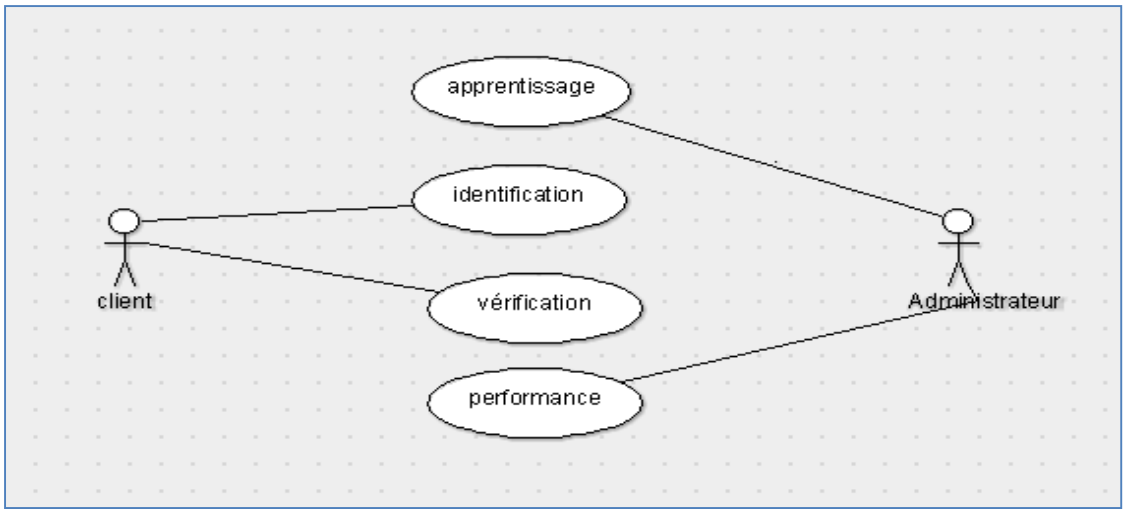

Figure IV .1. Diagramme de cas d'utilisation global

IV.1.3. Description textuelle des cas d'utilisation :

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. 4. Le résultat (Matrice LBP). 5. Enregistrement des modèles d'apprentissage (Matrice LBP) dans la base de données. 6. Affichage des résultats (message de réussite).

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 définie 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.
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 (utilisation des distances).
5. Trier les scores résultants de l'étape précédente pour indiquer la personne la plus proche de l'individu test.
6. Affichage des résultats.

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.
5. Calculer le degré de vraisemblance entre le modèle de l'individu test et son modèle enrôlée 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.
7. Affichage des résultats.

Cas d'utilisation : Performance
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 d'identification « TID », le Taux de faux rejets « FRR » et le Taux de fausse acceptations « FAR »). **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. 4. La mesure des performances du système : le calcul du TID, FAR, FRR. 5. Affichage des résultats : TID, FAR, FRR.

IV.1.4. Diagrammes de séquence (cas d'utilisation détaillés) :

On utilise les diagrammes de séquences pour décrire comment les éléments du système interagissent entre eux et avec les acteurs.

IV.1.4.1 Diagramme de séquence cas d'utilisation « Apprentissage »

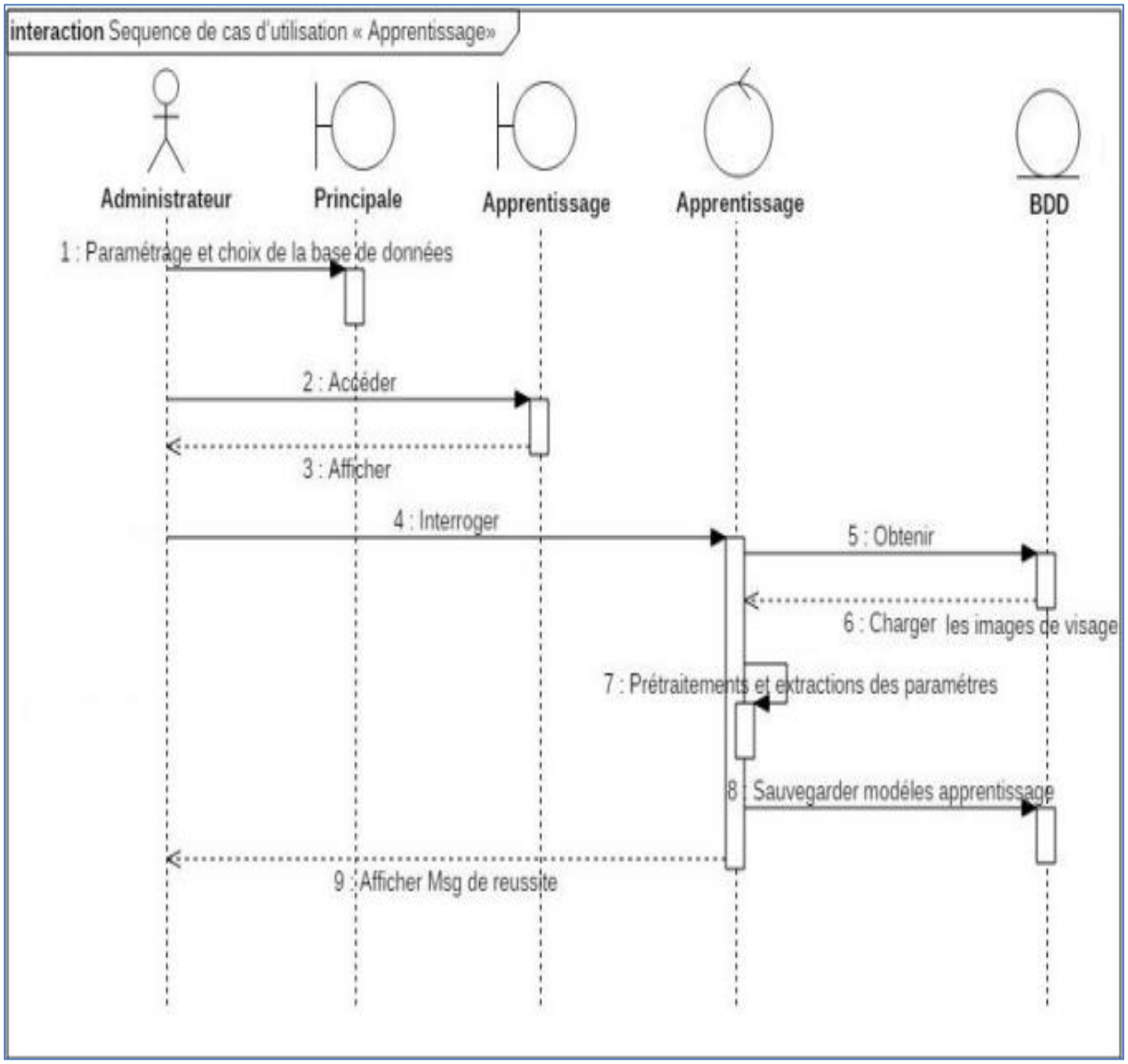

Figure IV.2. Diagramme de séquence cas d'utilisation « Apprentissage ».

Description du scénario d'apprentissage :

- L'administrateur choisit la configuration et la sélection de la base de données pour faire l'apprentissage.
- L'extraction des paramètres de l'ensemble des images d'apprentissage en utilisant l'approche LBP.
- Le résultat.
- Enregistrement des modèles d'apprentissage dans la base de données.
- Affichage des résultats (message de réussite).

IV.1.4.2 Diagramme de séquence cas d'utilisation « Identification »

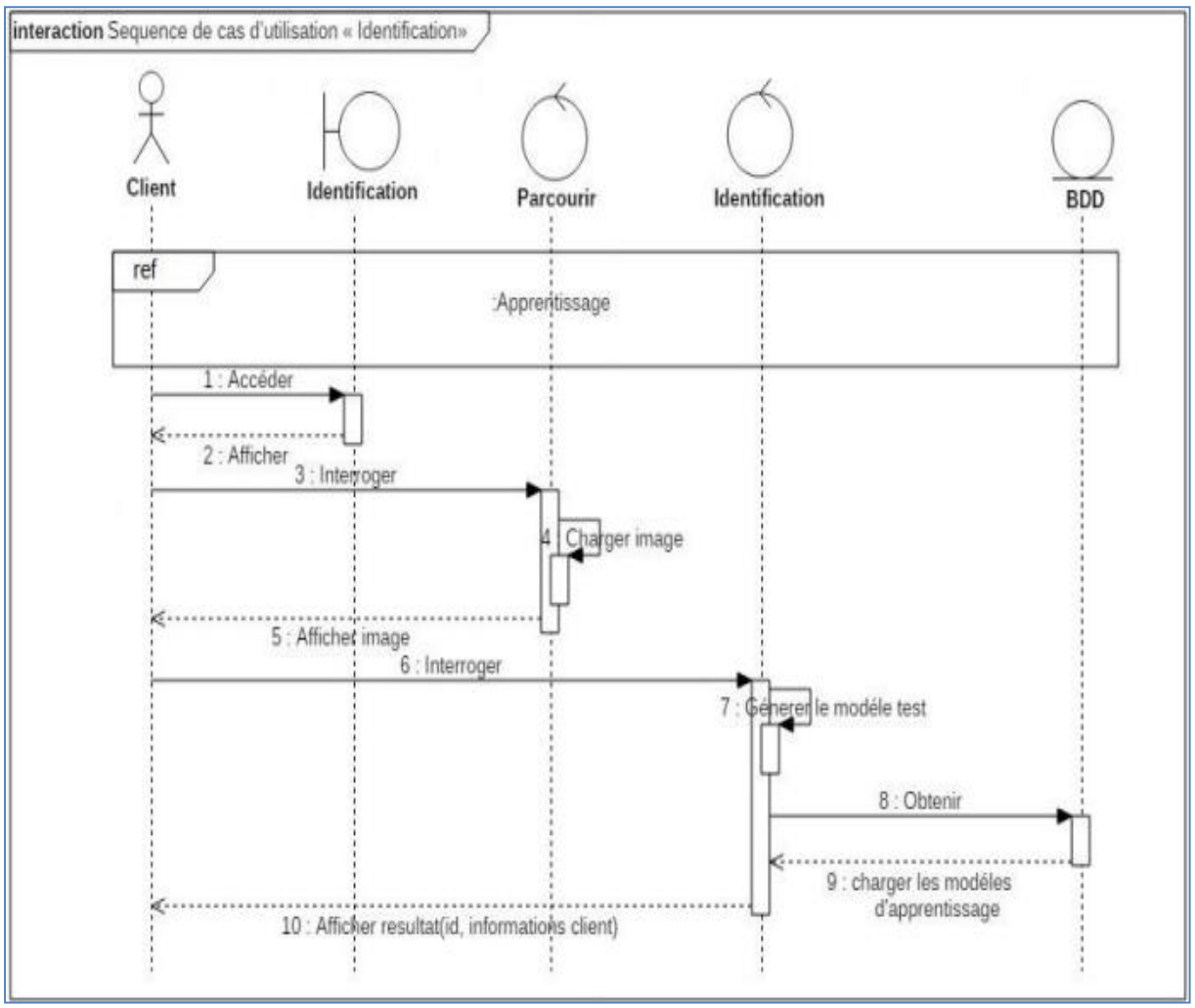

Figure IV.3. Diagramme de séquence cas d'utilisation « Identification »

Description du scénario d'identification :

- On prend une image de la base de données de l'individu test.
- Application des prétraitements nécessaires sur l'image pour éliminer le bruit.
- Extraction des paramètres pertinents de l'image test à l'aide de LBP.
- Calculer le degré de vraisemblance entre les paramètres de l'image test et tous les modèles clients enrôlées et stockés dans la base de données en utilisant les distances, à la fin de cette phase on aura des scores résultants.
- Trier les scores résultants de l'étape précédente pour indiquer la personne la plus proche de l'individu test.
- Affichage des résultat (identité de la personne).

IV.1.4.3 Diagramme de séquence cas d'utilisation « Vérification »

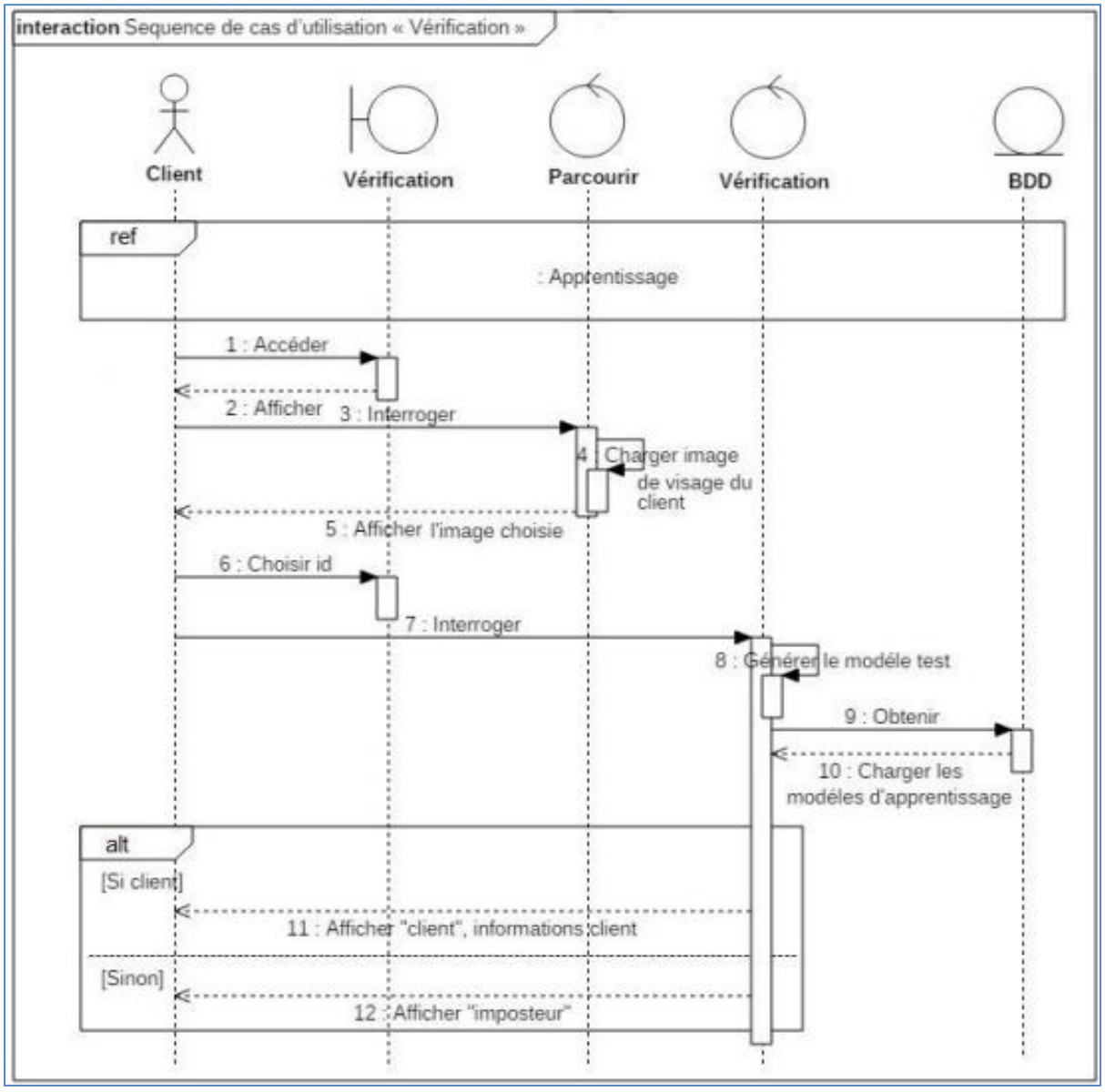

Figure IV.4. Diagramme de séquence cas d'utilisation « Vérification »

Description du scénario de vérification :

- On prend une image de la base de données de l'individu test.
- Le client introduit son identifiant.
- Application des prétraitements nécessaires sur l'image pour éliminer le bruit.
- Extraction des paramètres pertinents de l'image test à l'aide de LBP.
- Calculer le degré de vraisemblance entre le modèle de l'individu test et son modèle enrôlée dans la base de données.
- Comparer le score résultant avec le seuil optimal du système.
- Affichage des résultats.

IV.1.4.4. Diagramme de séquence cas d'utilisation « Performance »

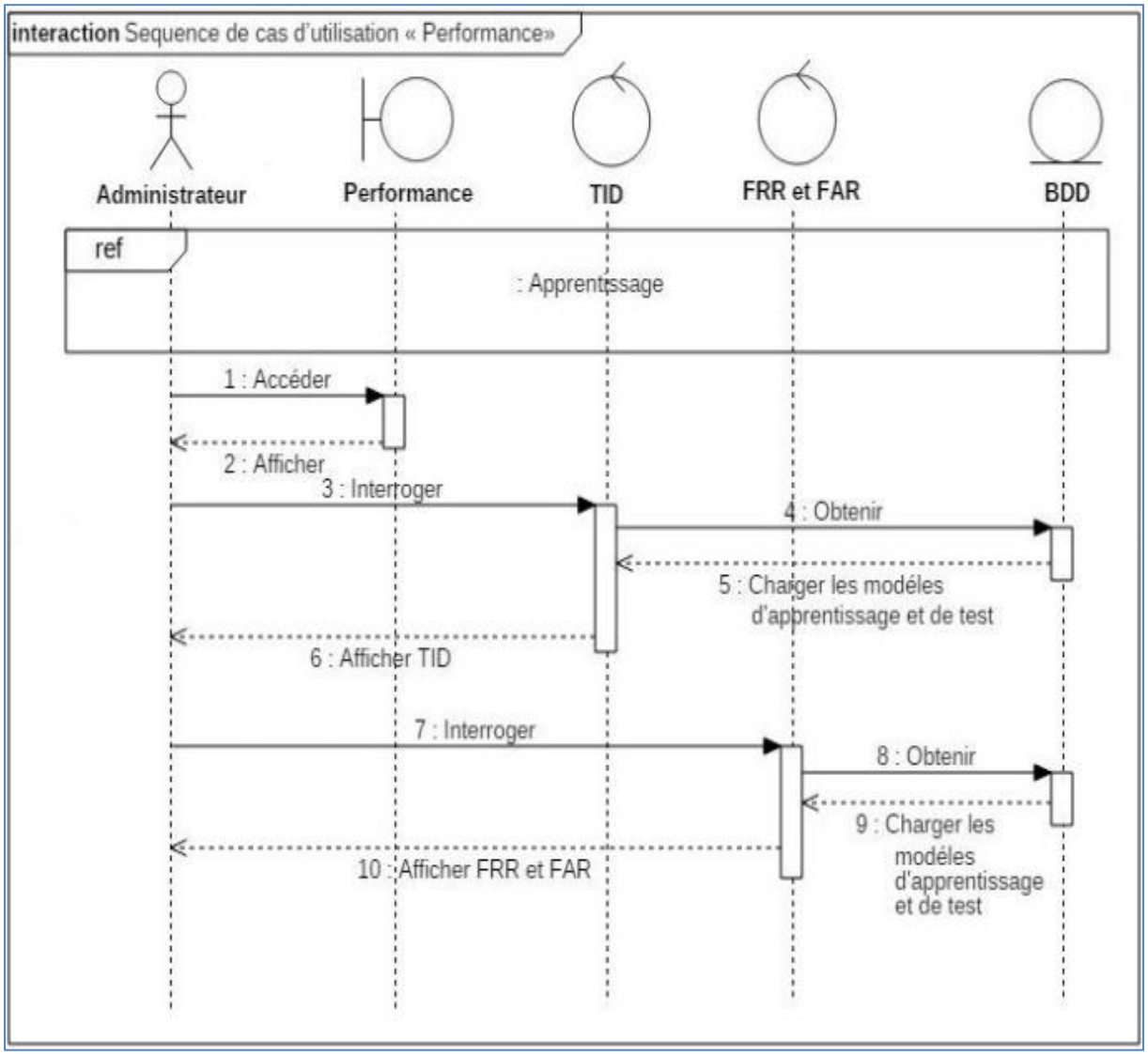

Figure IV.5. Diagramme de séquence cas d'utilisation « Performance »

Description du scénario de performance :

- L'administrateur choisit la configuration.
- La sélection de la base de données pour faire les tests.
- Chargement des modèles d'apprentissage et de teste déjà enregistrés.
- La mesure des performances du système : le calcul du TID, FAR, FRR pour la configuration choisie.
- Affichage des résultats : TID, FAR, FRR.

V.1.5 Architecture et fonctionnement du système

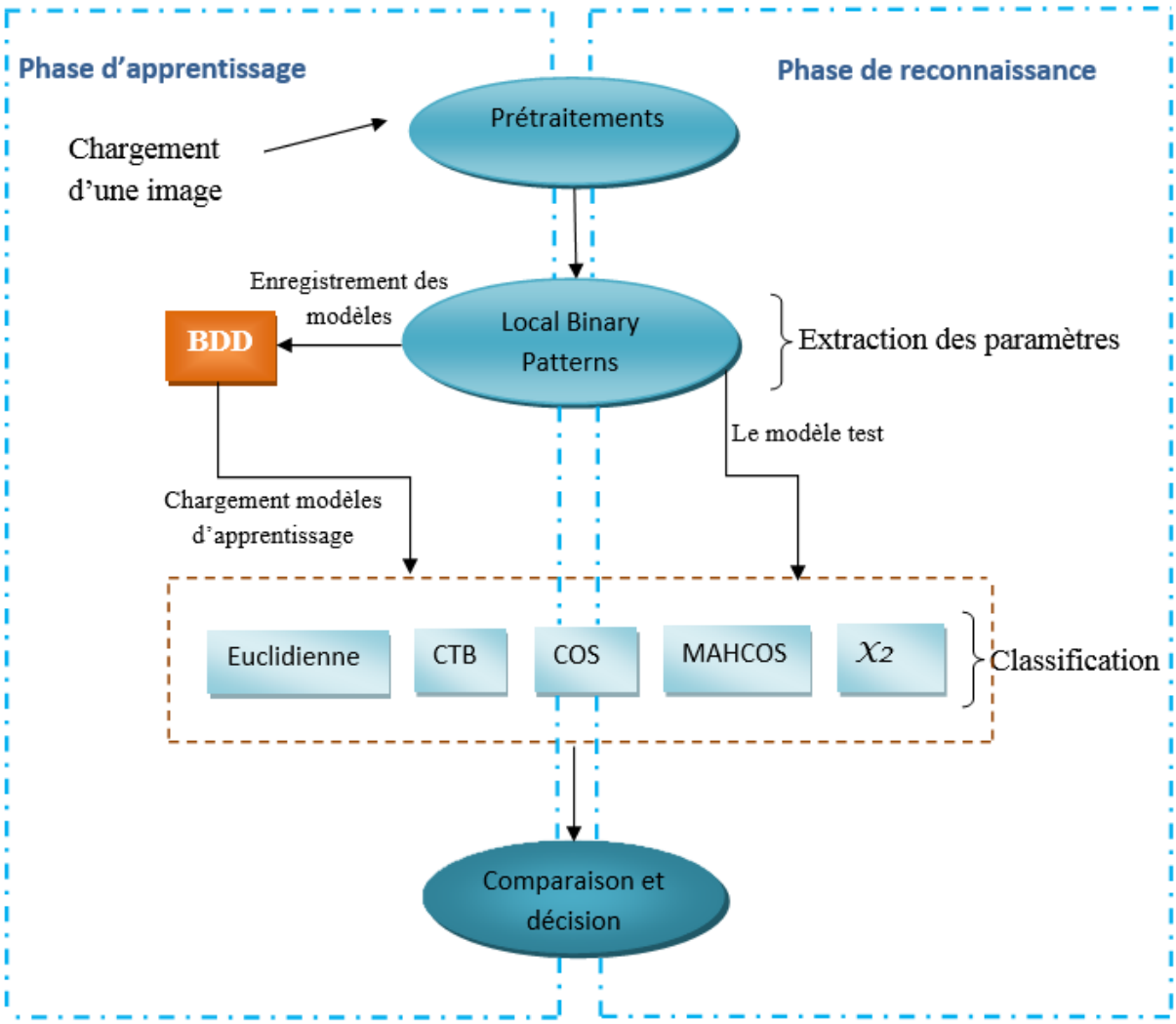

Figure IV.6. Diagramme de fonctionnement du système

V.1.5.1 L'Apprentissage

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

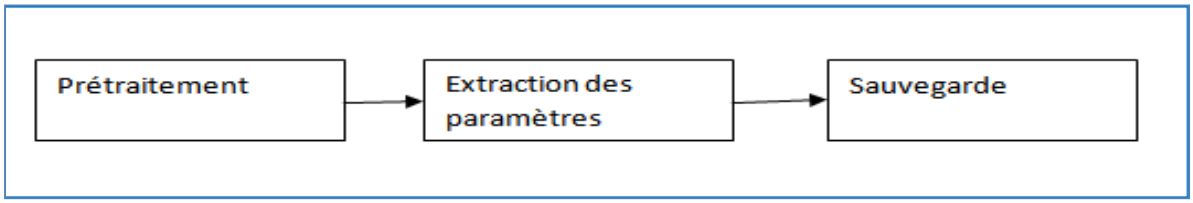

Figure IV.8. Représentation modulaire de la phase apprentissage

- **Module prétraitement :**

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

- **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 un visage et différentes d'une personne à une autre. L'extraction des caractéristiques est appliquée par l'approche LBP.

- **Module de sauvegarde :**

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

IV.1.5.2 Phase de reconnaissance et la prise de décision

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

1. 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 sauvegardées 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.

2. 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.

IV.1.5.3. Calcul des performances du système

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

1. Mode Identification

Dans le mode d'identification on s'intéresse au 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.

$$TID = \frac{nombre\ de\ clients\ correctement\ identifiés}{nombre\ total\ des\ clients}\ X\ 100$$

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 mesure r les performances en mode vérification.

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_extra
Si (dist_min_intra(i)<=Seuil)
Faux_rejet← Faux_rejet+1
Fin Si
Fin pour
FRR←(Faux_rejet/nbr_Test_intra) *100
```

Figure IV.9. 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
Fin pour
FAR←(Fausse_acceptation/nbr_Test_extra) *100
```

Figure IV.10. Calcul du FAR.

Remarque : Dans un système idéal TRF+TFA=0, mais ce n'est pas le cas dans la pratique ; quand TFR augmente TFA diminue et vice versa. Par conséquent il faut trouver un compromis entre les deux taux.

IV.2. 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.

IV.2.1 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.

IV.2.1.1 MATLAB

MATLAB est une abréviation de Matrix LABoratory. Écrit à l'origine, en Fortran, par Cleve Moler a la fin des années 1970, optimisé pour le traitement des matrices, d'où son nom. MATLAB est un environnement puissant, complet en plus de sa disponibilité est assurée sur plusieurs plateformes. C'est un environnement performant, ouvert et programmable qui permet de remarquables gains de productivité et de créativité. 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 2016 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 prenne nt en charge tous les outils mathématiques utiles au traitement et à l'analyse des images

IV.2.2 L'implémentation de notre système :

V.2.2.1 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 :

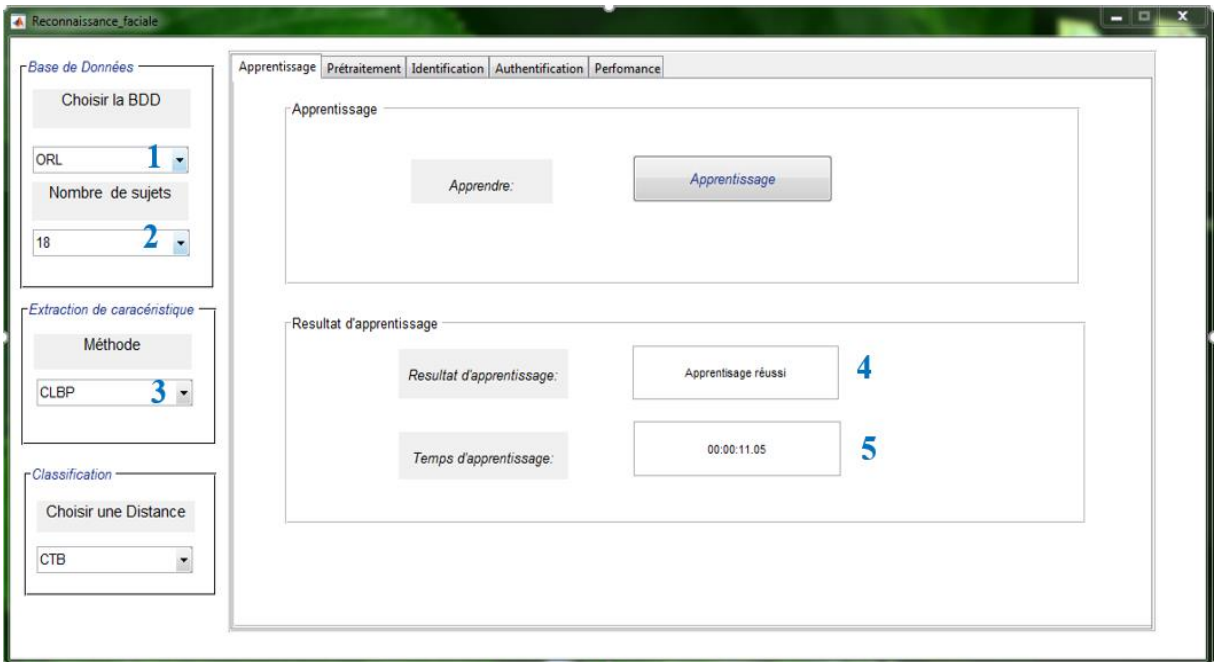

Figure IV.11. Interface apprentissage

1. Choix de la base de données.
2. Choix nombre du sujet dans la base de données (1 à 40).
4. Choix de méthode d'extraction (LBP, CLBP).

5. Résultat d'apprentissage.

6. Temps d'exécution de la phase apprentissage

Tests de performance :

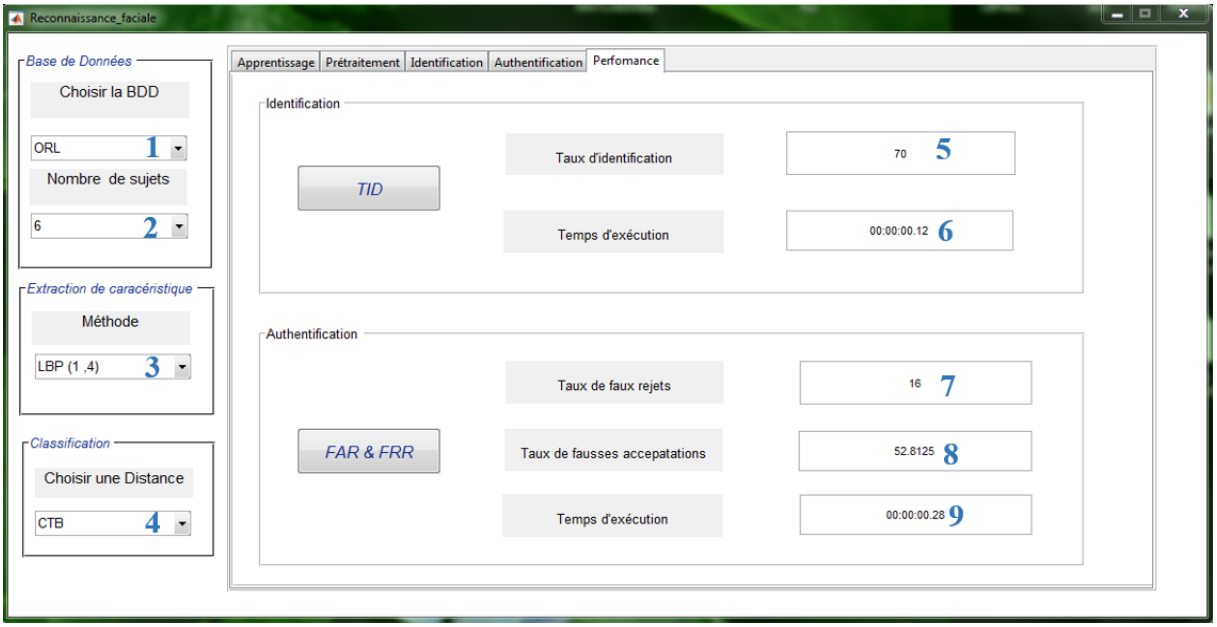

Figure IV.12. Interface performance

1. Choix de la base de données.
2. Choix nombre du sujet dans la base de données (1 à 40).
3. Choix de méthode d'extraction (LBP, CLBP).
4. Choix de la distance (euclidienne, norme CTB, cosine, mahcos, sqr).
5. Taux d'identification (TID)
6. Temps d'exécution de taux d'identification
7. Taux de faux rejets (FRR)
8. Taux de fausse acceptation (FAR)
9. Temps d'exécution de FAR et FRR

Interface identification :

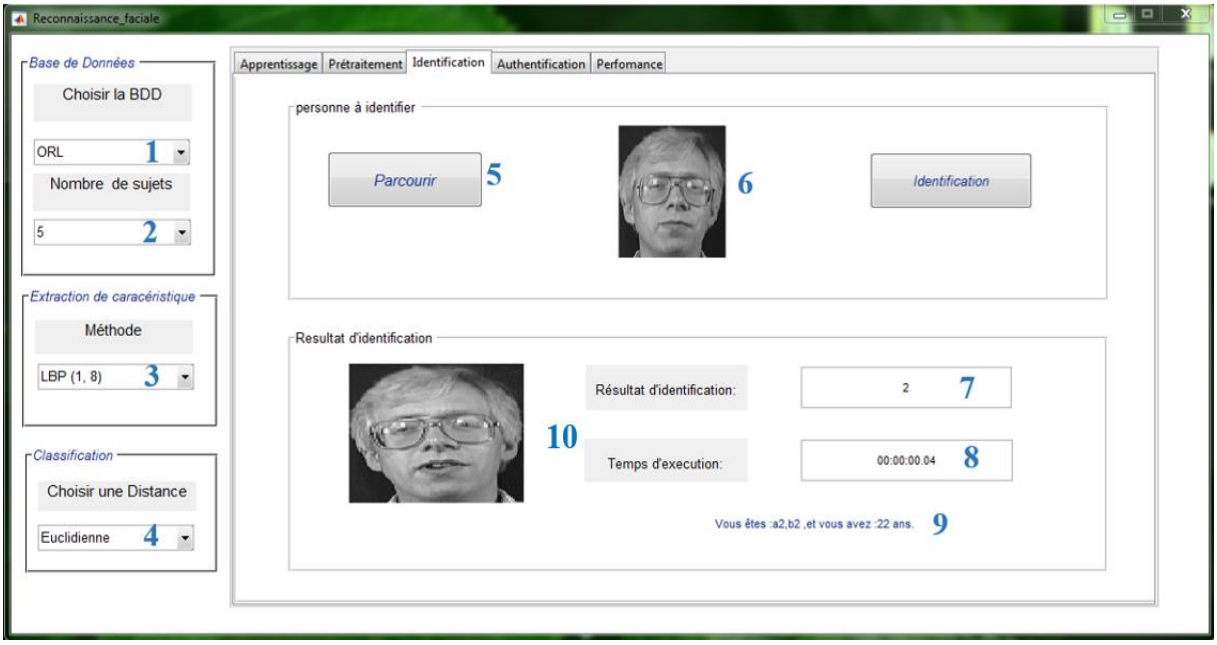

Figure IV.13. Interface identification.

1. Choix de la base de données.
2. Choix nombre du sujet dans la base de données (1 à 40).
3. Choix de méthode d'extraction (LBP, CLBP).
4. Choix de la distance (euclidienne, norme CTB, cosine, mahcos, sqr).
5. Chargement de l'image de l'individu test
6. Image de la personne à identifier
7. Résultat d'identification (identifiant client).
8. Temps d'exécution de la phase identification.
9. Les informations personnelles de la personne identifier.
10. L'image de la personne identifiée

Interface Authentification :

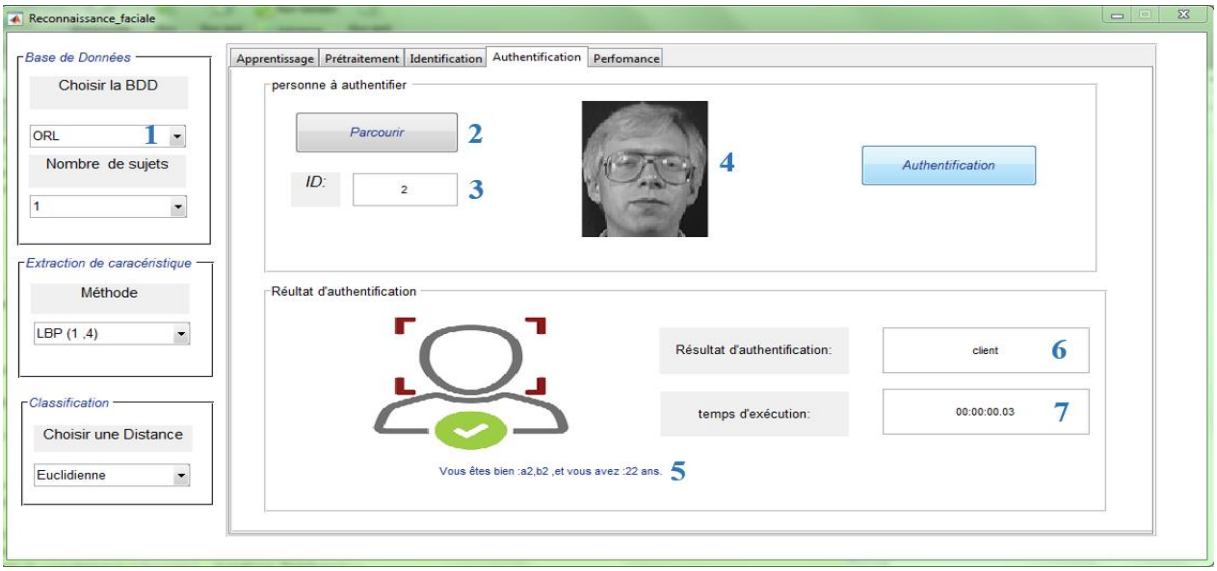

Figure IV.14. Interface authentification.

1. Choix de la base de données.
2. Chargement de l'image de l'individu à authentifier
3. Choix de l'identifiant (ID).
4. Choix de la distance (euclidienne, norme CTB, cosine, mahcos, sqr).
5. Résultat d'authentification (client, imposteur).
6. Temps d'exécution de la phase authentification.
7. Les informations personnelles de la personne identifier.

Interface prétraitement :

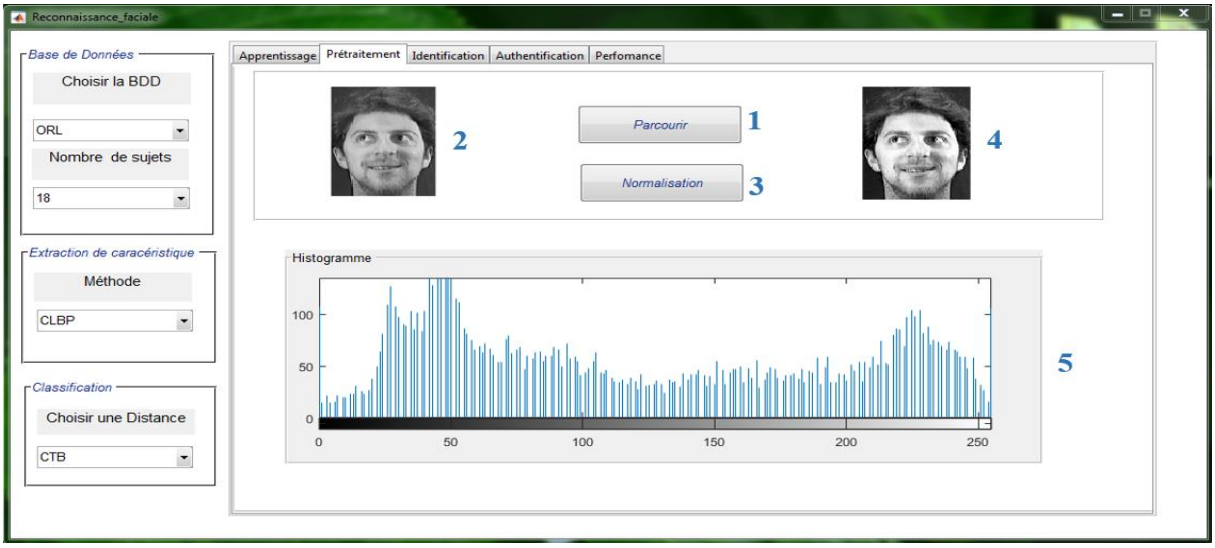

Figure IV.15. Interface prétraitement

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).

Conclusion :

Dans ce chapitre, nous avons montré le schéma général de notre système de reconnaissance de visages et les détails des modules qui le composent, ainsi que les différents outils de développement utilisés pour assurer son bon fonctionnement. dans le chapitre suivant nous allons voir les tests et les résultats obtenus par ce système.

CHAPITRE V

Tests et Evaluation des Resultats

Introduction :

Ce dernier chapitre présente les résultats d'évaluation du système de reconnaissance de visage que nous avons développé. Ceci à travers un ensemble de tests effectués pour les deux modes de reconnaissance : identification et vérification. Les différents résultats des tests obtenus sont par la suite analysés. Le but étant de simuler les conditions réelles dans lesquelles le système sera déployé et d'arriver à choisir les paramètres adéquats de la configuration afin d'optimiser les performances du système.

V.1. La Base de données ORL :

Conçu par AT&T laboratoires de l'université de Cambridge en Angleterre, la base de donnée ORL (Olivetti Research Laboratory) est une base de donnée de référence pour les systèmes de reconnaissances automatique des visages. En effet, tous les systèmes de reconnaissances de visages trouvés dans la littérature ont été testés en utilisant la base ORL, cette popularité est dû aux nombre de contraintes existantes dans cette base car là plus part des changements possibles et prévisibles du visage ont été pris en compte, comme par exemple : le changement de coiffure, la barbe, les lunettes, les changements dans les expressions faciales, etc. Ainsi que les conditions d'acquisition telles que : le changement d'échelle dû à la distance entre le dispositif d'acquisition et l'individu.

La base de données ORL est constituée de 400 images de l'ensemble de 40 individus, tel que chacun possède 10 poses 5 pour l'apprentissage et 5 pour le test

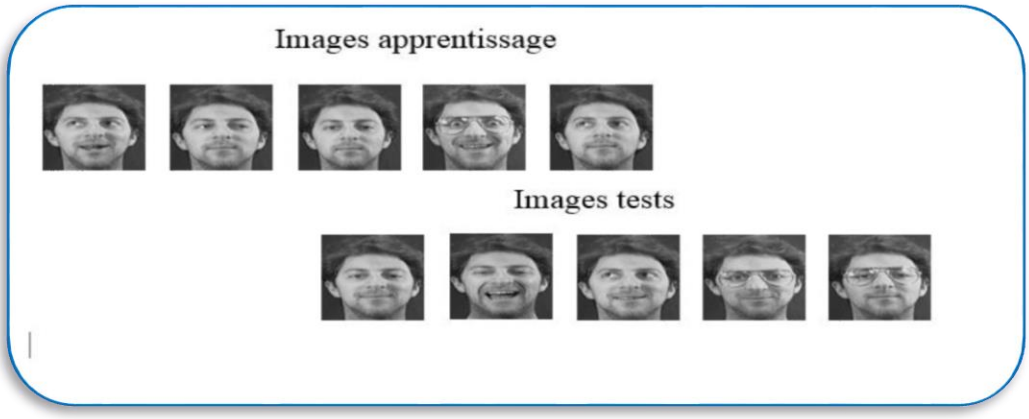

Figure V.1. Images tests et apprentissages d'un Client dans la base ORL.

Les poses ont été prises sur des intervalles de temps différents pouvant aller jusqu'à trois mois. L'extraction des visages à partir des images a été faite manuellement. Nous présenterons dans ce qui suit les figures montrant les spécificités de la base de données de référence ORL.

Figure V.2. Base de données ORL

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

Figure V.3. Exemple de changements d'orientations du visage

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

Figure V.4. 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 V.5. 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. Comme l'illustre cet exemple :

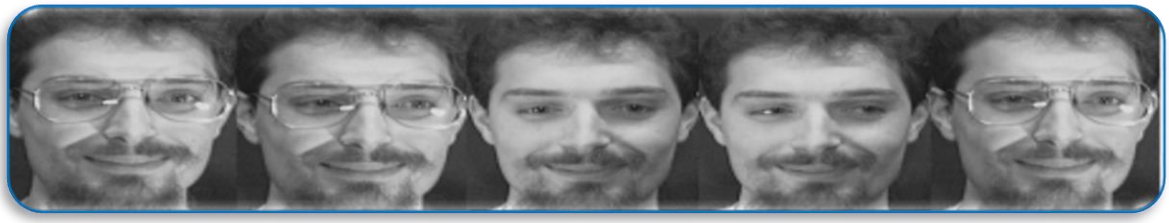

Figure V.6. Exemple de port de lunettes

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

Figure V.7. Exemple de changements de coiffure et de port de barbe

V.2.Evaluation du système :

Dans cette section on présentera l'influence des différents paramètres d'extraction et de méthode de classification 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 configuration 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 ctb) dans le but de faire une étude comparative des différentes configurations.

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 TFR (ou FRR) :** le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.
- **Taux Faux accepter TFA (ou FAR) :** le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

V.2.1. Configuration des paramètres du système :

Paramètres fixes du système	Paramètres variables du système
-le nombre d'image pour l'apprentissage :5 images. - le nombre d'image test :5 images. -Taille de l'image.	-Méthodes LBP et CLBP. -Le rayon R. -Le nombre du point du voisinage P. -les distances.

V.2.2. Résultats des Tests :

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

Dans les deux modes identification et authentification (vérification).

V.2.2.1. Mode identification :

- **Effet d'application de la méthode d'extraction LBP en variant le rayon et le voisinage et du choix de la méthode de classification sur le TID :**

			Euclidienne	Ctb	cosine	mahcos	X2
LBP	Rayon 1	Voisinage 4	69	68	68.5	68.5	68
		Voisinage 8	72	78	74.5	74.5	72.5
		Voisinage 16	68	82	75.5	75.5	69.5
	Rayon 2	Voisinage 4	77	78	77.5	77.5	77
		Voisinage 8	78.5	82.5	81.5	81.5	79
		Voisinage 16	67	84.5	81.5	81.5	66.5

Tableau V.1. Variation du taux d'identification TID (%) en fonction des variantes LBP et les distances.

En sachant que dans un système biométrique de reconnaissance, plus le taux de TID est plus proche de Cent (100) plus les performances sont bonnes et vice versa, d'où on constate que le meilleur résultat est 84.5%. Il est atteint en appliquant la méthode LBP (2,16) et la méthode de classification avec la distance de la norme « ctb »

En fixant la distance à Ctb, on varie le TID en fonction du rayon R et le voisinage P comme l'illustre le graphe suivant :

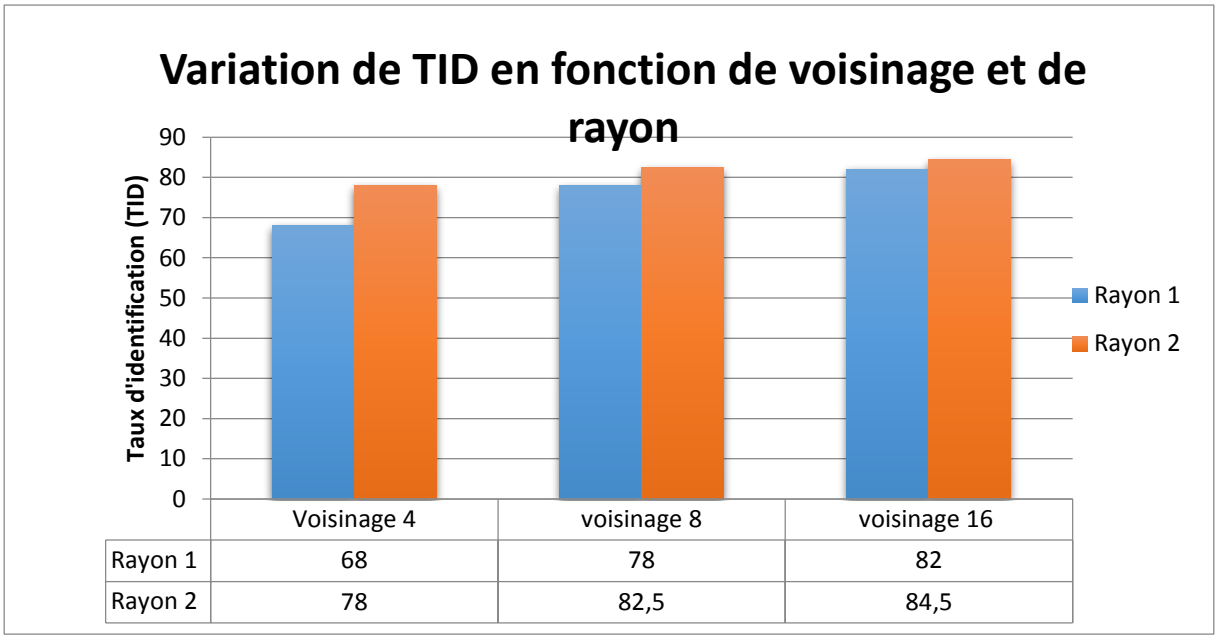

Figure V.8. Variation du taux d'identification TID (%) en fonction du rayon et voisinage.

On constate une amélioration du TID lorsque le nombre de points P de voisinage augmente de 4 à 8 points et de 8 à 16 points, on explique ce résultat par la meilleure représentation de la texture à mesure que P augmente.

Dans ce qui suit, on varie le taux d'identification en fonction des distances.

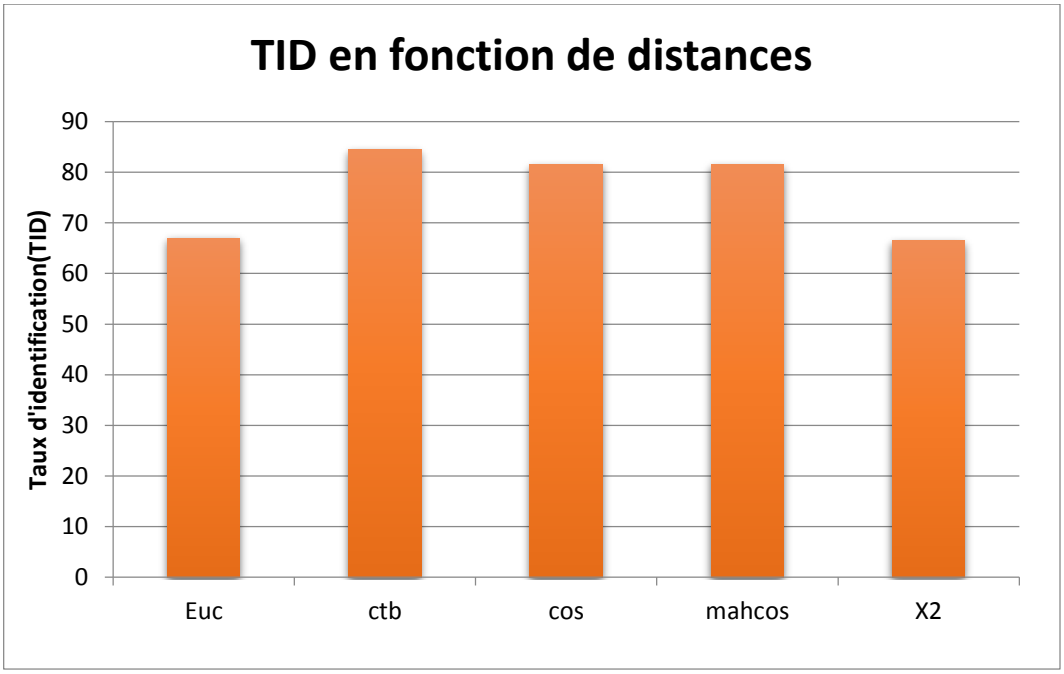

Figure V.9. Variation du taux d'identification TID (%) en fonction des distances.

V.2.2.2. Mode authentification (vérification) :

- **Effet de l'application du LBP et ses variantes et la méthode de classification sur le FAR :**

			Euclidienne	Ctb	cosine	mahcos	sqr
LBP	Rayon 1	Voisinage 4	30.70	39.49	51.99	51.99	43.82
		Voisinage 8	22.57	33.39	49.45	49.45	39.39
		Voisinage 16	37.57	37.65	53.9	53.9	42.07
	Rayon 2	Voisinage 4	46.46	47.92	58.51	58.51	53.55
		Voisinage 8	28.47	39.17	53.32	53.32	40.27
		Voisinage 16	35.93	36.13	52.69	52.69	36.67

Tableau V.2. Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage.

A travers les résultats générés, on perçoit que la distance de classification « Euclidienne » a donné la meilleure conséquence car son pourcentage est le plus bas (22 ,57%) mais reste toujours une valeur qui n'est pas performante, sachant que dans un système biométrique plus le FAR est proche de zéro plus les performances sont élevées et vice versa.

Dans ce qui suit, on varie le taux de fausses acceptations FAR en fonction du rayon et voisinage.

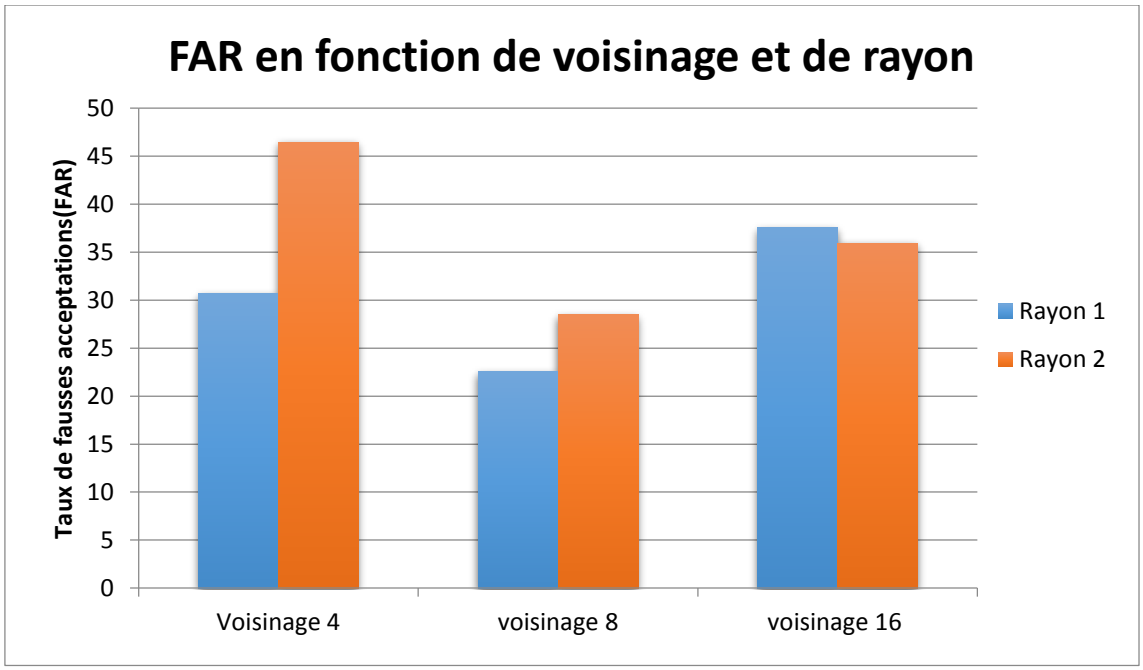

Figure V.10. Variation du taux de fausses acceptations FAR (%) en fonction du rayon et voisinage.

Le meilleur FAR est atteint en choisissant la méthode de classification avec la distance euclidienne, c'est ce qu'illustre le graphe suivant :

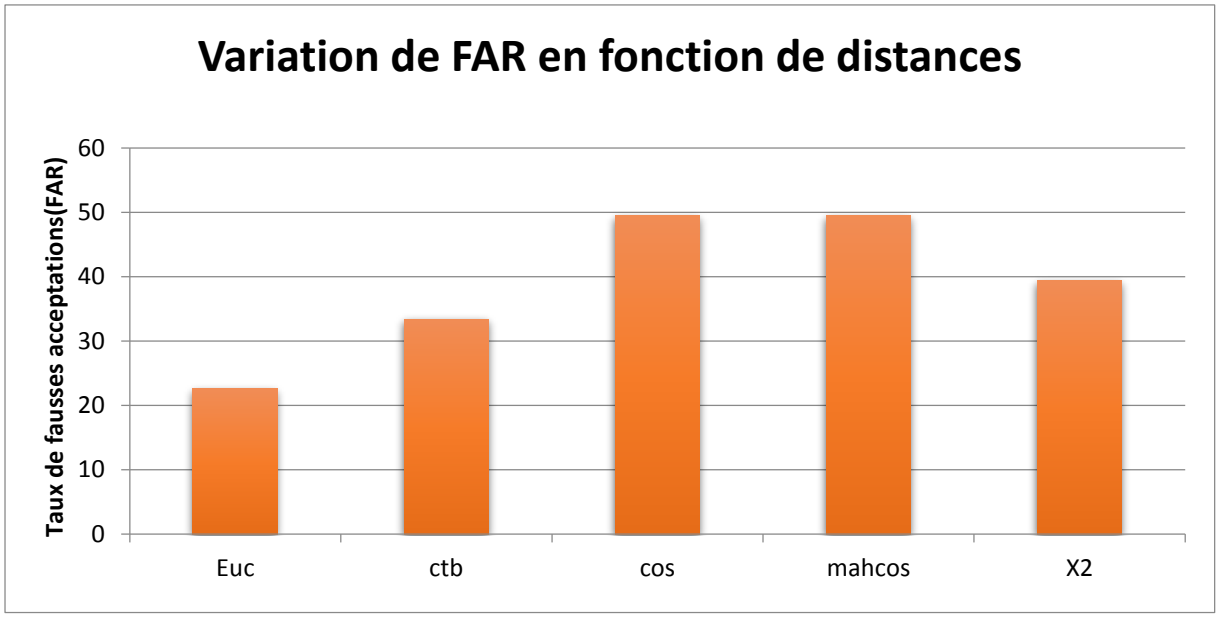

Figure V.11. Variation du taux de fausses acceptations FAR (%) en fonction des distances.

- **Effet de l'application du LBP et ses variantes et la méthode de classification sur le FRR :**

			Euclidienne	Ctb	cosine	mahcos	X2
LBP	Rayon 1	**Voisinage 4**	5.5	8.2	2.2	2.2	5.9
		Voisinage 8	15.9	10.5	3.4	3.4	10.2
		Voisinage 16	9.9	7.0	1.3	1.3	8.4
	Rayon 2	**Voisinage 4**	2.5	3.5	1.3	1.3	8.4
		Voisinage 8	12.90	7.0	3.5	3.5	11.3
		Voisinage 16	11.5	8.6	4.7	4.7	12.4

Tableau V.3. Variation du taux de faux rejets FRR (%) en fonction des distances et le rayon et le voisinage.

Dans le type LBP (1,16) et LBP (2,4) le FRR est meilleur (1,3%), on l'a varié en fonction des distances, on a trouvé les résultats suivants :

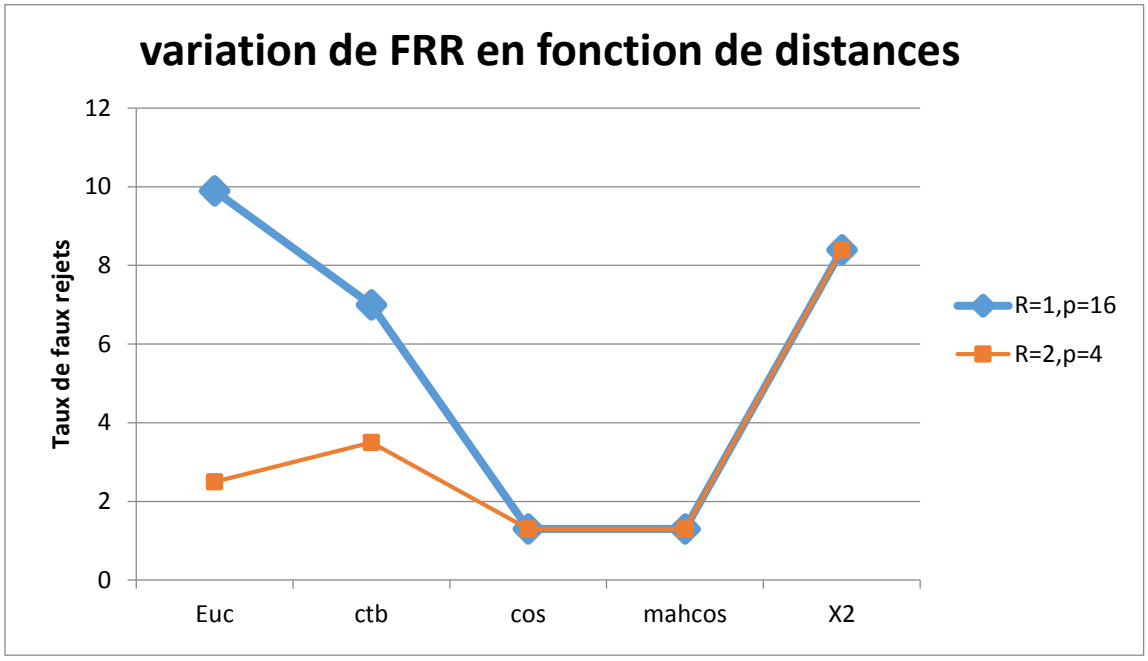

Figure V.12. Variation du taux de faux rejets FRR (%) en fonction de la distance.

On remarque à travers les résultats des tests voir (Tableau) et la figure ci-dessus qu'on atteint le taux de faux rejets FRR le plus bas avec la méthode de classification par les deux distances « Mahalcos » et « cosine ».

Synthèse 1 :

Après ces tests expérimentaux, les meilleurs résultats obtenus sont comme suivis :

- Meilleur résultat TID est **84,5** avec R=2 et P=16 en appliquant la distance « Ctb ».
- Meilleur résultat FAR est **22.57** avec R=1 et P=8 en appliquant la distance « euclidienne ».
- Meilleur résultat FRR est **1.3** avec R=2 et P=4 en appliquant la distance « cos » et « mahcos ».

V.2.2.3. Comparaison de l'approche LBP et l'approche CLBP :

➢ **Le taux d'identification entre LBP et CLBP en fonction des distances :**

	TID calculé avec LBP(1,8)	TID calculé avec CLBP(1,8)
Distance Euclidienne	72	71
Distance ctb	78	80
Distance cos	74.5	71
Distance mahcos	74.5	71
Distance X2	72.5	71

Tableau V.4.l.TID en fonction de la distance, LBP et CLBP.

La méthode CLBP donne le meilleur taux d'identification (80%) grâce au complément d'information contenu dans le S-CLBP, et M-CLBP et ça en appliquant la distance ctb. C'est ce qui est remarquable dans le graphe qui suit :

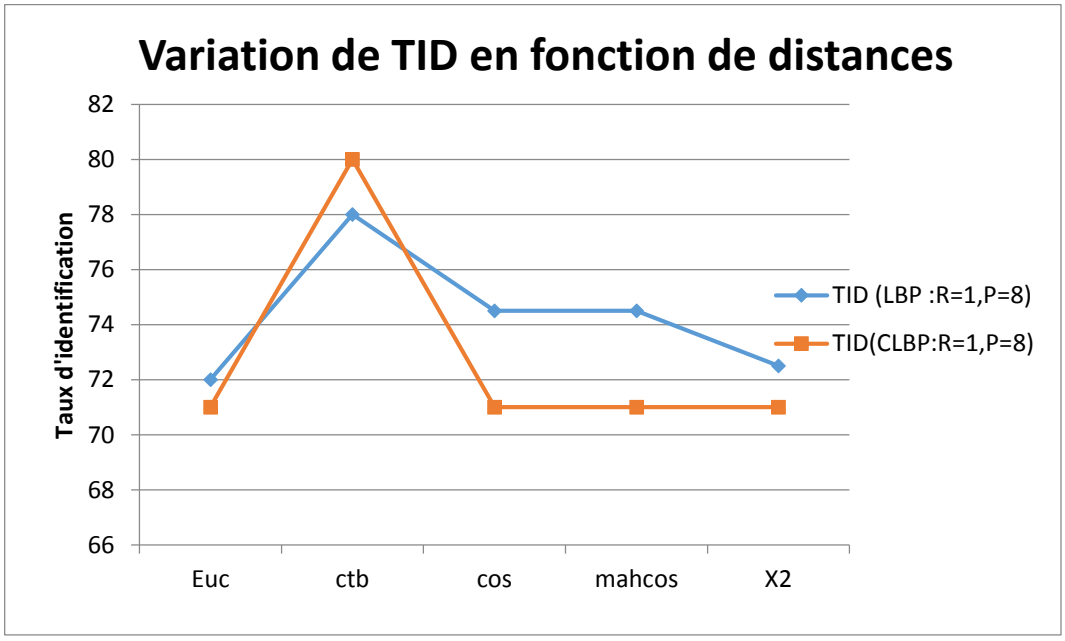

Figure V.13.le TID en fonction de la distance, LBP et CLBP.

On constate que les résultats sont proches dans les deux méthodes et le meilleur taux d'identification est atteint dans l'approche CLBP grâce au complément d'information contenu dans le S-CLBP, et M-CLBP.

➢ **Le taux de fausses acceptations (FAR) entre LBP et CLBP en fonction des distances :**

	FAR calculé avec LBP(1,8)	FAR calculé avec CLBP(1,8)
Distance Euclidienne	22.57	30.89
Distance ctb	33.39	33.75
Distance cos	49.45	48
Distance mahcos	49.45	48
Distance X2	39.39	40.97

Tableau V.5.le FAR en fonction de la distance, LBP et CLBP.

Les résultats de FAR en variant les distances utilisées et la méthode LBP et CLBP est donnés dans le graphe suivant :

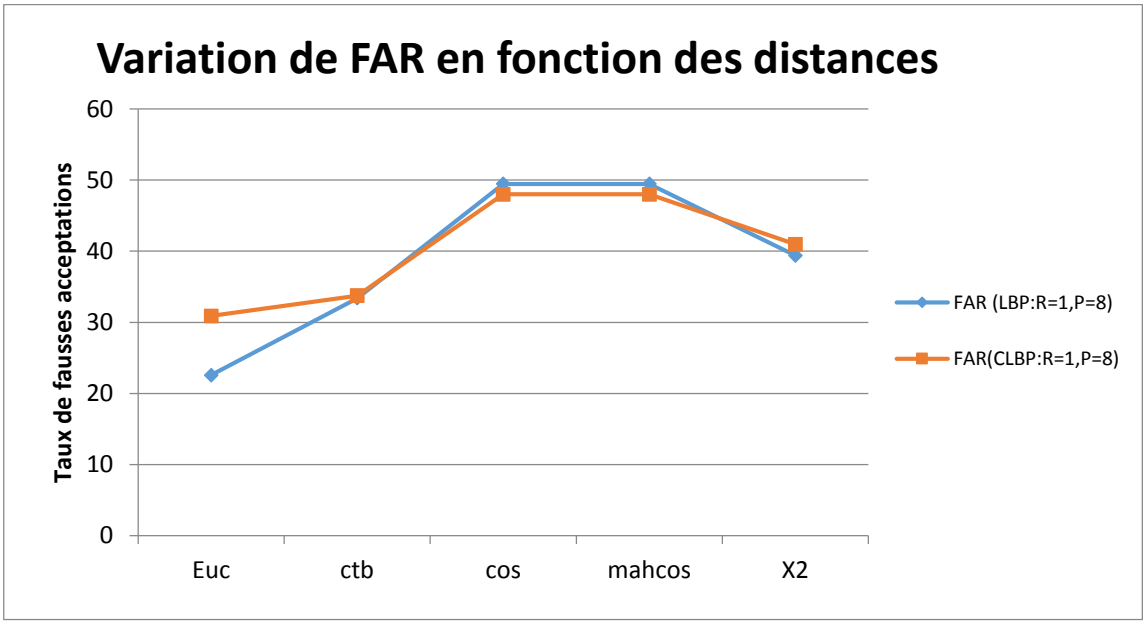

Figure V.14.le FAR en fonction de la distance, LBP et CLBP.

Les valeurs de FAR sont relativement proches dans les deux approches.et le meilleur résultat est trouvé en LBP (1,8).

➢ **Le taux de faux rejets (FRR) entre LBP et CLBP en fonction des distances :**

	FRR calculé avec LBP(1,8)	FRR calculé avec CLBP(1,8)
Distance Euclidienne	15.9	9
Distance ctb	10.5	6
Distance cos	3.4	1.6
Distance mahcos	3.4	1.6
Distance X2	10.2	4.8

Tableau V.6.le FRR en fonction de la distance, LBP et CLBP.

Les résultats de FRR en variant les distances utilisées et la méthode LBP et CLBP est donnés dans le graphe suivant :

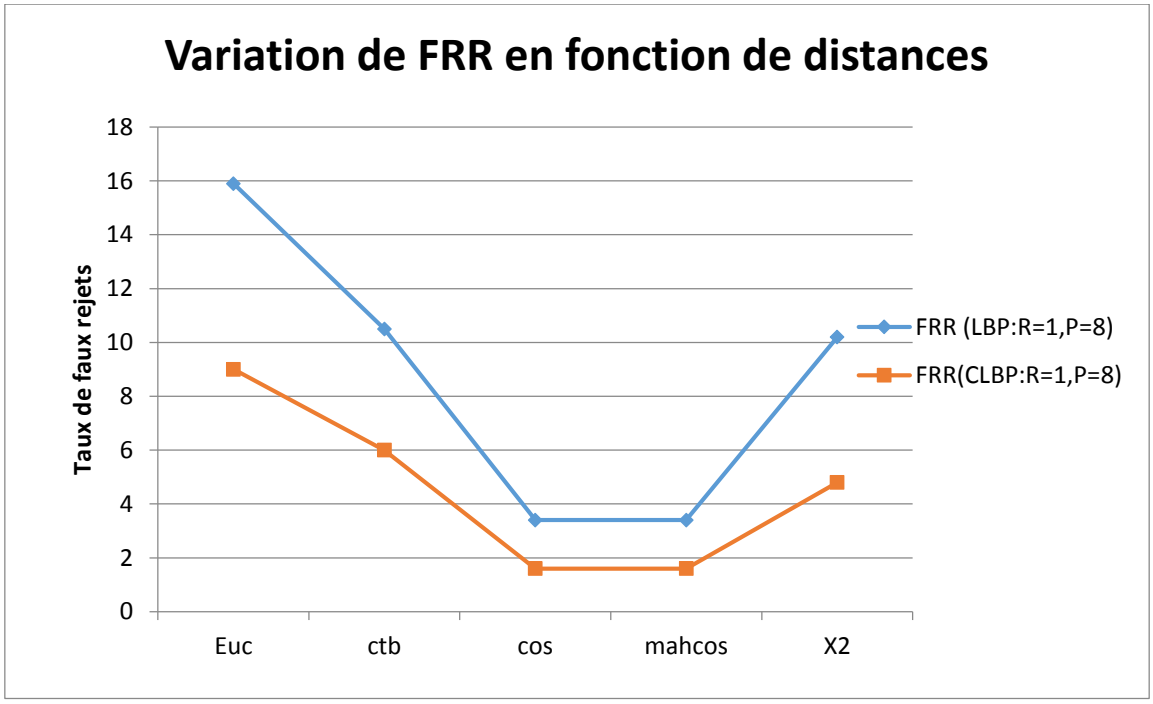

Figure V.15.le FRR en fonction de la distance, LBP et CLBP.

Le meilleur FRR est apparue dans l'approche CLBP en choisissant les distances « cos » et « mahcos ».

Synthèse 2 :

A travers ces tests effectués sur les deux approches, on peut résumer l'effet du choix de l'approche et la méthode de classification (les distances) dans ce qui suit :

-Meilleur TID est **80** donné par l'approche CLBP (1,8) en appliquant la distance « Ctb ».

-Meilleur FAR est **22.57** donné par l'approche LBP (1,8) en appliquant la distance « euclidienne ».

- Meilleur FRR est **1.6** donné par l'approche CLBP (1,8) en appliquant la distance « Cos » et « Mahcos ».

Le taux d'identification et le taux de faux rejets est meilleur dans l'approche CLBP grâce au complément d'information contenu dans le S-CLBP, et M-CLBP mais le taux de fausses acceptations est meilleur en utilisant l'approche LBP.

Conclusion :

Tout au long de ce chapitre, on a effectué des tests expérimentaux sur les différents paramètres constituant notre système de reconnaissance de visage, on a justifié les différents résultats obtenus par rapports aux différentes méthodes de classification et variantes utilisées.

Conclusion Générale

Conclusion et perspectives :

Ce travail s'inscrit dans le domaine de la reconnaissance automatique des visages. Celui-ci consiste à vérifier l'identité d'une personne à partir de son image. Utilisés principalement pour des raisons de sécurité et/ou confidentialité, les systèmes de reconnaissance automatique des visages sont souvent développés dans les applications de télésurveillance et l'accès à des endroits sécurisés.

La reconnaissance faciale est l'une des techniques biométriques les plus utilisées, elle présente un avantage d'être naturelle et facile à mettre en œuvre ; mais elle souffre d'un manque de fiabilité, à cause de l'influence des éléments externes tel que l'éclairage, la qualité du capteur et la variation des poses et des expressions.

En effet, nous avons conçu et réalisé un système de reconnaissance de visages dans ses deux modes (identification et vérification) basé sur l'approche LBP pour l'extraction et la modélisation de paramètres, la méthode de classification dite par mesure de similarité associé à cinq distance (Euclidienne," Mahalcos","Cosine", "Chi-carrée X2 " et la "norme Ctb"), dont nous avons constaté la puissance, la robustesse et la simplicité.

Dans notre système de reconnaissance, nous avons menés nos tests dans le but d'améliorer et d'évoluer ces performances dans ces deux modes (identification et vérification) en concluant la TID, FRR et FAR. A cet effet, les tests expérimentaux effectués sur la base de données ORL basés sur l'approche LBP et ses variantes (variation de rayon R et du point du voisinage P) et la variante CLBP, nous ont permis de constater que la modélisation par ces approches donne de meilleur résultat quand le voisinage augmente, et les mesures de performances sont meilleurs dans l'approche CLBP.

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

Par ailleurs, et dans le but d'améliorer notre travail nous avons relevé les perspectives suivantes :

-Effectuer plusieurs prétraitements afin d'améliorer la qualité de nos images.

-Comme c'était fait pour l'approche LBP, et pour améliorer la performance de notre système, lancer d'autres tests sur l'approche CLBP en augmentant plus le voisinage et le rayon

Conclusion et perspectives

-Utiliser la division en blocs pour l'image et appliquer l'approche LBP pour chaque bloc, ça emmène à améliorer la performance de notre système.

-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.

BIBIOGRAPHIE:

[1]: G. Roethenbaugh, "In Introcuction to biometrics and General History", Biometric Explained , Section 1,1998 .

[2]: N.Morizet « Reconnaissance biométrique par fusion multimodale du visage et de l'iris ». (Thèse de doctorat). Ecole doctorale d'informatique, télécommunication et électronique de Paris, France, 2009.

[3] : A.Charri, « Nouvelle approche d'identification dans les bases de données basées Sur une classification non supervisée ». (Thèse de doctorat). Université d'Evry d'Essone.

[4] : ATTALAH Billal, « Conception D'un système de reconnaissance des empreintes digitales par apprentissage ». (Thèse de magister).

[5] : BELILI Manel, FARSI Meriem, « Application de la DCT modifiée et GMM orthogonale Pour la vérification du visage ». (Thèse d'ingéniorat), 2012

[6] : BOUCHADDAK Mohamed, « Conception et Développement d'une application de gestion de temps de travail d'employés dans un parc d'entreprise ». Ecole supérieur de Communication de Tunis, 2007.

[7] : GUERFI ABANBSA.S, « authentification d'individus par reconnaissance de Caractéristiques biométriques liées aux visages, 2 D, 3D ». (Thèse de doctorat), université Evry Val d'Essone.

[8] : BOUJELLAL Sofiane, « Détection et identification de personne par méthode Biométriques ». (Thèse de magister), université Mouloud Mammeri Tizi-Ouzou (UMMTO).

[9] : BENCHENNANE Ibtissam, « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus ». (Thèse de doctorat).

[10] : Florent Peronnin et Jean-Luc Dugelay, « Introduction à la biométrie authentification Des individus par traitement Audio-Vidéo.

[11] : BETTAHAR. A et SABER. F, « Extraction des caractéristiques pour l'analyse

Biométrique d'un visage ». (Thèse de magister).

[12]: HASHIYADA. M, « development of biometric and ink for authentification Security ».

[13]: K. Phua, J. Chen, T.H.Dat and L.Shue.Heart "soud as a biometric. Pattern Recognition"

[14]: GUESMI Hannane, "Identification de personnes par fusion de différentes modalités Biométriques. (Thèse de doctorat).

[15] : Mohamed EL Abed, « Evaluation de système biométrique ».

[16] : Google Image : https://images.google.com

[17]: G. Roethenbaugh, "In Introcuction to biometrics and General History", Biometric Explained , Section 1,1998 .

[18]: N.Morizet « Reconnaissance biométrique par fusion multimodale du visage et de l'iris ». (Thèse de doctorat). Ecole doctorale d'informatique, télécommunication et électronique de Paris, France, 2009.

[19] : A.Charri, « Nouvelle approche d'identification dans les bases de données basées Sur une classification non supervisée ». (Thèse de doctorat). Université d'Evry d'Essone.

[20] : ATTALAH Billal, « Conception D'un système de reconnaissance des empreintes digitales par apprentissage ». (Thèse de magister).

[21] : BELILI Manel, FARSI Meriem, « Application de la DCT modifiée et GMM orthogonale Pour la vérification du visage ». (Thèse d'ingéniorat), 2012

[22] : BOUCHADDAK Mohamed, « Conception et Développement d'une application de gestion de temps de travail d'employés dans un parc d'entreprise ». Ecole supérieur de Communication de Tunis, 2007.

[23] : GUERFI ABANBSA.S, « authentification d'individus par reconnaissance de Caractéristiques biométriques liées aux visages,2 D, 3D ».(Thèse de doctorat), université Evry Val d'Essone.

[24] : BOUJELLAL Sofiane, « Détection et identification de personne par méthode

Biométriques ». (Thèse de magister), université Mouloud Mammeri Tizi-Ouzou (UMMTO).

[25] : BENCHENNANE Ibtissam, « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus ». (Thèse de doctorat).4

[26] : Florent Peronnin et Jean-Luc Dugelay, « Introduction à la biométrie authentification Des individus par traitement Audio-Vidéo.

[27] : BETTAHAR. A et SABER. F, « Extraction des caractéristiques pour l'analyse Biométrique d'un visage ». (Thèse de magister).

[28] : HASHIYADA. M, « development of biometric and ink for authentification Security ».

[29]: K. Phua, J. Chen, T.H.Dat and L.Shue.Heart "soud as a biometric. Pattern Recognition"

[30]: GUESMI Hannane, "Identification de personnes par fusion de différentes modalités Biométriques. (Thèse de doctorat).

[31] : Mohamed EL Abed, « Evaluation de système biométrique ».

[32] : MEBARKA BELAHCENE, Système de Reconnaissance de Visage .

[33] : Mr. GHALI Ahmed, Amélioration de la reconnaissance par le visage.

[34] : Kalghoum ANWAR, Institut supérieur d'informatique et de gestion de Kairouan en Tunisie, "Gestion des présences via la technologie de reconnaissance faciale ,2011.

[35] : M. A. Turk and A. P. Pentland, Face Recognition using Eigenfaces, Proc. IEEE, 1991, 586-591.

[36] : Nicolas MORIZET, Thomas EA, Florence ROSSANT, Frédéric AMIEL et AMARA. "Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie" P1-11. Institut Supérieur d'Electronique de Paris (ISEP), département d'Electronique, 2006.

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

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

[**39**] : Y. Hori, M. Kusaka, and T. Kuroda. "A 0.79mm2 29mW Real-Time Face Detection Core". Symposium on VLSI Circuits Digest of Technical Papers, pp. 188–

189, June 2006..

[**40**] : D. Bolme, J. Beveridge, M. Teixeira, and B. Draper. "The CSU Face Identification Evaluation System : Its Purpose, Features, and Structure". In : Proceedings of the 3rd International Conference on Computer Vision Systems (ICVS),

pp. 304–313, 2003.

[**41**] : Pierre Buyssens, Fusion de différents modes de capture pour la reconnaissance

du visage appliquée aux e- transactions (Thèse de Doctorat).

[**42**] : DJEDI Sara, Etude comparative de PCA et KPCA associées au SVM en

Biométrie.

[**43**] : Fabrice VERMONT, localisation de visage.

[**44**] : Mémoire online, lien :

http://www.memoireonline.com/02/13/6979/m_Reconnaissance - de- visages- parAnalyse-Discriminante- LineaireLDA- 4.html.

[45]: A.Hadid, T.Ahonen, Pietikäinen, Matti. «Computer vision using local binary Patterns». Springer, 2011.

[46]: R. HARALICK, K. SHANMUGAN, et I. DINSTEIN, « Textural features for image classification »; IEEE Transactions on Systems, Man and Cybernetics. 1973.

[47] : Belkacemi Lamia et Benamara Mohamed Adel, « Reconnaissance des personnes Par le visage dans des séquences vidéo », 2013

[48]: RODRIGUEZ Yann. « Face Detection and Verification using Local Binary Patterns». Thèse de doctorat à la faculté des sciences et techniques de l'ingénieur, Ecole Polytechnique Fédérale de Lausanne, Suisse. 2006

[49]: Z.Guo, L.Zhang, D.Zhang. «A Completed Modeling of Local Binary Pattern Operator for Texture Classification». IEEE tran .on image Processing. 2010.

[50]: P.Ronkainen. « A video-based face recognition system using local binary Patterns ». Thèse de master. Univesité d'Oulu, Finland. 2009.

[51] J. Sklansky. « Image segmentation and feature extraction ». Systems, Man and Cybernetics, IEEE Transactions on, 1978.

.

[52]: R.M. Haralick. « Statistical and structural approaches to texture ». Proceedings of the IEEE, 1979

[53]: M. Unser. « Description statistique de la texture. Application à l'inspection automatique ». Thèse de doctorat, EPFL, Lausanne, 1984.

[54]: T. Ojala, Pietikainen, M., & Harwood, D., "A comparative study of texture measures with classification based on feature distributions.," *In Pattern Recognition,* 1996.

[55]: Ojala, T., Pietikäinen, M., Mäenpää, T.: Multiresolution gray-scale and rotation invariant

texture classification with local binary patterns. IEEE Trans. Pattern Anal. Mach. Intell, 2002.

[56]: Ahonen, T., Hadid, A., Pietikäinen, M.: Face description with local binary patterns: Application to face recognition. IEEE Trans. Pattern Anal. Mach. Intell, 2006.

[57]: Mäenpää, T., Pietikäinen, M.: Texture analysis with local binary patterns. In: Chen, C.H, Wang, P.S.P. (eds.) Handbook of Pattern Recognition and Computer Vision. World Scientific, Singapore (2005).

[58] Ojala, T., Pietikäinen, M.: Unsupervised texture segmentation using feature distributions. Pattern Recognit, 1999.

[59] Kellokumpu, V., Zhao, G., Pietikäinen, M.: Dynamic texture based gait recognition. In: Advances in Biometrics. Lecture Notes in Computer Science.

[60] Ghoulia. B, Kouidri. Y : Etude comparative d'ensemble des descripteurs de texture pour la reconnaissance de visages, 2017

[61] T. Ahonen, A. Hadid, and M. Pietikainen. Face recognition with local binary patterns. In ECCV, 2004.