REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université 8 Mai 1945 – Guelma
Faculté des Sciences et de la Technologie
Département de Génie Electrotechnique et Automatique

Réf :2023 /2024

MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER Académique**

Domaine : Sciences et Technologie

Filière : Automatique

Spécialité : Automatique et Informatique industrielle

Par *: MEDJELEKH MOHAMED CHARIF et MERABTI ABDERRAHMEN*

Thème

Système de reconnaissance faciale

Soutenu publiquement, le 23/juin /2024. Devant le jury composé de :

M. Moussaoui Abdelkrim	Professeur	Univ. Guelma	Président/ Examinateur
Mme. Kechida Sihem	Professeur	Univ. Guelma	Examinateur principal
M. Griouz Badreddine	Professeur	Univ. Guelma	Encadreur

Année Universitaire : 2023/2024

TABLE DES MATIERES

REMERCIEMENT

Tout d’abord merci au bon DIEU le tout puissant, de nous avoir donné la force, la patience et la volonté pour réaliser ce travail dans des meilleures circonstances.

Nous ne saurons suffisamment remercier la personne qui nous a aidés à réaliser ce travail dans les meilleures conditions notre encadreur monsieur B.Geriouz Pour son encadrement, sa collaboration sérieuse et sa documentation, pour réaliser ce projet.

Nous remercions aussi tous les enseignants et les responsables du Département de génie électrotechnique et automatique de l’université de Guelma pour leurs aides et leurs encouragements.

Nous remercions également l’ensemble des membres de jury qui nous font l’honneur d’accepter de juger notre travail.

On remercier également nos parents pour leur soutien moral et financier durant nos études.

Sans oublier mes collègues durant les années d’étude.

Dédicace

Je dédie ce travail en premier lieu à nos chers parents Pour leur patience, leur amour, leur soutien et leurs encouragements.

A nos chers frères et sœurs.

Sans oublier tous les professeurs que ce soit du

Primaire, du moyen, du secondaire ou d'enseignement supérieur.

Enfin, je n'oublier pas tous mes amis et ma grande famille.

LISTE DES FIGURES

LISTE DES TABLEAUX

ABREVIATIONS ET SYMBOLES

IBG.	International Biometric Group.
FAR	False Acceptance Rate.
FRR	False Rejection Rate.
ROC	Receiver Operating Characteristic.
DET	Detection Error Tradeoff.
EER.	Equal Error Rate.
WER	Weighted Error Rate.
HTER	Half-Total Error Rate.
WTER	Weighted Total Error rate.
MIT	Machine Learning Techniques.
FRVT	Facial Recognition Vendor Test.
FERET	Facial Recognition Technology Database.
KNN	Plus proches voisins.
LBP	Local Binary Patterns.
LPQ	Local Phase Quantization.
BSIF	Binarized Statistical Image Features
SVM	Machine à vecteurs de support.
CNN	Convolutional Neural Network
ORL	Olivetti Research Laboratory.

INTRODUCTION GENERALE

Dans un monde où la sécurité et l'efficacité des systèmes d'identification sont de plus en plus cruciales, la biométrie s'affirme comme une solution technologique de premier plan. La biométrie, qui repose sur l'analyse des traits physiologiques, chimiques ou comportementaux d'un individu tels que le visage, l'iris, l'odeur, la démarche ou la signature électronique, offre des méthodes d'authentification d'identité plus sûres et fiables. Particulièrement tel système se fait particulièrement sentir dans des domaines critiques comme le contrôle d'accès sécurisé, le franchissement des frontières internationales et les applications légales. Ce mémoire s'attache à explorer en profondeur les aspects théoriques et pratiques de la biométrie, en mettant l'accent sur la reconnaissance faciale, l'une des modalités biométriques les plus prometteuses.

Le premier chapitre introduit les concepts fondamentaux de la biométrie. Il définit cette discipline en détaillant ses caractéristiques principales, ses différentes modalités et ses domaines d'application. La biométrie est présentée comme une technologie émergente capable de répondre aux exigences croissantes de sécurité et de gestion de l'identité à grande échelle.

Le deuxième chapitre se concentre sur l'utilisation du visage comme méthode biométrique. La reconnaissance faciale, bien que naturelle et intuitive pour les humains, pose des défis considérables pour les systèmes informatiques. Depuis la fin des années soixante-dix, ce domaine est devenu un axe de recherche majeur, en raison de ses nombreuses applications, notamment dans la surveillance des lieux publics. Diverses méthodes ont été développées pour l'identification des individus à partir de leurs visages, exploitant aussi bien des images fixes que des séquences vidéo.

Le troisième chapitre détaille les étapes essentielles de la reconnaissance faciale. Il couvre le prétraitement des images, l'extraction des caractéristiques et les méthodes de classification. L'importance du prétraitement pour améliorer la qualité des données et réduire les variations indésirables est mise en avant. Les techniques d'extraction des caractéristiques, telles que l'approche des eigenfaces, Local Binary Patterns (LBP), Local Phase Quantization (LPQ) et Binary Robust Independent Elementary Features (BSIF), sont explorées. Ensuite, les algorithmes de classification comme la Machine à Vecteurs de Support (SVM) et les K plus proches voisins (KNN) sont discutés. Enfin, des techniques de réduction de dimensionnalité comme l'Analyse Discriminante Linéaire (LDA) et la PCA sont examinées pour optimiser la représentation des données et améliorer la précision de la classification.

Le dernier chapitre présente les résultats obtenus à partir de la base de données ORL, illustrant l'efficacité et la précision des méthodes discutées précédemment. Ces résultats démontrent la faisabilité et les performances des systèmes de reconnaissance faciale développés, validant ainsi les approches théoriques et méthodologiques adoptées dans ce mémoire.

Ce mémoire vise à offrir une compréhension globale de la biométrie, avec un focus particulier sur la reconnaissance faciale, et à démontrer comment des techniques avancées peuvent être intégrées pour créer des systèmes d'identification fiables et performant

Chapitre I : La biométrie

I.1. Introduction

La biométrie constitue la discipline permettant d'authentifier l'identité d'un individu en se basant sur ses traits physiologiques, chimiques ou comportementaux tels que le visage, l'iris, l'odeur, la démarche ou la signature électronique, entre autres. En réponse à la nécessité de méthodes fiables d'identification humaine dans des contextes critiques tels que le contrôle d'accès sécurisé, le franchissement des frontières internationales et les applications légales, la biométrie émerge comme une technologie viable pouvant être intégrée dans des systèmes de gestion d'identité à grande échelle [1]. Ce chapitre vise à définir le concept de biométrie, à explorer ses caractéristiques, ses modalités et à examiner ses domaines d'application.

I.2. Définition de la biométrie

La biométrie est une technologie qui regroupe l'ensemble des techniques informatiques visant à reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. Les données biométriques ont la particularité d'être uniques et permanentes. Elles permettent de ce fait le "traçage" des individus et leur identification certaine [2].

I.2.1. Origine de la biométrie

La biométrie est l'héritière de l'anthropométrie, inventée en 1882 par le criminologiste français Alphonse Bertillon, permettant la reconnaissance des personnes arrêtées et condamnées sur la base de photos et d'informations signalétiques (mensurations osseuses, signes particuliers). Adopté par la plupart des services de police européens et américains, ce système a été ensuite abandonné en raison de son manque de précision.

I.2.2. Caractéristiques Biométriques

Une caractéristique biométrique est une donnée contenant l'essentiel des informations permettant de différencier deux individus. Pratiquement n'importe quelle caractéristique physiologique ou comportementale peut être considérée comme une caractéristique biométrique, également appelée modalité.[3 Sept facteurs déterminant la convenance des traits physiques ou comportementaux pour être utilisés dans une application biométrique ont été identifiés. [4].

- Universalité : toute personne ayant accès à l'application doit posséder le trait.
- Unicité : le trait doit être suffisamment différent d'une personne à une autre.
- La permanence : ceci signifie que le trait biométrique ne change pas dans le temps.
- Mesurabilité : il devrait être possible d'acquérir et de numériser les données biométriques à l'aide d'un dispositif approprié.
- La performance : ceci spécifie non seulement la réalisation d'une vérification exacte, mais également les conditions de ressource de réaliser avec exactitude une vérification acceptable.
- La robustesse : ceci se rapporte à l'influence du fonctionnement ou des facteurs environnementaux (canal, bruit, déformations...) qui affectent l'exactitude de la vérification [5].
- Acceptabilité : les individus qui vont utiliser cette application doivent être disposés à présenter leurs traits biométriques au système.

I.2.3. Domaine d'application

Les applications de la biométrie peuvent être très diverses ; les limitations ne peuvent être que l'imagination d'un individu. Il est devenu alors que le collecteur des modèles différents est utilisé dans différentes zones pour différents types de fonctionnalités. Quelques applications de la biométrie dans les différents secteurs sont présentées :

- Les propriétaires sont facilitées par la biométrie coffre-fort et serrures biométriques, qui permettent la plus grande sécurité et de fiabilité.
- Entrée de petits bureaux ou de grandes organisations, résidentielles, les institutions et le gouvernement peuvent être garantis grandement avec l'utilisation de systèmes de contrôle d'accès biométriques.
- La mise en œuvre de la biométrie dans les services financiers tels que les guichets automatiques, les kiosques, l'enregistrement de compte bancaire permet d'individualiser et de garder l'intimité privée.
- Dans des domaines tels que les services sociaux et les soins de santé, la biométrie peut éviter les droits frauduleuses et de renforcer la vie privée des dossiers médicaux.
- Dans les dispositifs électroniques, tels que les téléphones intelligents, les tablettes, les cartes téléphoniques, les ordinateurs personnels, l'accès au réseau, l'accès et la connexion à Internet peut être pris énormément privé et sécurisé.

- La biométrie est largement utilisée dans l'application de la loi, par exemple, la personnalisation de permis de conduire, l'identification contrôlée dans les établissements correctionnels et des prisons, des fusils intelligents, le confinement de la maison et des appartements, des enquêtes, l'identification et l'authentification des criminels avec une grande précision, une meilleure sécurité de l'aéroport. [6].

La variation des applications avancées ci-dessus, montre la polyvalence et la large gamme de facilité d'utilisation des systèmes biométriques qui ne se limite pas à un usage individuel, ni est-il uniquement aux buts juridiques; il est l'outil de chacun pour assurer Droit à la vie privée et la véritable pratique d'identification.

I.2.4. Le marché mondial de la biométrie

IBG (International Biometric Group) édite régulièrement un rapport sur le marché de la biométrie. 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 figure 1.1 montre les revenus du marché de la biométrie prévu entre l'année 2009 et 2014.

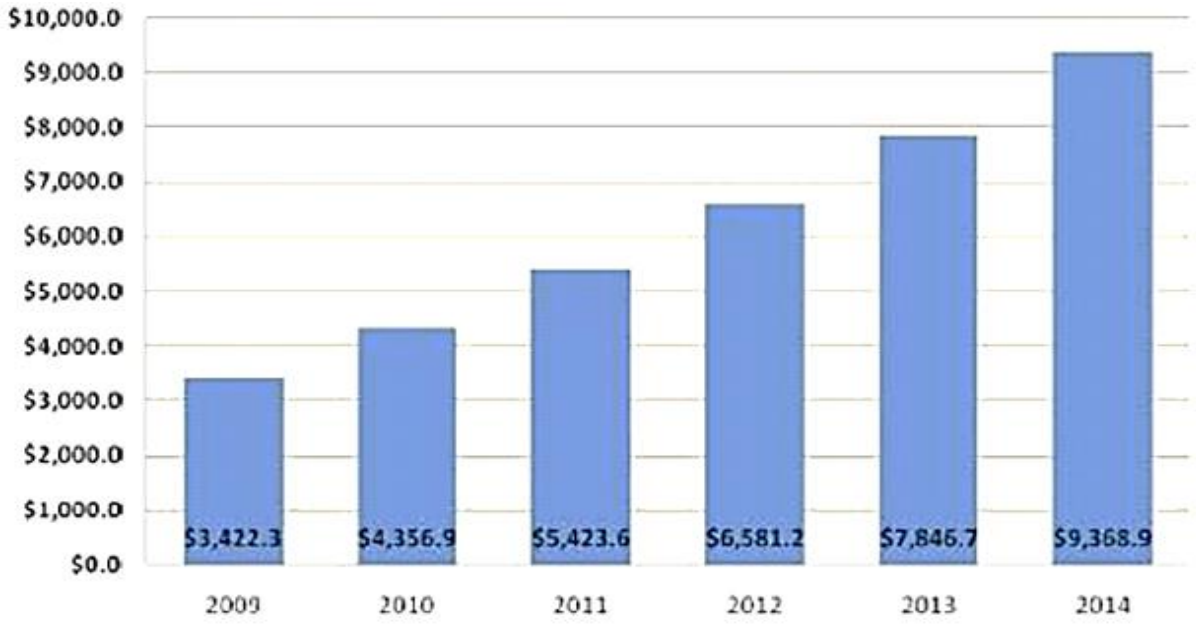

Figure 1. 1: Revenus de la vente de technologies biométriques de 2009 à 2014 selon IBG.

I.2.5. Les modalités biométriques

Chaque caractéristique biométrique qui satisfait aux conditions précédentes, peut être utilisée pour identifier un individu, elle est appelé modalité biométrique, et se classer selon le type : physiologique ou comportementale, comme le montre la Figure 1.2

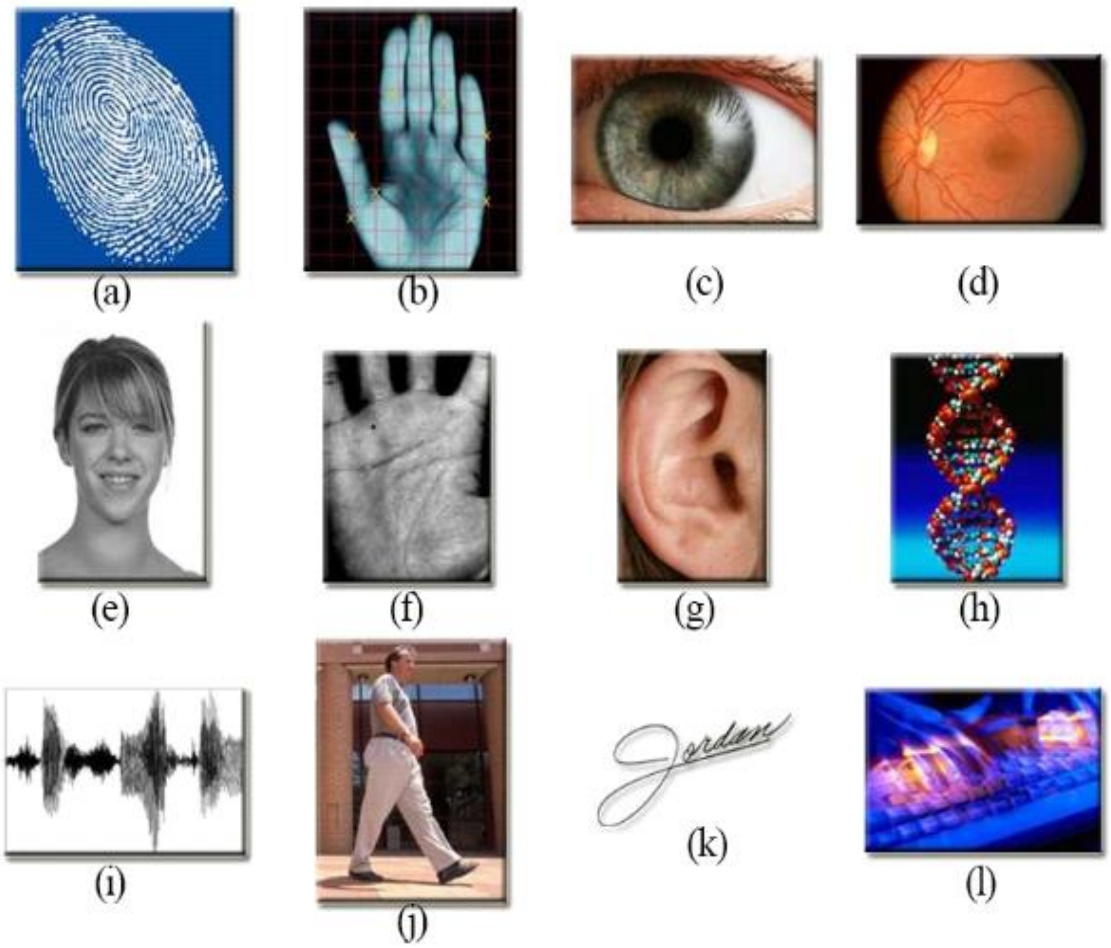

Figure 1. 2: Exemples de modalités biométriques (physiologiques et comportementales).[8]

- **Les modalités physiologiques ou morphologiques (également nommés statique ou passive) :**

Ces modalités sont basées sur les caractéristiques anatomiques ou physiologiques. Ces caractéristiques sont obtenues sans qu'il soit nécessaire que les utilisateurs effectuent une action spécifique. Les modalités les plus communes qui appartiennent à ce groupe sont : empreintes digitales, le visage, l'iris, la rétine, la main / géométrie de doigt, la paume, la reconnaissance

des formes vasculaires et de l'ADN. Il y a aussi de nouvelles modalités telles que la forme de l'oreille ou l'odeur corporelle.

- **Empreinte digitale :** L'identification à l'aide des empreintes digitales est la technique biométrique que la plupart de gens connaissent. Il s'agit de la plus vieille technique biométrique [7], les lecteurs d'empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Ces éléments sont appelés minuties [8]. L'utilisation est facile, il suffit de poser le doigt au-dessus du lecteur, mais certaines personnes peuvent créer de "faux doigts" [7]
- **Visage :** Le visage est sujet à une variabilité tant naturelle (vieillissement, par exemple) que volontaire (des produits de beauté, chirurgie esthétique, grimaces...). Cette réalité demeurera un défi pour des systèmes d'identification de visage. La reconnaissance du visage est utilisée comme système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics. Elle est parmi les techniques les plus acceptables, mais elle nécessite un arrière-plan simple et fixe pour que le résultat soit précis [7].
- **L'iris :** L'iris est la partie colorée de l'œil qui entoure la pupille noire. L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Son inspection attentive révèle de nombreuses structures détaillées uniques et indépendantes du code génétique de l'individu et pratiquement ne varient pas pendant la vie

- **Les modalités comportementales (également nommées dynamique ou active) :**

Ces modalités sont basées sur les caractéristiques biométriques qui impliquent l'exécution de certaines activités. Cette activité entraîne un comportement qui a été appris ou acquis au fil du temps. Ces modalités sont la signature dynamique, frappe, et l'une des plus récentes reconnaissances de la, démarche. Reconnaissance vocale est également une autre modalité biométrique qui pourrait être classé dans ce groupe, même si elle implique vraiment les caractéristiques physiques et comportementales.

Écriture (signature) : La vérification par signature comme technique est parmi les premières utilisées dans le domaine de la biométrie. Elle se base généralement sur le fait que l'utilisateur signe avec un stylo électronique sur une palette graphique. Il y a plusieurs systèmes concurrents

dans ce domaine analysant les caractéristiques spécifiques d'une signature comme précision géométrique, variations de vitesse, pression exercée sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé…. Ces données sont enregistrées pour comparaison ultérieure. Certains systèmes ne font qu'enregistrer l'image statique de la signature pour comparaison [8].

Voix humaine : est une caractéristique biométrique intéressante, puisqu'elle dépond des facteurs comportementaux et physiologiques. Initialement une table de référence de la voix d'une personne doit être construite. Pour ce faire, celle-ci doit lire une série de phrases ou de mots à plusieurs reprises. L'identification par la voie est basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son

Démarche : Il s'agit de reconnaître un individu par sa façon de marcher et de bouger. En analysant les déformations des jambes et bras au niveau des articulations. La démarche serait en effet étroitement associée à la musculature naturelle donc elle est très personnelle [9], l'intérêt de cette technologie réside que l'identification de démarche se situe dans la capacité d'identifier un individu à distance.

Dynamique de frappe au clavier : Un tel système est peu coûteux, mais pas celui-ci car il ne nécessite pas de matériel d'acquisition autre que le clavier de l'ordinateur. Il s'agit d'un dispositif logiciel qui calcule la durée entre frappes, fréquence des erreurs où son temps de relâchement « Software Only », cette mesure est capturée environ mille fois par seconde, elle est appliquée au mot de passe qui devient ainsi beaucoup plus difficile à «imiter », lors de la mise en place de cette technique il est demandé à l'utilisateur de saisir son mot de passe une dizaine de fois de suite.

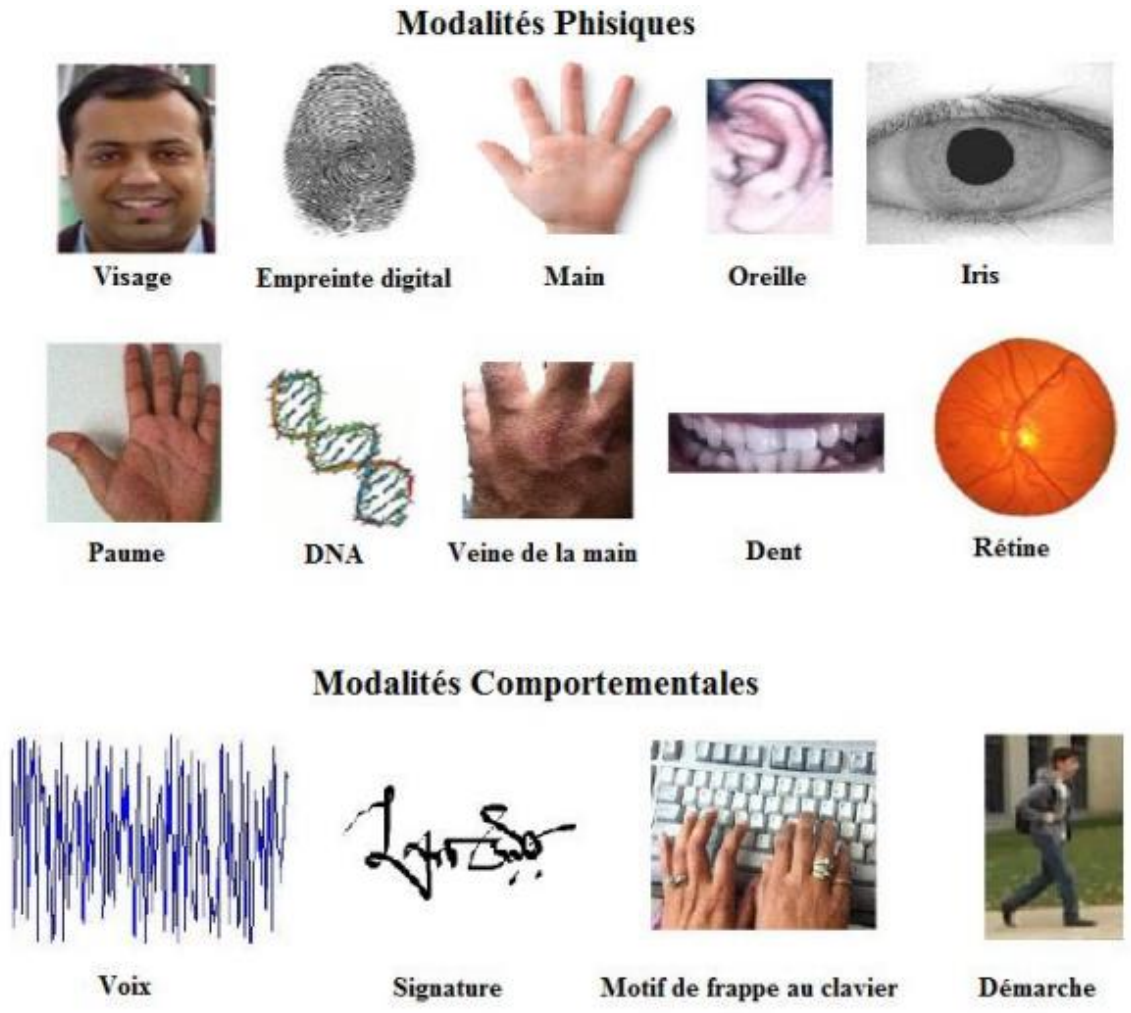

Figure 1. 3: Différentes modalités biométriques physiques et comportementales.[8]

I.2.6. Les différentes techniques biométriques

La comparaison entre les différentes biométries permet de choisir une technologie en fonction des contraintes liées à l'application. En effet, chaque caractéristique (ou modalité) biométrique a ses forces et ses faiblesses, et faire correspondre un système biométrique spécifique à une application dépend du mode opérationnel de l'application et des caractéristiques biométriques choisies.

- **Les avantages et les inconvénients des différentes modalités biométriques.**

Le Tableau 1.1 compte les avantages et les inconvénients des différentes modalités biométriques.

Tableau 1. 1 : Avantages & inconvénients des différentes modalités.

Modalités	Avantages	Inconvénients
Iris	– L'iris recèle plus de données que les empreintes digitales. – Stable durant toute la vie d'une personne. – Technique fiable	– Les effets d'illumination et d'occlusion (les yeux bougent quand on capture l'image). – La qualité de l'image n'est pas bonne. – Les contours de la pupille et de l'iris ne sont pas circulaires. – Nécessite des dispositifs de détection spéciaux.
Visage	– Technique moins cher. – Visage capturé à distance – Technique simple	Technologie sensible à : – Les variations d'âge. – À l'utilisation des artifices (moustaches, barbe, lunettes…). – Les variations expression et poses. – variations d'illumination
Empreintes digitales	– Laissons derrière nous à chaque fois que nous touchons un objet.	– Difficulté de lire l'empreinte digitale pour les travailleurs manuels. – Images à faible contraste

	– Nous aider à la recherche sur une scène de crime – Elles sont fiables et inchangeable durant la vie d'un individu.	– Mauvaise acquisition d'image – Nécessite dispositifs de détection spéciaux. Nécessitant un contact physique
Signature	– Plus confortable – Utilisé dans le document administratif. – Accepter par les personnes – Rapide et efficace	– Besoin d'une tablette graphique – On ne peut pas utiliser à contrôle d'accès extérieur Les signatures falsifiées (imitation
Voix	– Efficace au téléphone – Rapide et efficace – acceptées par les personnes	– Sensible au bruit ambiant. – Voix enregistrées Sensible à l'état physique et émotionnel de l'individu

- **Comparaison entre les différentes modalités biométriques**

Le Tableau I.2 présente une comparaison des modalités biométriques existantes en fonction de ces caractéristiques [10] :

Tableau 1. 2: Comparaison des modalités biométriques (H=Haut, B=Bas et M=Moyenne).

Modalités	Universalité	Unicité	Permanence	Performance	Acceptabilité	Contre la falsification
L'iris	H	H	H	H	B	H
Le visage	H	B	M	B	H	B
L'ADN	H	H	H	H	B	B
La voix	M	B	B	B	H	B
La signature	L	B	B	B	H	B
l'oreille	M	M	H	M	H	M
La rétine	H	H	M	H	B	H
La démarche	M	B	B	B	H	M
L'empreinte digitale	M	H	H	H	M	H

I.3. Le système de la reconnaissance biométrique

Un système biométrique est essentiellement un système qui acquiert des données biométriques d'un individu, extrait un ensemble de caractéristiques à partir de ces données, puis le compare à un ensemble de données stocké au préalable dans une base de données pour pouvoir enfin exécuter une action ou prendre une décision à partir du résultat de cette comparaison [4]. Comme le montre la Figure I.4, la structure globale de tout système biométrique se compose de quatre étapes principales, qui fonctionnent de manière séquentielle pour obtenir le résultat du système

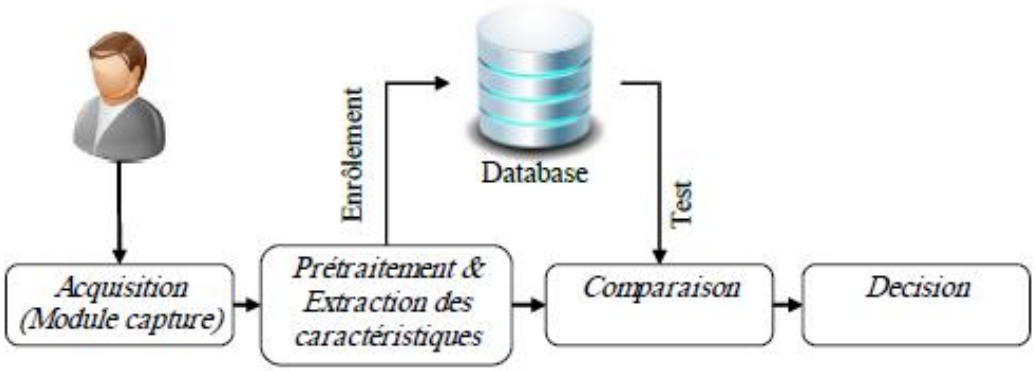

Figure 1. 4: La structure globale d'un système biométrique.[4]

I.3.1. Structure d'un système biométrique

La structure d'un système biométrique est toujours la même et comprend deux phases distinctes : l'enregistrement et l'authentification pour une application de vérification ou identification.

Un système biométrique comprend 4 modules (Figure 1.4) dont certains sont communs à la phase d'enregistrement et à celle d'authentification : l'acquisition, l'extraction des caractéristiques, la comparaison et la décision.

L'acquisition et l'extraction de caractéristiques ont lieu lors de l'enregistrement et lors de l'authentification. L'extraction de caractéristiques est une représentation de la donnée (par exemple image ou signal temporel acquis) sous la forme d'un vecteur que l'on cherche à être à la fois représentatif de la donnée et discriminant vis à vis des autres données (issues d'autres personnes). Lors de l'enregistrement, le vecteur des caractéristiques extrait de l'échantillon biométrique est appelé référence et est stocké sur le support personnel ou dans une base de données selon l'application. Lors de la phase d'authentification, les modules d'acquisition et d'extraction de caractéristiques permettent d'obtenir une représentation de la donnée biométrique à tester dans l'espace des caractéristiques.

Le module de comparaison est utilisé lors de la phase d'authentification pour comparer les vecteurs de caractéristiques de référence et de test.

Le module de décision sert ensuite à prendre une décision à partir de la sortie du module de comparaison qui correspond à un score de similarité entre les deux vecteurs de caractéristiques (souvent un nombre réel entre 0 et 1).

I.3.2. Le mode de reconnaissance

La reconnaissance peut être une vérification ou une identification [11].

- **Le mode de vérification ou d'authentification**

La vérification est une comparaison "un à un", dans laquelle le système valide l'identité d'une personne en comparant les données biométriques saisies avec le modèle biométrique de cette personne stocké dans la base de données du système. Dans un tel mode, le système doit alors répondre à la question suivante : «Suis-je réellement la personne que je suis en train de proclamer?»

- **Le mode d'identification**

C'est une comparaison "un à N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. Ce mode consiste à associer une identité à une personne. En d'autres termes, il répond à des questions de type : ` Qui suis-je ?'.

Les schémas d'un système de vérification et d'un système d'identification sont illustrés dans la figure I.5 ; le processus d'enrôlement, qui est commun à ces deux tâches est également illustré. Le module d'enrôlement correspond à l'enregistrement biométrique des individus dans la base de données du système. Pendant la phase d'enrôlement, la caractéristique biométrique d'un individu est capturée par un lecteur biométrique pour produire une représentation numérique.

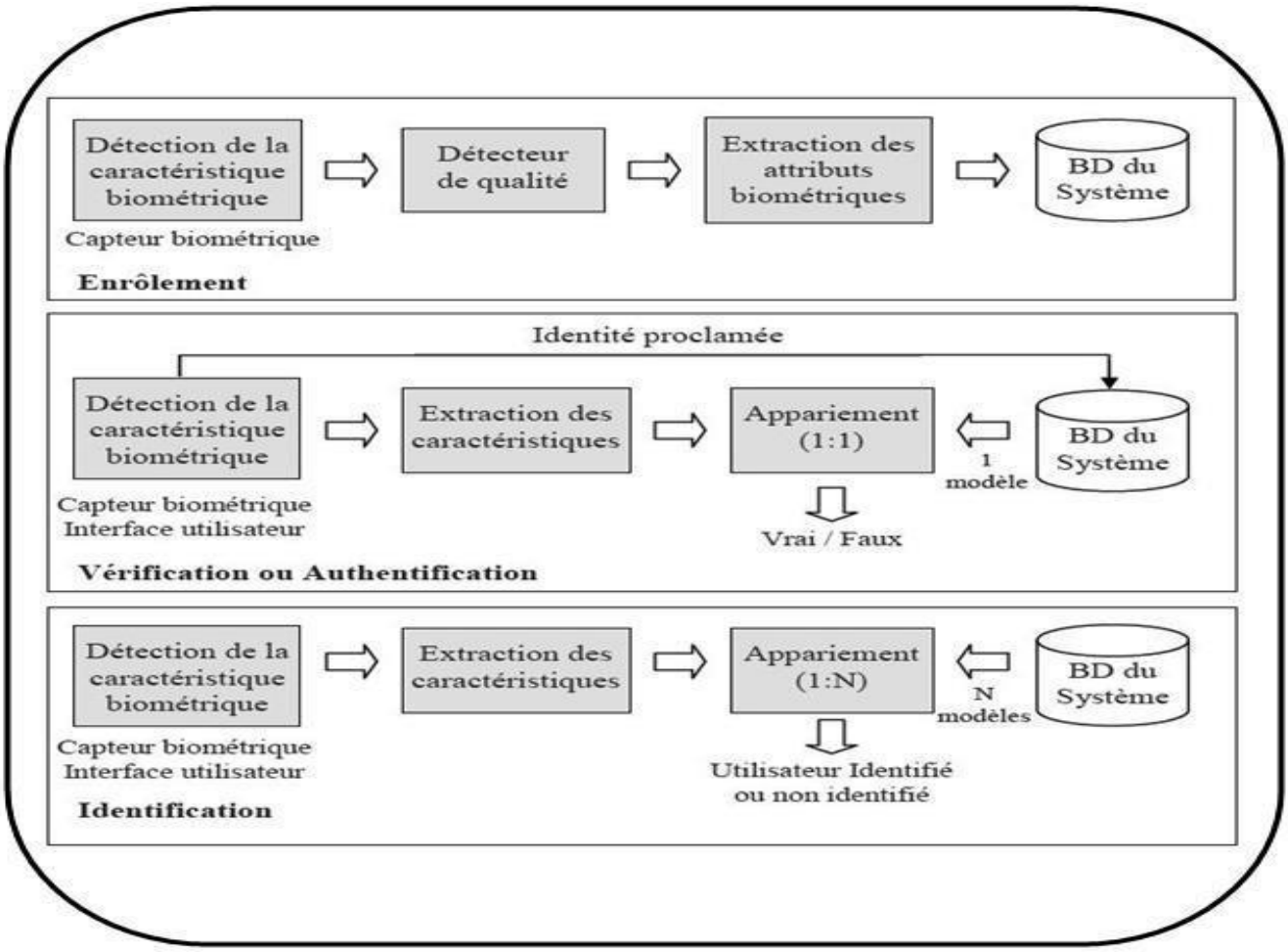

Figure 1. 5: Diagrammes des processus d'enrôlement, de vérification et d'identification.[11]

I.4. Evaluation des performances des systèmes biométriques

Une question qui se pose souvent dans ce domaine est la suivante :

« Quelle est la meilleure technique biométrique ? » La réponse naturellement est qu'il n'y a aucune meilleure technique biométrique en termes absolus, tout dépend de la nature précise de l'application et des raisons de son exécution. L'International Biométrique Group [IBG] a effectué une étude basée sur quatre critères d'évaluation :

Intrusive : l'existence d'un contact direct entre le capteur utilisé et l'individu à Reconnaitre, comme la reconnaissance par l'iris qui est jugée comme étant intrusive

Fiabilité : Elle dépend de la qualité de l'environnement (éclairage par exemple) dans lequel se trouve l'utilisateur. Ce critère influe sur la reconnaissance de l'utilisateur par le système.

Coût : Il se doit d'être modéré, c'est-à-dire que la collecte de l'information ne doit pas être relativement coûteuse pour établir une base de données, exemple : pour une reconnaissance de l'iris un appareil photo numérique d'une certaine qualité est nécessaire.
Effort : Il est requis par l'utilisateur lors de la saisie de mesures biométrique, et il doit être réduit le plus possible.

Au même temps, En représentant par définir les différentes mesures des taux d'erreur en vérification d'identité des systèmes biométriques et les courbe de performance. Ensuite, nous présenterons les points de fonctionnement et son déférent type et les points de fonctionnement.

Pour estimer les performances d'un système biométrique, Philips et al ont défini trois types d'évaluation différenciés par le niveau de spécificité d'une application l'évaluation technologique, l'évaluation de scénario et l'évaluation opérationnelle.

I.4.1. Mesure des taux d'erreur

Nous allons nous concentrer sur l'évaluation "technologique" des systèmes biométriques, c'est-à-dire, une évaluation de leurs taux d'erreurs pour la vérification d'identité en utilisant une base de données biométriques, Il y a donc des "erreurs" des systèmes biométriques que nous ne traiterons pas car elles dépendent du module d'acquisition. Ces "erreurs" sont en réalité des impossibilités d'acquisition.

Lorsque l'on évalue la partie "algorithmique" des systèmes biométriques on encore détecter deux types d'erreur :

Impossibilités de comparaison : (dépend du module d'extraction ou du module de comparaison) : Ce type d'erreur est dû au module de traitement (extraction et comparaison) qui contient en général une partie contrôle qualité. Si le système est incapable de fournir un score associé à une comparaison on parle alors d'impossibilité de comparaison ("failure to match" en anglais).
Erreurs de classification : (dépend du module de décision et donc du seuil de décision) : Il existe 2 types d'erreurs de classification correspondant aux mauvaises décisions pour les 2 classes (Client et Imposteur) mesurées de manière différente. Ces erreurs de décision sont de deux types :
Fausses Acceptations (FA) **:** si le système déclare l'individu comme étant le client alors que c'est un imposteur.
Faux Rejets (FR) **:** si le système rejette l'individu alors que c'est le client.

Lors de l'évaluation d'un système de vérification sur une base de données, on mesure des taux d'erreur sur cette base.

Taux de Fausses Acceptations FAR (False Acceptance Rate). Ce taux représente le pourcentage d'individus reconnus par le système biométrique alors qu'ils n'auraient pas dû l'être. Le système classe alors deux caractéristiques provenant de deux personnes différentes comme appartient à la même personne (indique la probabilité qu'un utilisateur soit reconnu comme quelqu'un d'autre) [4], [7].

$$FAR=\frac{nombre\ des\ imposteurs\ accepte}{nombre\ total\ d'accés\ imposteurs} \quad (Eq.\ 1.1)$$

Taux de Faux Rejets FRR (False Rejection Rate). Ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés. Personneme classe alors deux caractéristiques biométriques provenant de la même personne comme provenant de deux personnes différentes (indique la probabilité qu'un utilisateur connu soit rejeté) [7], [12].

$$FRR=\frac{nombre\ des\ clients\ rejetés}{nombre\ total\ d'accés\ clients} \quad (Eq.\ 1.2)$$

I.4.2. Les points de fonctionnement

Pour les applications, on doit fixer un seuil avec lequel on prend les décisions d'acceptation ou de rejet de l'utilisateur. Cela correspond donc à choisir un point de fonctionnement du système.

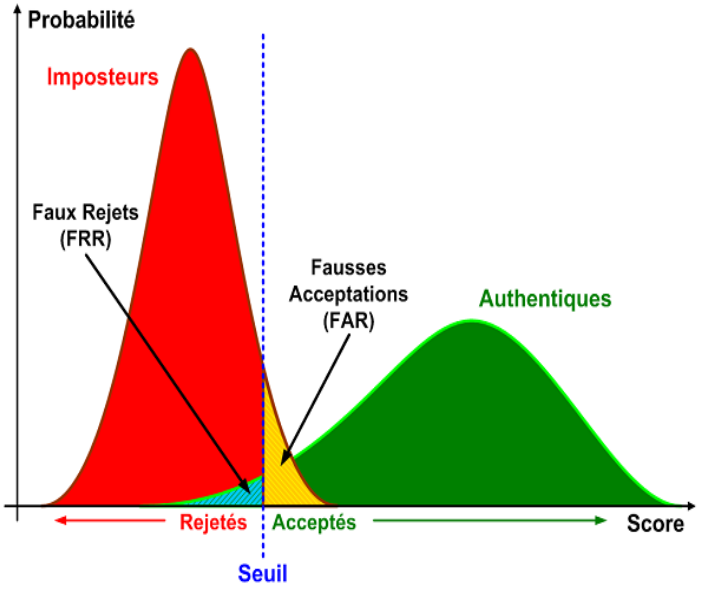

Figure 1. 6: Illustration du FRR et du FAR.

I.4.3. Les courbes de performance

Les courbes de performances permettent de représenter les performances pour toutes les valeurs du seuil sans fixer un seuil a priori. Par exemple on peut représenter l'évolution des deux taux d'erreurs (FAR et FRR) lorsque le seuil varie pour les distributions de scores Client et Imposteur représentés sur la (figure 1.7) *:*

Comme les taux d'erreurs FAR et FRR dépendent tous les deux du même seuil de décision, on peut également représenter sur une courbe la variation du FRR en fonction de

FAR lorsque le seuil varie.

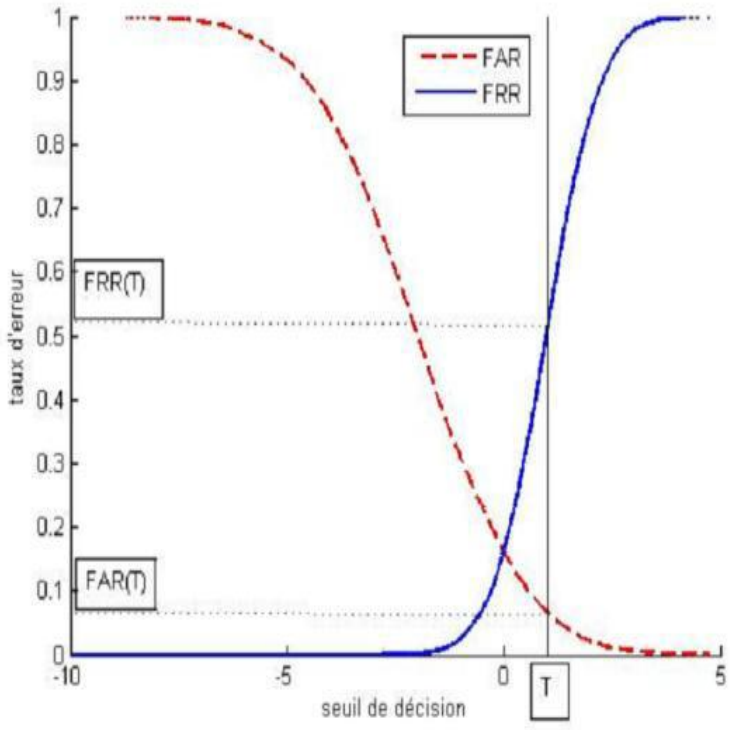

Figure 1. 7: Variation des taux de Faux Rejets (FRR) et taux de Fausses Acceptations (FAR du seuil de décision varie) en fonction.

Ces courbes s'appellent des courbes ROC (Receiver Operating Characteristic) représentées sur la (Figure 1.8).

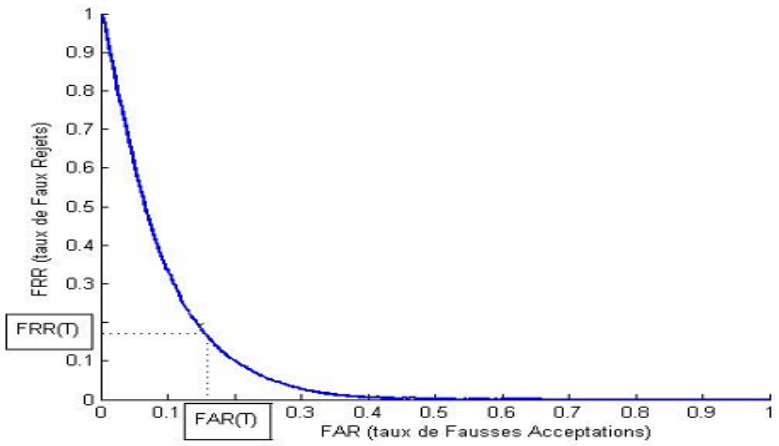

Figure 1. 8: La courbe ROC.

Ou des courbes DET (Detection Error Tradeoff) représentées sur la (*Figure 1.9)* lorsque les échelles pour les deux taux d'erreurs sont logarithmiques

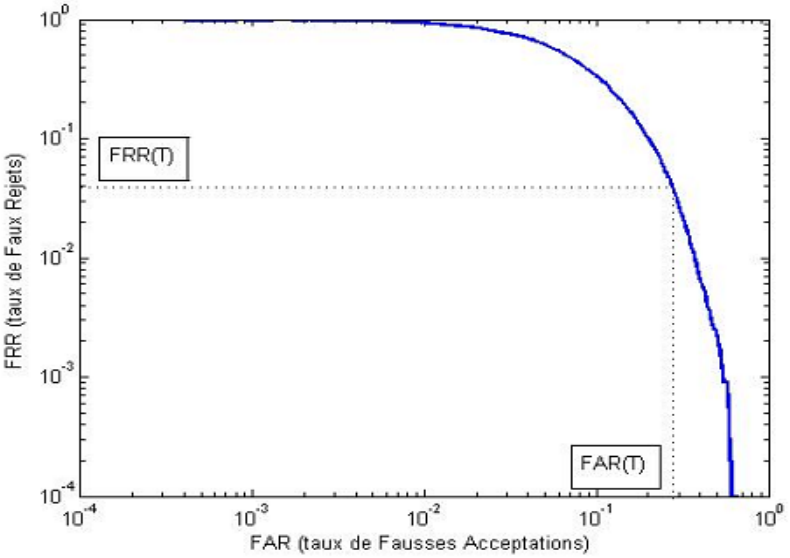

Figure 1. 9: Les courbes DET.

I.4.4. Les différents types de point de fonctionnement

Les 4 types de points de fonctionnement les plus utilisés sont :

EER : "Equal Error Rate" ou taux d'erreurs égales. Ce point de fonctionnement correspond au seuil qui donne des taux FAR et FRR égaux.

WER :"Weighted Error Rate" ou taux d'erreur pondéré. Ce point de fonctionnement correspond au seuil tel que le FRR est proportionnel au FAR avec un coefficient qui dépend de l'application. Le seuil du WER est égal au seuil de l'EER lorsque ce coefficient est égal à 1.

FAR fixé : Ce point de fonctionnement correspond au seuil tel que le taux FAR est égal à un taux fixé par l'application (par exemple 1% ou 0.1%).

La performance du système est donnée par le taux FRR pour cette valeur de FAR fixée.

I.4.5. Les points de fonctionnement sur les courbes de performance

Sur la Figure suivante sont représentés des exemples des quatre types de points de fonctionnement présentés ci-dessus. La (Figure 1.10*)* représente ces mêmes points de fonctionnement sur une courbe ROC.

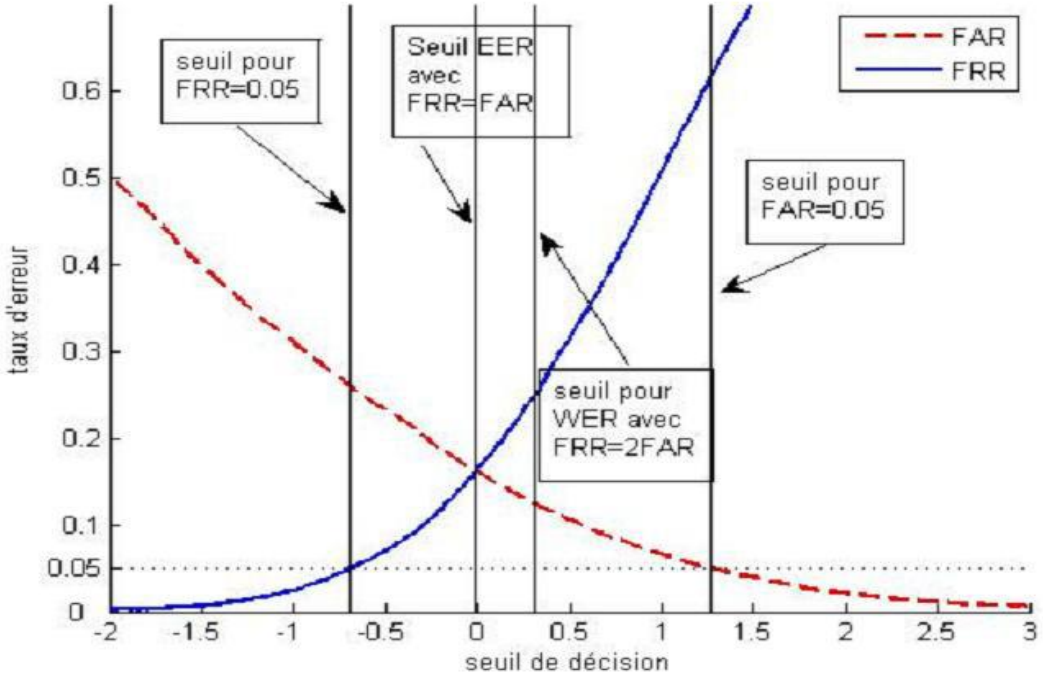

Figure 1. 10:Les points de fonctionnement représentés sur une courbe des taux d'erreurs en fonction du seuil de décision.

Le seuil du point EER (Equal Error Rate) correspond au seuil pour lequel les deux taux d'erreurs, FAR et FRR, sont égaux, il correspondant donc à l'intersection des deux courbes sur la (Figure 1.9*)*. Il correspond à l'intersection de la courbe avec la première bissectrice pour les courbes ROC ou DET comme représenté sur la (Figure 1.10*)*.

Sur les (Figures 1.10*)* et (*1.9)*, sont représentés le point WER tel que FRR = 2FAR et les points FAR = 0.05 et FRR = 0.05.

Sur la (Figure 1.8) (courbe ROC), le terme de point de fonctionnement prend tout son sens car il s'agit bien d'un point localisé sur la courbe et pour lequel on peut estimer les valeurs des taux d'erreurs, FAR et FRR.

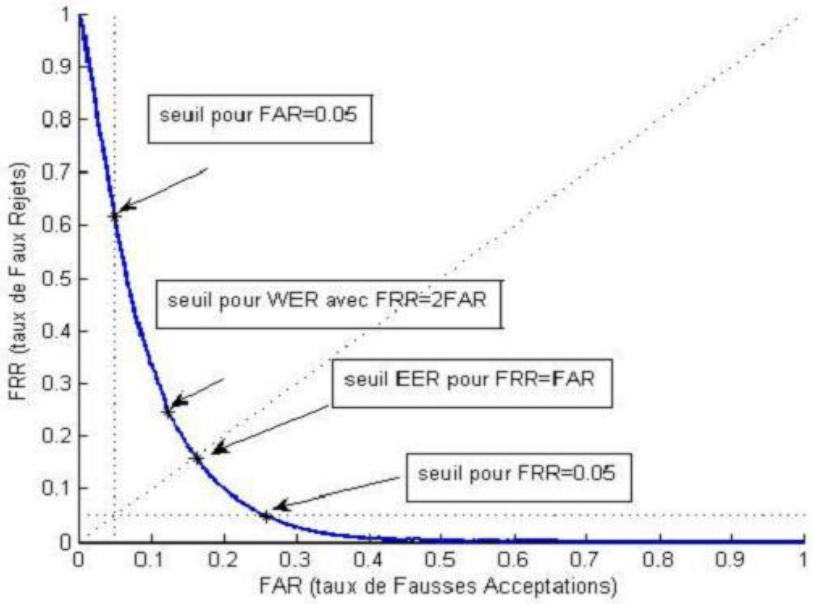

Figure 1. 11: Les points de fonctionnement représentés sur une courbe des taux d'erreurs en Fonction du seuil de décision.

Pour chacun de ces points on peut ensuite estimer plusieurs valeurs à partir des FAR et FRR. La valeur la plus classique est l'erreur moyenne aussi appelé HTER (Half Total Error Rate) qui correspond à la moyenne entre le FAR et le FRR : HTER= $\frac{FAR+FRR}{2}$ *(Eq. 1.3)*

Cette valeur de l'HTER est plutôt utilisée pour les points de fonctionnement associés à l'EER ou proches de l'EER où les deux taux d'erreurs sont du même.

Pour les points de fonctionnement associés au WER (Weighted Error Rate), il est logique d'utiliser une valeur globale d'erreur qui tienne compte de cette pondération.

On utilise alors le WTER (Weighted Total Error rate) tel que :

WTER = αFAR + (1 − α) FRR *(Eq. 1.4)*

Dans notre exemple précédent où l'on cherche le point de fonctionnement qui correspond à FRR = 2FAR, $\alpha = \frac{2}{3}$

Pour les deux autres points de fonctionnement qui correspondent à des valeurs fixées pour le FAR ou pour le FRR, dans ces deux cas on n'utilise pas de valeur globale du taux d'erreur mais la valeur du taux d'erreur non fixé. Par exemple pour le point correspondant à

FAR = 0.05 on lit sur la (*Figure 1.10)* que FRR = 0.61.

I.4.6. Quel point de fonctionnement pour quelle application

Le point de fonctionnement qui définit le choix du seuil dans le module de décision dépend de l'application visée. En général lorsqu'il n'y a pas d'application dénie mais qu'il s'agit d'un test de performance sur une base de données préenregistrée, on utilise le plus souvent l'EER (c'est-à-dire les deux taux d'erreurs égaux) car c'est un point de fonctionnement assez neutre qui ne favorise aucun des deux types d'erreurs. En revanche lorsqu'une application est dénie ou lorsque l'on connaît les objectifs de performance, on peut utiliser les autres points de fonctionnement et le plus souvent les points de fonctionnement correspondant à des niveaux fixés pour l'un des deux types d'erreurs.

Le compromis à faire pour le réglage du seuil de décision est le compromis entre confort et sécurité. Le confort correspond à un taux de Faux Rejets bas et la sécurité à un taux de Fausses Acceptations bas.

En général pour un besoin de sécurité on fixe FAR = 1% ou FAR = 0.1% selon le niveau de sécurité souhaité. Pour un besoin de confort on fixe FRR = 1% ou FRR = 0.1% en fonction du degré de confort souhaité.

Cependant, il est important de noter que le seuil de décision associé au point de fonctionnement choisi va être estimé sur une base de données, dite de développement, avec laquelle on règle les paramètres qui seront ensuite utilisés pour l'application en condition réelle. Le choix de cette base de données est primordial pour le bon réglage d'un système biométrique. Tout d'abord la base de données doit être représentative de l'application visée mas surtout elle doit être de taille sue sante. En particulier, pour estimer des seuils de décision pour des taux de FAR ou de FRR fixés et faibles (par exemple FAR = 0.1%), cela nécessite un grand nombre de données pour avoir de la précision dans des zones où il y a peu d'erreurs.

I.5. Conclusion

Dans ce chapitre, On a présenté la biométrie et le système biométrique de façon générale. Nous avons cité les caractéristiques, le domaine d'application et les différentes modalités puis on a détaillé pour le fonctionnement d'un système biométrique que ce soit pour la vérification et l'identification. Nous avons aussi présenté les différentes méthodes d'évaluation de performances d'un système biométrique, pour nous on doit utiliser les mesures FAR, FRR et EER,

II. Chapitre II : Généralités sur la reconnaissance faciale

II.6. Introduction

Ces dernières années, la demande croissante pour des systèmes automatisés d'identification des individus a mis en avant l'utilisation efficace et naturelle du visage à cette fin. Les images faciales sont largement adoptées comme méthode biométrique courante pour cette identification. Cependant, bien que les êtres humains puissent aisément reconnaître les visages, cette tâche s'avère être un défi considérable pour les systèmes informatiques. La reconnaissance des visages est devenue un domaine de recherche actif depuis la fin des années soixante-dix, motivée par sa diversité d'applications, telles que la surveillance dans les lieux publics [13].

Au fil des ans, diverses méthodes de reconnaissance faciale ont été développées, notamment basées sur des images fixes ou des séquences d'images (vidéo). Cependant, l'identification des individus à partir de leurs visages demeure une tâche complexe en vision numérique. Les systèmes de reconnaissance faciale visent à acquérir, traiter et interpréter les images pour réaliser cette tâche, offrant ainsi une surveillance discrète des espaces sans nécessiter la coopération des individus.

II.7. Reconnaissance faciale

Le développement des systèmes biométriques basés sur la reconnaissance faciale est relativement récent. En 1981, les chercheurs Hay et Young ont avancé que l'être humain, pour reconnaître un visage, utilise à la fois ses caractéristiques globales et locales. Des recherches plus poussées ont ensuite été menées pour déterminer si cette capacité de reconnaissance pouvait être reproduite de manière informatique.

C'est grâce aux travaux du professeur Teuvo Kohonen (1989), chercheur en réseaux neuronaux à l'Université d'Helsinki, et aux travaux de Kirby et Sirovich (1989) de l'Université Brown de Rhode Island, qu'un système de reconnaissance faciale appelé "EIGENFACE" a été développé par le MIT.

Ce système capture l'image du visage à l'aide d'une caméra. Le sujet peut se présenter volontairement devant celle-ci, ou son image peut être capturée à son insu pour en extraire certaines caractéristiques. En fonction du système utilisé, l'individu peut être soit positionné

devant l'appareil, soit en mouvement à une certaine distance. Les données biométriques ainsi obtenues sont ensuite comparées à une base de données de référence [14].

II.8. Pourquoi choisir le visage ?

La technologie de reconnaissance faciale, l'une des principales technologies biométriques, a joué un rôle de plus en plus crucial dans le domaine de la recherche, en raison des progrès rapides dans des domaines tels que la photographie numérique et Internet.

Malgré les critiques affirmant que la reconnaissance faciale est une forme de biométrie relativement peu fiable en raison de la sensibilité du signal acquis à des variations plus importantes que d'autres caractéristiques, telles que les changements d'éclairage, les variations de position du visage, la présence ou l'absence de lunettes, etc., plusieurs techniques de traitement d'images ont émergé ces dernières années. Parmi celles-ci, on trouve la détection faciale, la normalisation de l'éclairage, et autres. De plus, le développement significatif des technologies de caméra numérique atténue l'impact de ces problèmes.

La reconnaissance faciale présente plusieurs avantages par rapport à d'autres technologies biométriques : elle est naturelle, non intrusive et facile à utiliser. De plus, les capteurs utilisés sont peu coûteux (une simple caméra), faciles à installer et largement acceptés dans les lieux publics, ce qui permet d'accumuler des bases de données de plus en plus importantes et d'améliorer les performances de la reconnaissance. En revanche, pour les empreintes digitales et l'iris, le sujet doit être très proche du capteur et coopérer pour l'acquisition de l'image, sans oublier le coût élevé de l'équipement nécessaire à cette acquisition.

Classée en deuxième position dans l'industrie de la biométrie avec une part de marché de 15%, juste derrière les empreintes digitales, la reconnaissance faciale représente un compromis intéressant entre le coût et la précision [15].

II.9. Principales difficultés de la reconnaissance de visage

Pour le cerveau humain, la reconnaissance faciale est une tâche visuelle complexe. Bien que les humains puissent détecter et identifier des visages dans une scène avec facilité, créer un système automatique capable d'accomplir ces tâches représente un défi considérable. Ce défi est d'autant plus important lorsque les conditions de capture des images sont très variables. Deux types de variations sont associés aux images de visages : inter et intra sujet. La variation

inter-sujette est limitée en raison de la similitude physique entre les individus. En revanche, la variation intra-sujet est plus étendue et peut être attribuée à plusieurs facteurs, que nous analysons ci-dessous [16].

II.9.1. Changement d'illumination

L'aspect d'un visage dans une image subit d'importantes variations en fonction de l'éclairage de la scène lors de la capture (voir figure 2.1). Ces fluctuations de luminosité compliquent considérablement la tâche de reconnaissance faciale. En effet, les altérations de l'apparence dues à l'éclairage peuvent parfois être plus problématiques que les différences physiques entre les individus, ce qui peut conduire à une mauvaise classification des images. Cet aspect a été confirmé expérimentalement dans l'étude d'adini et al, où une base de données de 25 individus a été utilisée. L'identification des visages dans des environnements non contrôlés demeure donc un domaine de recherche ouvert. Les évaluations FRVT ont révélé que la variabilité de l'éclairage constitue un défi majeur pour la reconnaissance faciale.

Figure 2. 1: Les étapes de la reconnaissance de visage[16].

II.9.2. Variation de pose

Le niveau de reconnaissance faciale diminue considérablement en présence de variations de pose dans les images. Cette problématique a été confirmée par des évaluations menées sur les bases de données FERET et FRVT. Les variations de pose sont reconnues comme un obstacle majeur pour les systèmes de connaissance faciale. Lorsque le visage est vu de côté par rapport au plan de l'image (avec une orientation inférieure à 30°), il est possible de normaliser sa posture en identifiant au moins deux caractéristiques faciales (passant par les yeux). Cependant, au-delà d'une rotation de 30°, la normalisation géométrique devient impossible (voir figure 2.2).

Figure 2. 2: Exemple de variation d'éclairage[16].

II.9.3. Expressions faciales

Un autre élément qui influe sur l'apparence du visage est l'expression faciale (voir figure 2.3). Les déformations du visage dues aux expressions faciales se concentrent principalement sur la partie inférieure du visage. Les caractéristiques faciales situées dans la partie supérieure restent généralement constantes. Elles suffisent généralement pour une identification. Cependant, puisque l'expression faciale altère l'apparence du visage, elle entraîne inévitablement une baisse du taux de reconnaissance. L'identification des visages avec expression faciale demeure un défi non résolu et d'actualité. L'information temporelle offre une connaissance supplémentaire significative pouvant contribuer à résoudre ce problème.

Figure 2. 3: Exemples de variation d'expressions[16].

II.9.4. Présence ou absence des composants structurels

La présence des éléments structurels comme la barbe, la moustache, ou encore les lunettes peut considérablement altérer les caractéristiques faciales telles que la forme, la couleur ou la taille du visage. De plus, ces éléments peuvent dissimuler les traits faciaux fondamentaux, entraînant ainsi un échec du système de reconnaissance. Par exemple, des lunettes opaques peuvent rendre difficile la distinction de la forme et de la couleur des yeux, tandis qu'une moustache ou une barbe peut modifier la forme du visage.

II.9.5. Occultations partielles

Les visages peuvent être partiellement cachés par des objets dans l'environnement ou par le port d'accessoires tels que des lunettes, des écharpes, etc. Dans le cadre de la biométrie, il est crucial que les systèmes proposés soient non intrusifs, c'est-à-dire qu'ils ne nécessitent pas la coopération active des sujets. Par conséquent, il devient essentiel de pouvoir identifier les visages même lorsqu'ils sont partiellement masqués. Gross et ses collègues ont examiné comment le port de lunettes de soleil ou d'un cache-nez, qui dissimule la partie inférieure du visage, affecte la reconnaissance faciale. Leur étude a utilisé la base de données AR. Leurs résultats expérimentaux suggèrent que, dans de telles circonstances, les performances des algorithmes de reconnaissance demeurent limitées.

II.10. Système de reconnaissance de visage

Le processus de reconnaissance faciale implique la capture, le traitement, l'analyse et la comparaison du visage avec une base de données d'images enregistrées. Ce système identifie 80 points nodaux sur le visage humain pour mesurer différentes variables faciales telles que la longueur et la largeur du nez, la profondeur de l'œil et la structure osseuse du visage. Habituellement, les différentes phases de la reconnaissance faciale sont présentées dans la figure 2.4 [17].

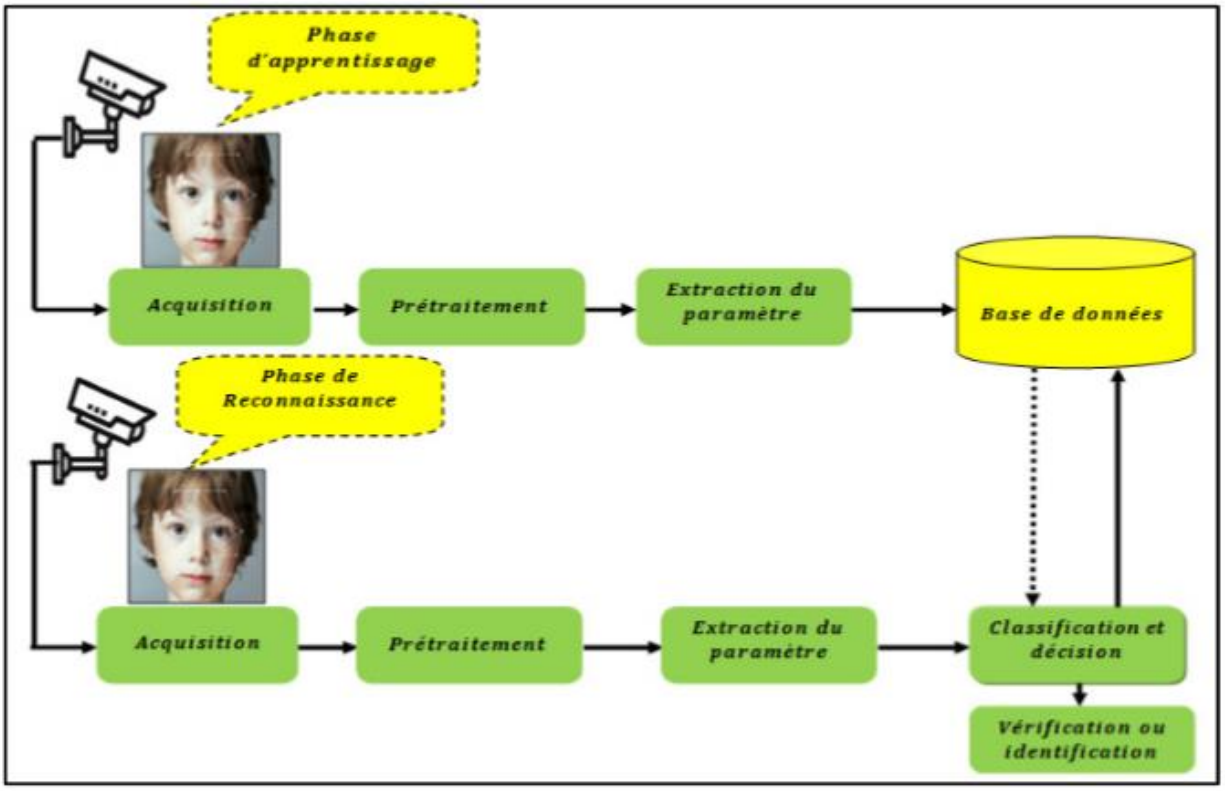

Figure 2. 4: Architecture d'un système de reconnaissance de visage[17].

Chaque système de reconnaissance de visage comporte deux phases d'exécution, l'un pour l'apprentissage et l'autre pour la reconnaissance

a. Phase d'apprentissage (d'enrôlement)

Une étape du processus consiste à enregistrer les informations biométriques des individus identifiés dans le système. Un capteur biométrique est utilisé pour capturer l'échantillon biométrique d'une personne, qui est ensuite traité pour extraire ses caractéristiques. Ces caractéristiques sont converties en une représentation numérique qui constitue le modèle de l'individu. Ce modèle est ensuite stocké dans la base de données pour permettre l'identification ultérieure.

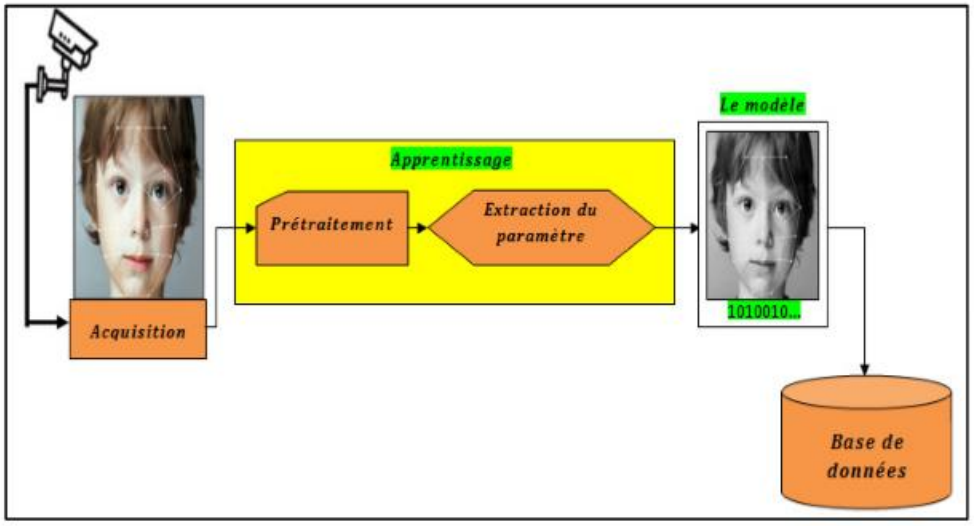

Figure 2. 5: Phase d'apprentissage[17].

b. Phase de reconnaissance(Test)

Pour déterminer l'identité de l'utilisateur pour l'un d'eux Identification ou vérification (authentification) :

Mode de vérification (d'authentification) : Le système doit répondre à une question de type "Êtes-vous la personne qui prétend être ?" Pour cela, il nécessite qu'un utilisateur réclame une identité avant qu'une comparaison biométrique ne soit effectuée. L'utilisateur peut revendiquer son identité en utilisant un nom d'utilisateur, un prénom ou un numéro d'identification personnelle. Ensuite, le système doit vérifier si l'identité revendiquée correspond à celle enregistrée dans la base de données en réalisant une comparaison avec un seul des modèles présents dans la base de données (1:1). La réponse renvoyée par le système peut être soit "identique", soit "non-identique".

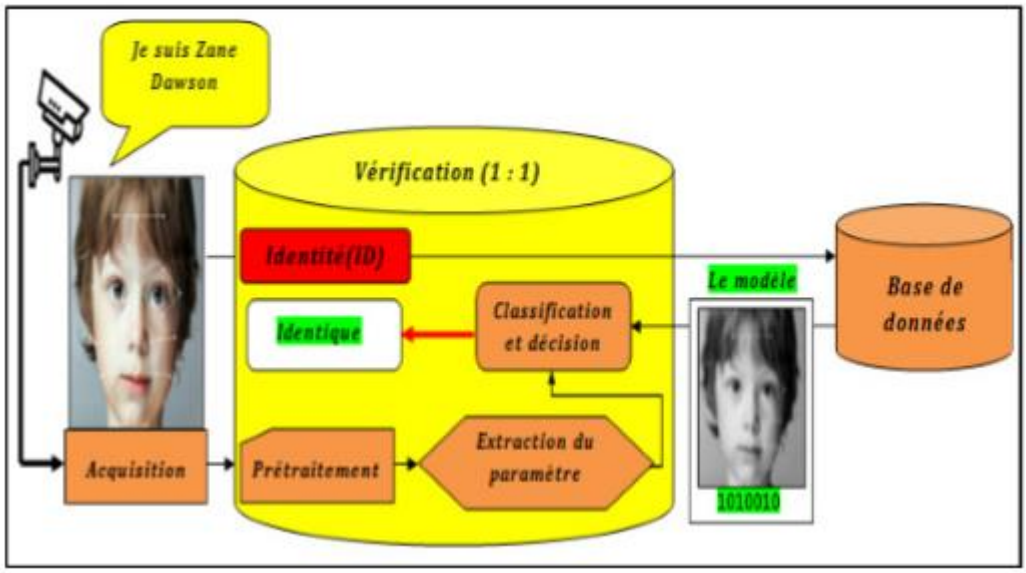

Figure 2. 6: Phase de reconnaissance : le mode de vérification [17].

Mode d'identification : Le système cherche à déterminer l'identité d'une personne à partir d'une base de données, sans nécessiter qu'un utilisateur réclame une identité avant les comparaisons biométriques. Il s'agit d'une comparaison de type un avec plusieurs (1 : N), où le système biométrique répond à la question "Vous êtes dans ma base de données, qui êtes-vous ?" La réponse retournée par le système est une identité.

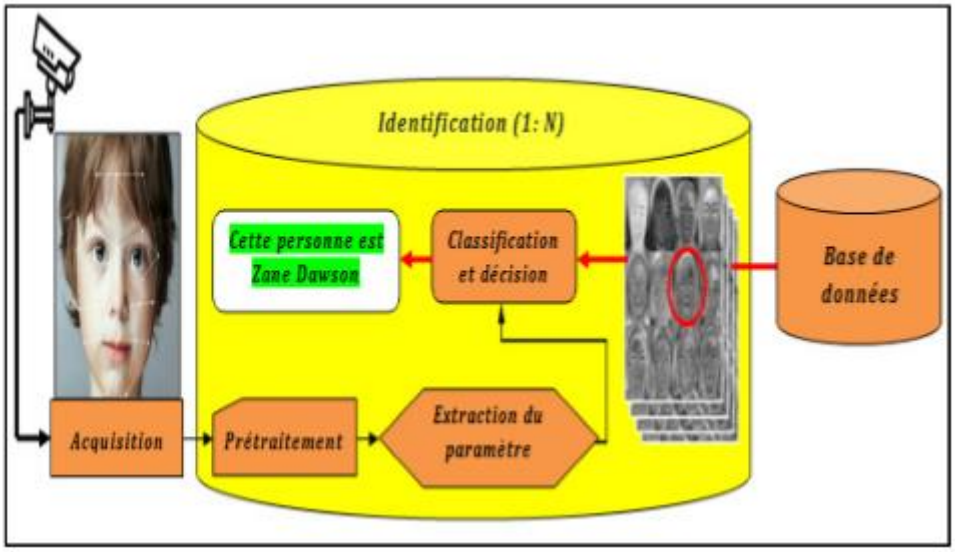

Figure 2. 7: Phase de reconnaissance : le mode d'identification[17].

II.11. Le fonctionnement de la reconnaissance de visage

La reconnaissance automatique des visages est confrontée à une multitude de défis, car le visage est une structure dynamique sujette à des variations constantes, influencées par divers facteurs. L'objectif fondamental d'un système de reconnaissance faciale est de déterminer la classe à laquelle appartient un visage inconnu. La figure 2.8 présente de manière graphique la méthodologie générale utilisée pour concevoir de tels systèmes [18].

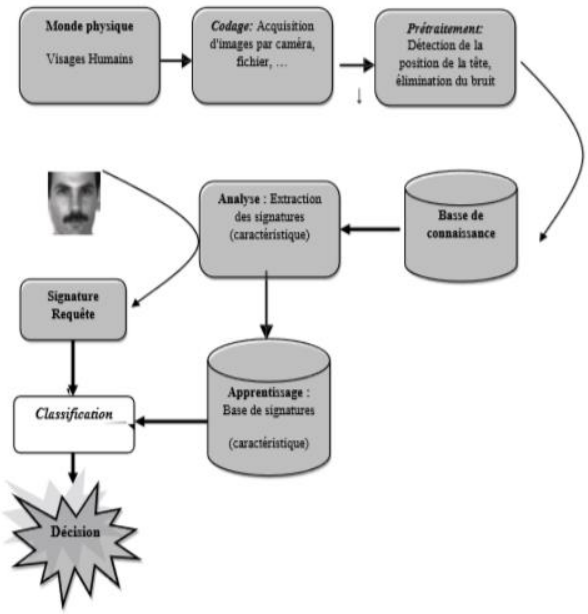

Figure 2. 8: Système de reconnaissance de visage[18].

II.11.1. Acquisition

Un système d'acquisition doté d'un capteur est employé pour obtenir une caractéristique spécifique de l'utilisateur, tel qu'un microphone pour la voix. Cette étape consiste à extraire d'éléments du monde réel une représentation bidimensionnelle pour des objets en 3D. Cette opération peut être statique (par exemple, un appareil photo, un scanner, etc.) ou dynamique (caméra, webcam), où une séquence vidéo est capturée, donnant ainsi une image brute (voir la figure 2.9).

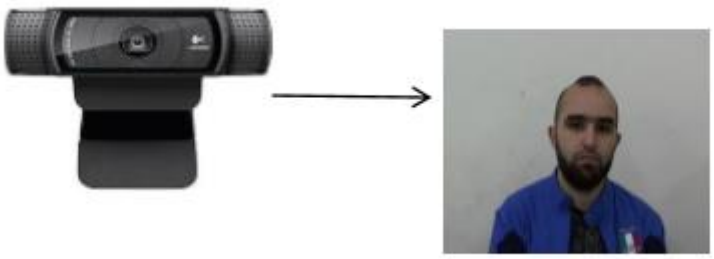

Figure 2. 9: Exemple d'acquisition d'une image[18].

II.11.2. Détection de visage

L'efficacité des systèmes biométriques basés sur l'authentification faciale repose principalement sur la méthode utilisée pour localiser le visage dans l'image. Dans la littérature scientifique, ce problème est souvent désigné sous le terme de "détection de visages" (voir la figure 2.10). De nombreuses recherches ont été menées dans ce domaine, conduisant au développement de diverses techniques, de la simple détection du visage à la localisation précise des régions caractéristiques telles que les yeux, le nez, les narines, les sourcils, la bouche, les lèvres, les oreilles, etc.

Figure 2. 10:Détection de visage[18].

II.11.3. Prétraitement

Les données biométriques sont traitées pour éliminer le bruit causé par l'environnement ou le dispositif de capture. Ce processus nécessite l'application de techniques de traitement et de restauration d'images pour éliminer le bruit. Ensuite, une détection de visages est effectuée, une opération qui peut être très complexe, surtout lorsque l'image contient plusieurs visages ou lorsque l'arrière-plan n'est pas neutre.

II.11.4. Extraction

Parfois appelée indexation, représentation ou modélisation, cette étape implique l'utilisation d'une image ou d'un enregistrement vocal en entrée. La segmentation est alors effectuée pour extraire les caractéristiques nécessaires au processus d'authentification. Par exemple, cela peut consister à isoler le visage du fond d'une image lors d'une identification faciale. L'objectif est d'extraire les informations pertinentes contenues dans le signal capturé. Le choix de ces informations pertinentes revient à établir un modèle pour le visage, qui doit être à la fois distinctif et non redondant.

II.11.5. Classification

Lors de l'examen des modèles stockés dans la base de données, le système sélectionne un ensemble de modèles qui présentent une similarité maximale avec celui de la personne à identifier, formant ainsi une liste restreinte de candidats. Ce processus de classification intervient uniquement dans le cas de l'identification, car dans le cas de l'authentification, seul un modèle est retenu (celui de la personne prétendue).

II.11.6. Apprentissage

En général, notre approche repose sur l'apprentissage d'une distance entre les visages. Nous disposons d'un ensemble de paires d'images de visages, certaines représentant des individus différents, d'autres montrant la même personne mais avec des variations d'expression, de pose ou d'éclairage. Pour chaque paire, nous avons des annotations indiquant si les visages appartiennent à la même personne ou non. Notre méthode de calcul de similarité comprend quatre grandes étapes :

Chaque visage est représenté par un vecteur d'attributs.

Nous appliquons une méthode de réduction de dimensionnalité. Tout en créant un espace de représentation qui distingue au mieux les données positives des données négatives (paires de visages identiques ou différents).

Nous effectuons un apprentissage semi-supervisé où les données de test (dont les étiquettes ne sont pas connues) sont utilisées pour affiner la structure des données dans l'espace de représentation. Cette phase repose sur la construction d'un graphe où les nœuds représentent les paires de visages et les arêtes représentent les relations entre ces paires.

Nous formons un classifieur qui combine les informations extraites des deux méthodes précédentes pour évaluer la similarité entre deux visages inconnus. Cela implique de mémoriser les représentations calculées lors de la phase d'analyse pour les individus connus. Généralement, les étapes d'analyse et d'apprentissage sont combinées en une seule phase (voir la figure 2.11).

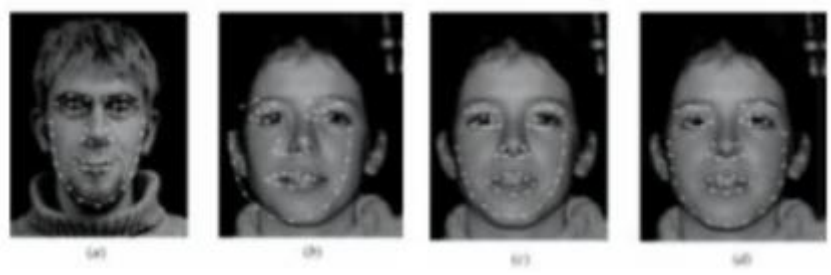

Figure 2. 11: Exemple d'image d'apprentissage[18].

II.11.7. Décision

Dans le cadre de l'identification, il consiste à examiner les modèles sélectionnés par un agent humain et à prendre une décision en conséquence. Quant à l'authentification, la stratégie de décision nous permet de choisir entre deux alternatives : soit l'identité de l'utilisateur correspond à celle proclamée ou recherchée, soit elle ne correspond pas. C'est dans ce module que le système émet sa réponse, soit en identifiant la personne la plus proche dans la base de données, soit en effectuant une vérification (oui ou non). Pour évaluer la différence entre deux images, il est nécessaire d'introduire une mesure de similarité. Il convient de souligner que le système de vérification automatique des visages repose entièrement sur la méthode de localisation. [19]

II.12. Avantages et inconvénients de la reconnaissance de visage

Les avantages et inconvénients des méthodes de reconnaissance de visage sont récapitulés par le tableau 2.1 :

Tableau 2. 1: Avantages et inconvénients de la reconnaissance du visage.

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

II.13. Conclusion

La reconnaissance faciale émerge comme l'une des technologies biométriques les plus en vogue, aux côtés du balayage de l'iris et de l'empreinte digitale. Ses applications en constante évolution se déploient dans divers secteurs tels que la santé, la sécurité, la défense, la médecine légale et les transports, exigeant une précision accrue. Toutefois, plusieurs défis persistent lors du développement de ces technologies, notamment la gestion des différentes poses, variations d'éclairage, expressions faciales, ainsi que la présence ou l'absence de composants structuraux. Ces défis occupent actuellement une place importante dans la recherche, en espérant trouver des solutions innovantes qui ouvriront de nouvelles perspectives.

III. Chapitre III : Les algorithmes de reconnaissance faciale

III.1. Introduction :

Dans ce chapitre, nous explorerons les étapes essentielles de la reconnaissance faciale, en mettant l'accent sur le prétraitement des images, l'extraction des caractéristiques et les méthodes de classification. Nous commencerons par discuter de l'importance du prétraitement pour améliorer la qualité des données et réduire les variations indésirables. Ensuite, nous examinerons les techniques d'extraction des caractéristiques, en mettant en lumière l'approche des eigenfaces qui utilise l'Analyse en Composantes Principales (PCA). Nous aborderons ensuite les algorithmes de classification tels que la Machine à Vecteurs de Support (SVM) et les K plus proches voisins (KNN) pour identifier les visages dans les images. Enfin, nous discuterons des techniques de réduction de dimensionnalité comme l'Analyse Discriminante Linéaire (LDA) et l'Analyse en Composantes Principales (PCA), qui permettent une meilleure représentation des données et une classification plus précise des visages. En combinant ces différentes méthodes, nous serons en mesure de construire des systèmes de reconnaissance faciale efficaces et précis.

III.2. Les étapes générales d'un algorithme de reconnaissance faciale

La vue d'ensemble du système de reconnaissance des expressions faciales est illustrée dans la figure 1. Ce système comprend les étapes principales telles que le prétraitement des images de visage, l'extraction des caractéristiques et la classification.

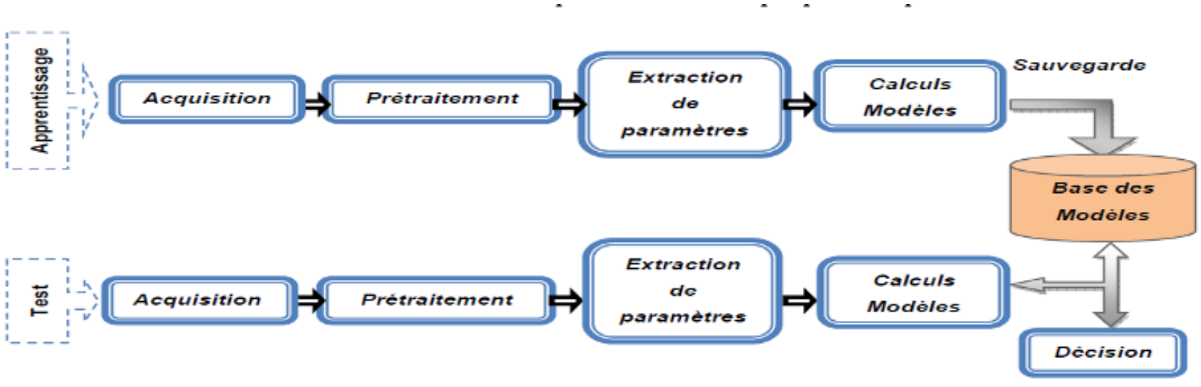

Figure 3. 1: Architecture du système de reconnaissance faciale.[11]

III.3. Prétraitement

Le prétraitement constitue une étape cruciale dans les systèmes biométriques axés sur la reconnaissance faciale, car il joue un rôle déterminant dans l'efficacité du processus d'identification. La localisation du visage dans l'image, également appelée détection faciale, est un aspect essentiel de cette phase. De nombreuses recherches ont été menées dans ce domaine, aboutissant au développement de diverses techniques allant de la simple détection faciale à la localisation précise des différentes parties du visage telles que les yeux, le nez, les sourcils, la bouche, les lèvres, les oreilles, etc.

Cependant, les solutions existantes présentent des limitations car elles ne fonctionnent généralement bien que dans des environnements contrôlés. Elles ne sont donc pas adaptées à la variabilité des conditions de capture dans la vie quotidienne, notamment [20] :

La pose : Les images de visages peuvent varier en fonction de l'orientation du visage.

La présence ou l'absence de composants structuraux : Des éléments tels que la barbe, la moustache et les lunettes peuvent introduire une grande variabilité dans les caractéristiques faciales, affectant la forme, la couleur et la taille des composants structuraux du visage.

Les occultations : Les visages peuvent être partiellement masqués par d'autres objets dans une image, par exemple dans une photo de groupe où certains visages peuvent être partiellement cachés par d'autres.

Les conditions d'éclairage : Les conditions d'éclairage, telles que la distribution de la source de lumière, son intensité et son spectre, ainsi que les caractéristiques de l'appareil photographique, peuvent influencer l'apparence d'un visage dans une image capturée.

Ces facteurs de variabilité rendent la détection et la localisation des visages dans les images plus complexes et nécessitent le développement de techniques robustes capables de relever ces défis pour obtenir des performances satisfaisantes dans diverses conditions de capture.

III.4. L’extraction des caractéristiques

L'étape d'extraction des caractéristiques vise à identifier les traits distinctifs du visage qui le rendent à la fois unique par rapport à celui d'autres personnes et robuste face aux variations propres à la personne elle-même. Ces caractéristiques sont essentielles pour que le

visage d'une personne ne soit pas confondu avec celui d'une autre tout en conservant sa propre identité dans différentes conditions d'acquisition.

Au début des recherches sur la reconnaissance faciale, on considérait qu'une représentation du visage devait nécessairement prendre en compte des éléments tels que la bouche, les yeux, le nez et leur géométrie relative. Cependant, cette approche s'est avérée limitée. Une analyse plus approfondie du visage était alors nécessaire pour identifier d'autres caractéristiques pertinentes. Dans certaines méthodes, seule la détection des yeux est utilisée pour normaliser le visage, après quoi une analyse globale du visage est effectuée.

Dans l'outil FaceSDK [21] il existe 70 caractéristiques du visage que plusieurs auteurs ont utilisé dans leurs travaux, la figure suivante illustre les 70 caractéristiques du visage.

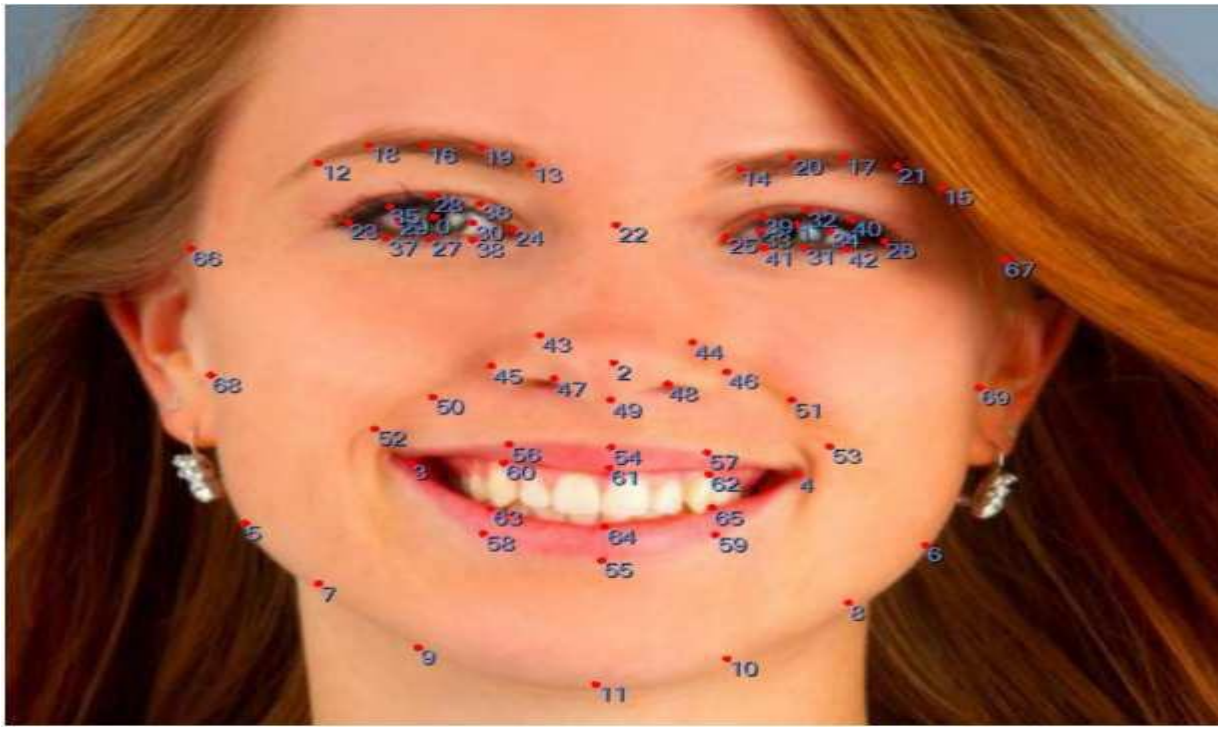

Figure 3. 2: Les 70 points d'intérêt du visage de FaceSDK [21] .

III.4.1. Local Binary Patterns (LBP) [22]

C'est une technique utilisée pour décrire la texture ou les motifs dans une image. Par exemple, prenons une empreinte digitale qui capture les caractéristiques uniques de différentes textures comme les surfaces rugueuses, lisses et texturées

Pour comprendre LBP, imaginez regarder une image en niveaux de gris pixel par pixel. Pour chaque pixel, nous examinons son voisinage, qui se compose du pixel lui-même et de ses pixels environnants. Pour créer le code LBP d'un pixel, nous comparons la valeur d'intensité de ce

pixel avec les valeurs d'intensité de ses voisins. Nous attribuons une valeur de 1 si l'intensité d'un voisin est égale ou supérieure à l'intensité du pixel central, et une valeur de 0 si elle est inférieure.

En partant d'un pixel de référence, nous parcourons le voisinage dans le sens des aiguilles d'une montre ou dans le sens contraire des aiguilles d'une montre. À chaque étape, nous comparons l'intensité du voisin actuel avec l'intensité du pixel central et attribuons un 1 ou un 0 en conséquence. Une fois les comparaisons terminées pour tous les voisins, nous obtenons une séquence de 1 et de 0. Cette séquence est le code LBP pour le pixel central. Il représente le motif de texture dans ce voisinage. En répétant ce processus pour chaque pixel de l'image, nous générons une représentation LBP complète de l'image. Nous pouvons ensuite utiliser cette représentation pour décrire et analyser les propriétés de texture de l'image.

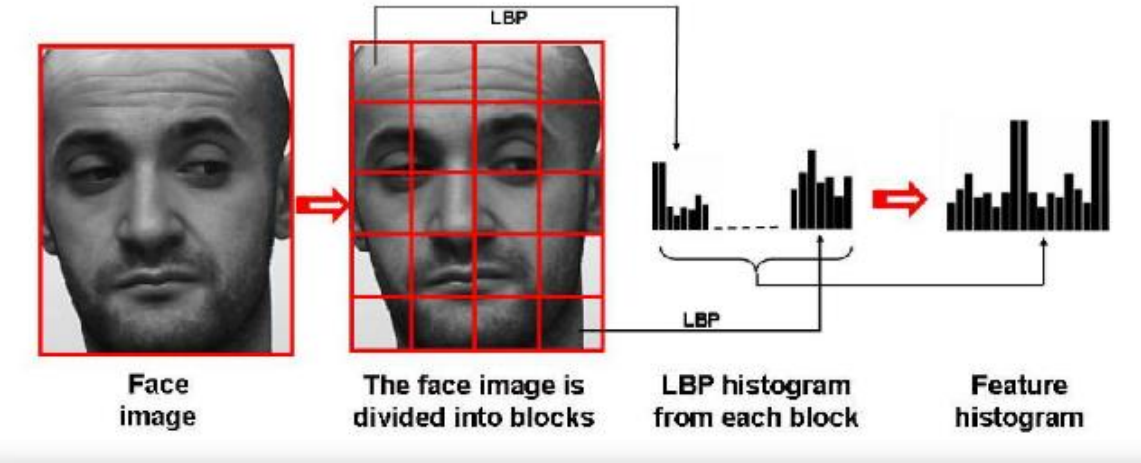

Figure 3. 3: Local Binary Patterns (LBP).[22]

III.4.2. Local Phase Quantization (LPQ) [23]

C'est une méthode de traitement d'images qui vise à capturer les informations de phase locale dans une image. Contrairement à LBP qui se concentre sur les variations d'intensité des pixels, LPQ se concentre sur les variations de phase des coefficients de Fourier locaux.

Transformée de Fourier locale : Tout d'abord, une région locale de l'image est extraite. Cette région est généralement définie par une fenêtre de taille fixe. Ensuite, la transformée de Fourier est appliquée à cette région pour convertir l'information spatiale en information fréquentielle. La transformée de Fourier permet de décomposer l'image en ses composantes de fréquence.

Quantification de la phase : Une fois la transformée de Fourier appliquée, la phase de chaque coefficient de Fourier est calculée. La phase représente la composante de l'information de l'image qui encode la variation de forme ou de texture. Ensuite, la phase de chaque coefficient est comparée à la phase des coefficients voisins dans la région locale. Cette comparaison permet de quantifier la phase en attribuant des valeurs discrètes en fonction des différences de phase.

Création des codes LPQ : Les valeurs discrètes obtenues par la quantification de la phase sont utilisées pour former des codes LPQ. Ces codes sont généralement des séquences de bits qui représentent les motifs de phase locaux dans l'image.

Utilisation des codes LPQ : Une fois les codes LPQ générés pour toute l'image, ils peuvent être utilisés pour décrire et analyser les structures et les motifs présents dans l'image. Comme les codes LBP, les codes LPQ sont robustes et peuvent être utilisés dans diverses applications telles que la reconnaissance d'objets, la détection de texture, la classification d'images, etc.

LPQ présente l'avantage d'être robuste aux variations d'éclairage et de contraste dans l'image, ce qui en fait une technique populaire pour l'analyse des textures et des motifs dans des conditions d'éclairage variables.

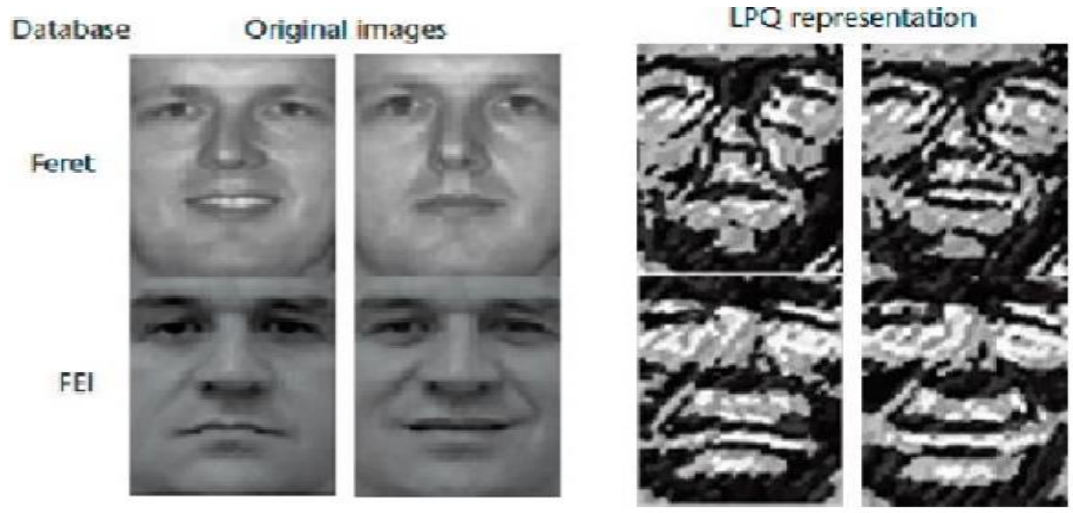

Figure 3. 4: Local Phase Quantization (LPQ).[23]

III.4.3. : Binarized Statistical Image Features (BSIF) [24]

C’est une autre méthode de traitement d'images utilisée pour extraire des caractéristiques locales robustes à partir d'images. Tout comme LBP et LPQ, le BSIF est utilisé pour la description de texture et la reconnaissance d'objets.

Voici un aperçu de la technique BSIF :

Filtrage par des filtres binaires : Le BSIF utilise un ensemble de filtres binaires pour extraire des caractéristiques locales à partir de l'image. Ces filtres sont conçus pour capturer des informations sur les textures et les structures locales de l'image.

Réponse à l'image filtrée : Chaque filtre binaire est appliqué à l'image d'entrée, produisant une réponse pour chaque pixel de l'image. Cette réponse est généralement calculée en effectuant une opération de corrélation ou de convolution entre le filtre et l'image.

Binarisation : La réponse de chaque filtre est ensuite binarisée en attribuant une valeur de 1 si la réponse dépasse un seuil prédéfini, et une valeur de 0 sinon. Cette binarisation permet de créer des motifs binaires qui capturent les informations de texture locales.

Formation de caractéristiques : Les motifs binaires obtenus à partir de chaque filtre sont concaténés pour former un vecteur de caractéristiques pour chaque pixel de l'image. Ces vecteurs de caractéristiques sont utilisés pour décrire la texture de l'image.

Utilisation des caractéristiques : Une fois les caractéristiques extraites, elles peuvent être utilisées dans différentes tâches de traitement d'images telles que la reconnaissance d'objets, la classification d'images, la détection de texture, etc.

Le BSIF est particulièrement utile dans les scénarios où la robustesse aux variations d'éclairage et de contraste est importante, tout en fournissant une représentation compacte et discriminante des textures dans l'image. Il est largement utilisé dans divers domaines, y compris la vision par ordinateur, la surveillance, la reconnaissance de formes, etc.

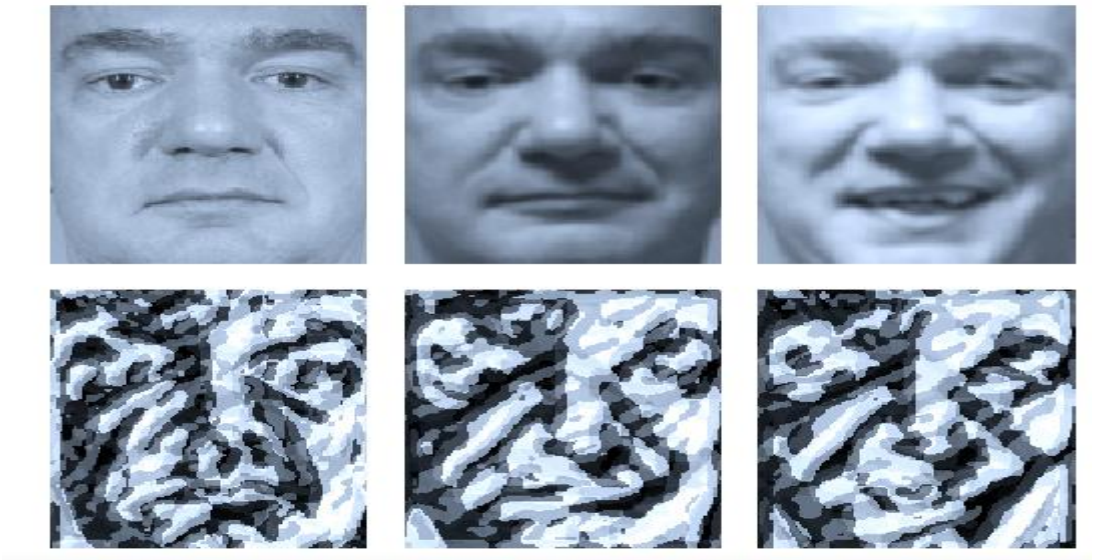

Figure 3. 5: Binary Robust Independent Elementary Features (BSIF). [24]

III.5. Les algorithmes de classification

L'algorithme de classification fait partie des méthodes d'apprentissage supervisé. C'est-à-dire que les prédictions sont réalisées à partir de données historiques. À l'inverse de l'apprentissage non supervisé où il n'y a pas de classes prédéfinies.

III.5.1. Machine à vecteurs de support (SVM)

La Machine à Vecteurs de Support (SVM) appartient à l'apprentissage supervisé et est un algorithme qui peut à la fois réaliser la classification et la régression [25]. Son principe est de trouver un hyperplan à marge maximale. L'hyperplan à marge maximale divise deux classes en deux parties avec la distance maximale aux données les plus proches. Si nous fournissons suffisamment de données pour créer un modèle SVM, la prédiction de nouvelles données sera très précise. Cependant, étant donné que la Machine à Vecteurs de Support convient uniquement à la classification binaire, si nous voulons réaliser une classification multi-classe, nous devons construire n*(n-1)/2 machines à vecteurs et les combiner ensemble. Enfin, grâce à un vote un à un, nous trouvons la classe des données.

Dans le domaine de la reconnaissance faciale, après le processus de réduction de dimensionnalité, nous mettons les eigenfaces dans le modèle SVM pour l'entraîner. Ensuite, ce classificateur nous donnera la réponse à qui est cette personne sur l'image. Cependant, que ce soit les eigenfaces ou le modèle SVM, ils ont tous des inconvénients. Les prédictions des eigenfaces auront des différences significatives si les images ont seulement des différences d'éclairage et le modèle SVM ne prend en charge que de petites quantités de données. Si nous voulons réaliser la reconnaissance faciale basée sur de grandes données, le calcul du SVM nécessite un grand temps. [25]

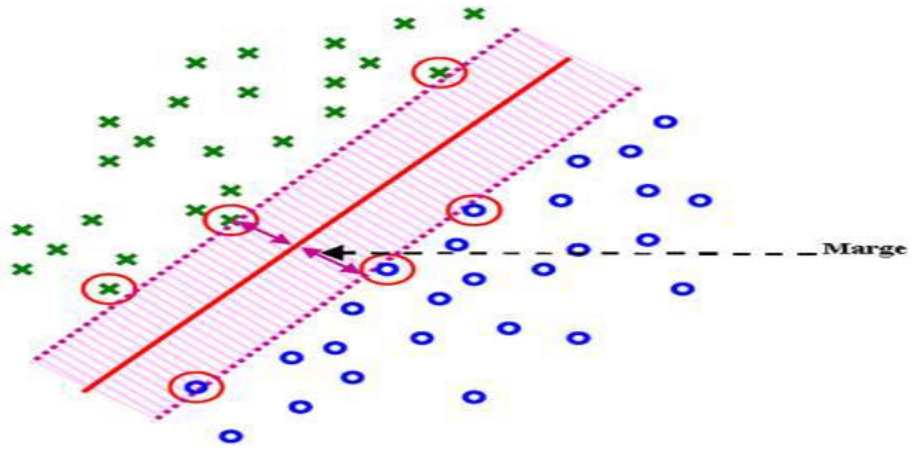

Figure 3. 6: Exemple de deux classes linéairement séparables. L'hyperplan déterminé par la SVM, maximisant la marge, permet de séparer les deux classes de manière optimale.

- **Avantage des machines vectorielles du support**

L'algorithme SVM demeure efficace dans les espaces de grande dimension. Il conserve son efficacité même lorsque le nombre de dimensions dépasse celui des échantillons. En outre, il exploite un sous-ensemble des points d'apprentissage dans la fonction de décision, ce qui le rend également efficace en termes de consommation de mémoire.

- **Inconvénients des machines vectorielles du support**

Les SVM ne produisent pas directement d'estimations de probabilité. Pour obtenir ces estimations, une étape de validation est nécessaire.

III.5.2. K plus proches voisins (KNN)

L'algorithme des K plus proches voisins (KNN) est largement reconnu comme l'un des algorithmes de classification les plus simples et les plus couramment utilisés. Bien qu'il soit considéré comme un algorithme d'apprentissage paresseux, sa simplicité et sa capacité à s'adapter à diverses situations en font un choix populaire.

KNN est non paramétrique, ce qui signifie qu'il ne fait aucune hypothèse sur la distribution des données. Au lieu de cela, il se base sur la similarité des caractéristiques pour classer de nouveaux points de données en se référant à des données d'entraînement existantes.

Dans le contexte de la reconnaissance faciale, KNN se révèle être un outil puissant en raison de sa capacité à apprendre à partir des données d'entraînement et à classifier précisément de

nouvelles instances. Sa flexibilité permet une personnalisation aisée et un ajustement des paramètres pour répondre aux besoins spécifiques des applications. De plus, sa robustesse au bruit et sa capacité à gérer de grandes quantités de données en font un choix pertinent pour les applications réelles en reconnaissance faciale [26].

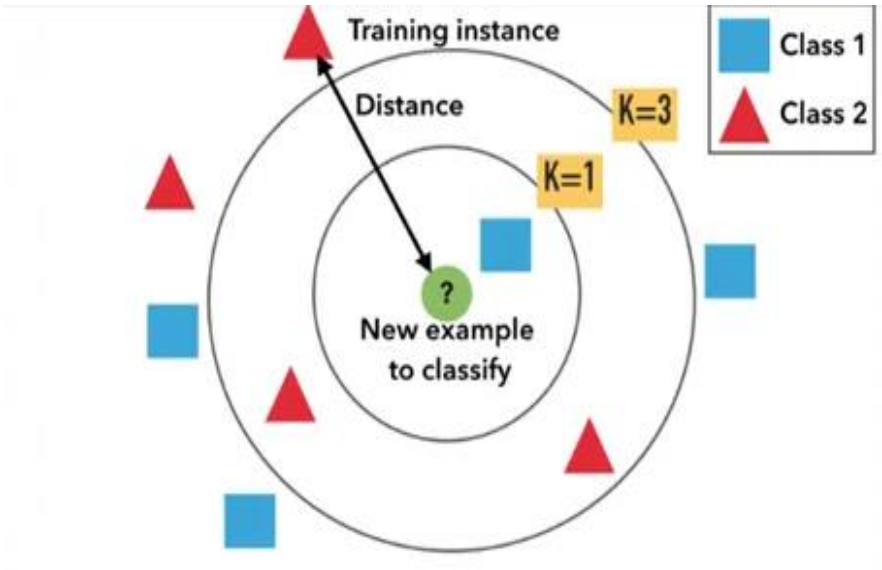

Figure 3. 7: Exemple de classification KNN.

III.6. Les algorithmes de réduction

Un algorithme de réduction est un algorithme permettant de simplifier un problème en transformant une instance de celui-ci en une nouvelle instance de plus petite taille.

III.6.1. Analyse en Composantes Principales (ACP)

L'Analyse en Composantes Principales (ACP) est un algorithme utilisé pour réduire la dimensionnalité d'un ensemble de données à travers des transformations orthogonales [27]. Ce processus de réduction de dimension permet de diminuer le travail de calcul tout en maintenant la précision de l'information. Dans le domaine de la reconnaissance faciale, étant donné que les images de personnes sont composées de milliers de pixels, l'Analyse en Composantes Principales peut aider à réduire la dimension en un petit nombre, appelé eigenfaces.

Cet algorithme comporte deux étapes : la décentralisation et la recherche d'un système de coordonnées. La décentralisation consiste à placer l'origine des coordonnées au centre des données. Cela facilite les calculs ultérieurs car l'origine est nulle. La recherche du système de coordonnées consiste à trouver une direction qui présente la variance maximale de ces données. L'ACP utilise la matrice de covariance pour réaliser cela. La matrice de covariance reflète la corrélation entre deux variables. Ainsi, en calculant les vecteurs propres et les valeurs propres,

l'ordinateur déterminera dans quelle mesure les coordonnées tournent et quelle est la variance des coordonnées dans cette direction. Selon le principe de l'ACP, plus la valeur des valeurs propres est grande, plus l'information restante est précise. Ainsi, si quelqu'un souhaite réduire la dimension en k dimensions, l'ordinateur conserve les k plus grandes valeurs propres, qu'il utilise pour créer plusieurs eigenfaces.

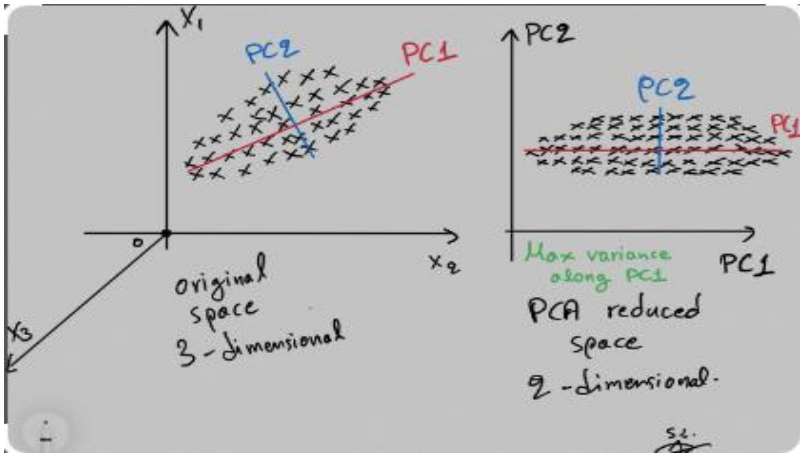

Figure 3. 8: modèle ACP.

III.6.2. L'Analyse Discriminante Linéaire (ADL)

L'Analyse Discriminante Linéaire (LDA), aussi connue sous le nom d'Analyse Discriminante Normale ou Analyse de la Fonction Discriminante, est une méthode de réduction de dimensionnalité largement employée dans les problèmes de classification supervisée. Son objectif est de mieux comprendre les différences entre les groupes en séparant efficacement deux classes ou plus. L'ADL agit en projetant les caractéristiques d'un espace de dimension supérieure dans un espace de dimension inférieure. En apprentissage automatique, elle est utilisée comme un algorithme d'apprentissage supervisé spécialement conçu pour la classification, avec pour but d'identifier une combinaison linéaire de caractéristiques permettant de mieux distinguer les classes au sein d'un ensemble de données.

Par exemple, lorsqu'il faut séparer deux classes, elles peuvent présenter plusieurs caractéristiques. Se baser uniquement sur une de ces caractéristiques pour la classification risque d'entraîner un chevauchement, comme illustré dans la figure ci-dessous. C'est pourquoi il est nécessaire d'augmenter le nombre de caractéristiques pour une classification plus précise.

L'ADL opère en projetant les données sur un espace de dimension inférieure qui maximise la séparation entre les classes. Elle parvient à cela en identifiant un ensemble de discriminants

linéaires qui optimisent le rapport de la variance interclasses à la variance intra-classe. En d'autres termes, elle cherche les directions dans l'espace des caractéristiques qui permettent de mieux discriminer les différentes classes de données.

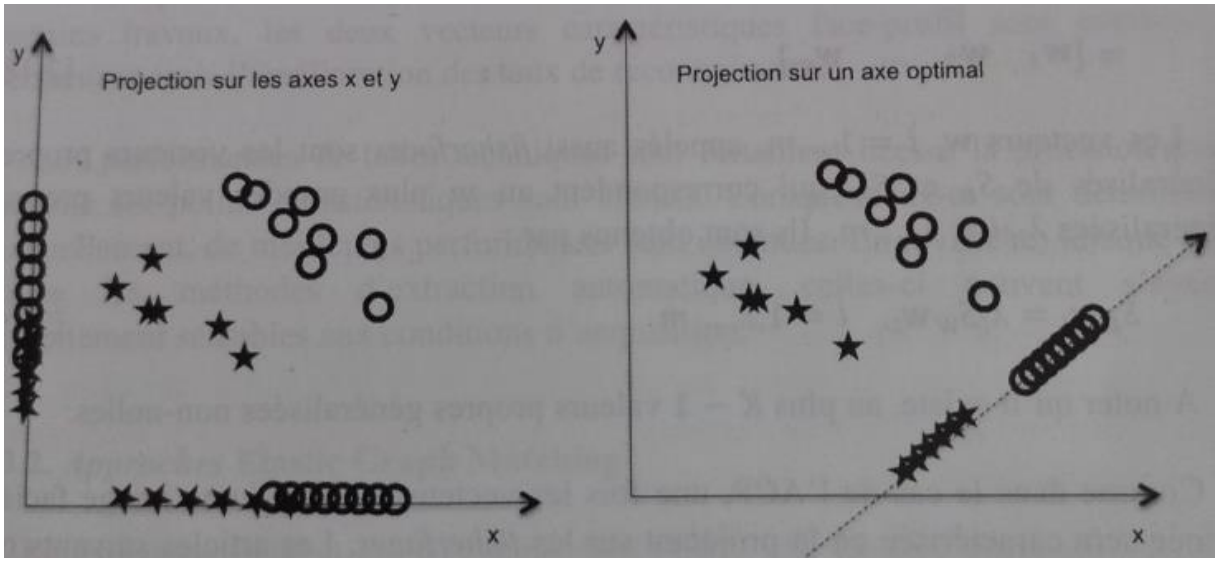

Figure 3. 9: Séparation des classes par LDA.

III.6.3. PCA vs. LDA [28]

PCA et LDA sont similaires en ce sens qu'ils réduisent tous deux les dimensions d'un échantillon. Cependant, les projections PCA ne tiennent pas compte des étiquettes des classes. Une approche alternative consiste à s'éloigner de l'ACP vers un algorithme optimal pour la classification (par opposition à la reconstruction). L'Analyse Discriminante Linéaire (LDA) trouve une projection qui maintient les différentes classes éloignées les unes des autres.

L'ACP conserve la variance maximale.

L'ADL permet la discrimination des classes en trouvant une projection qui maximise la dispersion entre les classes et minimise la dispersion au sein des classes.

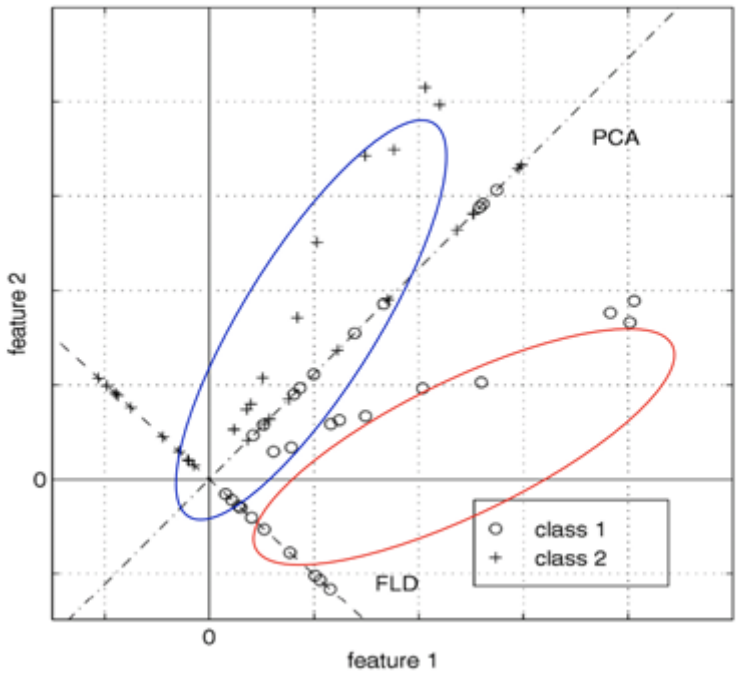

Figure 3. 10: PCA vs. LDA.

La différence entre les projections PCA et LDA est démontrée dans la figure ci-dessus. L'ACP préserve la variance maximale et mappe les points des classes le long de la ligne avec une pente positive, ce qui rend difficile la distinction de la classe des points. Pendant ce temps, l'ADL mappe les points sur la ligne avec une pente négative, ce qui fait que les points sont situés à proximité d'autres points de leur classe et loin des points de la classe opposée.

III.7. La méthode eigenfaces

La base de la méthode eigenfaces est l'analyse des composants principaux (PCA). Eigenfaces et PCA ont été utilisés par Sirovich et Kirby pour représenter efficacement les images du visage [29]. Ils ont commencé avec un groupe d'images de visage originales, et ont calculé le meilleur système vectoriel pour la compression d'image. Ensuite, Turk et Pentland ont appliqué les Eigenfaces pour faire face au problème de reconnaissance [30]. L'analyse des composants principaux est une méthode de projection vers un sous-espace et est largement utilisée dans la reconnaissance des modèles. Un objectif de la PCA est le remplacement de vecteurs corrélés de grandes dimensions par des vecteurs sans corrélation de dimensions plus petites. Un autre objectif est de calculer une base pour l'ensemble de données. Les principaux avantages du PCA sont sa faible sensibilité au bruit, la réduction des exigences

de la mémoire et de la capacité, et l'augmentation de l'efficacité due à l'exploitation dans un espace de dimensions plus petites.
La stratégie de la méthode Eigenfaces consiste à extraire les traits caractéristiques du visage et à représenter le visage en question en tant que combinaison linéaire des soi-disant « eigenfacies » obtenus par le processus d'extraction du caractère.
Les principaux composants des visages dans l'ensemble d'entraînement sont calculés. La reconnaissance est réalisée à l'aide de la projection du visage dans l'espace formé par les faces propres. Une comparaison est faite sur la base de la distance euclidienne des eigenvectors des eigenfaces et de l'eigenface de l'image en question. Si cette distance est suffisamment petite, la personne est identifiée. D'autre part, si la distance est trop grande, l'image est considérée comme appartenant à un individu pour lequel le système doit être formé.

III.8. Conclusion

En conclusion, L'intégration des eigenfaces avec des algorithmes de classification tels que SVM et KNN, les méthodes d'extraction des caractéristiques telles que les Local Binary Patterns (LBP), Local Phase Quantization (LPQ) et : Binarized Statistical Image Features (BSIF). Ainsi que des techniques de réduction de dimensionnalité comme LDA et PCA, offre un cadre robuste pour la reconnaissance faciale. Les eigenfaces réduisent la dimensionnalité tout en capturant les caractéristiques discriminantes, améliorant ainsi la précision de la classification. LDA maximise la séparation des classes, tandis que PCA capture la variance maximale. Cette combinaison réduit la complexité des données, minimise le sur ajustement et améliore la généralisation, permettant des systèmes de reconnaissance robustes et précis.

IV. Chapitre IV : Résultats et Discussion

IV.1. Introduction

Dans ce chapitre, nous allons exploiter un ensemble d'images sélectionnées à partir de la base de données de test « ORL ». Pour prevue la performance de notre système, ce système est comme tout es système biométrique passe les étapes suivant : Acquisition des données, Prétraitement, Extraction des paramétrées, réduction des paramétrées et classification.et nous avons étudies trois types de descripteur telle que LBP, LPQ, BSIF. Ensuite nous avons présente les essentielles de notre résultat afin de compare avec l'état de l'art.

IV.2. Base de donne ORL

Afin de comparer et évaluer les résultats des mesures de similarité fractionnaires et pondérées, nous avons fait appel à une base de visages internationale très répandue dans le domaine de la reconnaissance de visages : l'ORL. Cette dernière, dont un extrait est illustré dans la figure 4.1, comprend 40 individus ayant chacun 10 points de vue distincts. Les photos ont une taille de (80×70) pixels. L'utilisation de cette base permet d'évaluer les systèmes de reconnaissance faciale en fonction des variations dans les conditions d'éclairage, des expressions faciales (sourire, yeux fermés), de la pose et des occultations partielles (port de lunettes) [31].

Figure 4. 1: Les 40 personnes de la base ORL[31].

IV.3 Les Paramètres

Nous avons d'abord importé l'image et l'avons lue à travers le programme MATLAB. Veuillez consulter figure 4.2 ci-dessous.

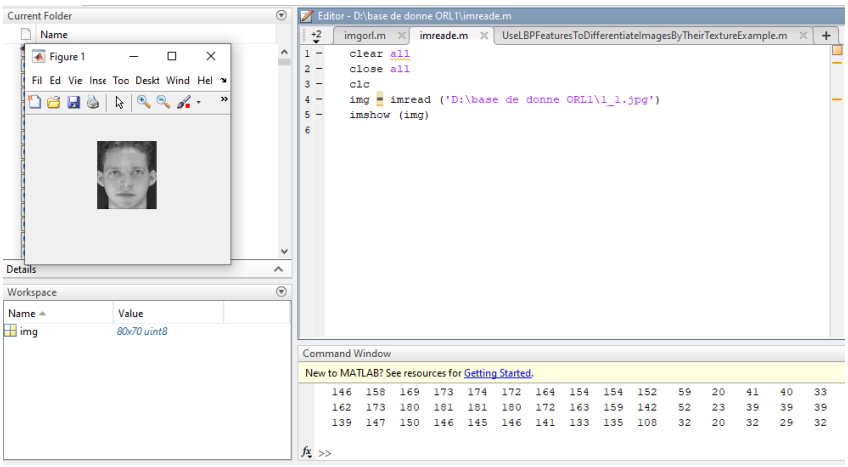

Figure 4. 2: Le programme de lecture d'image.

Une fois que nous avons acquise l'image et identifié ses dimensions, nous avons modifié sa taille afin de simplifier le processus de traitement. Voir la figure 4.3

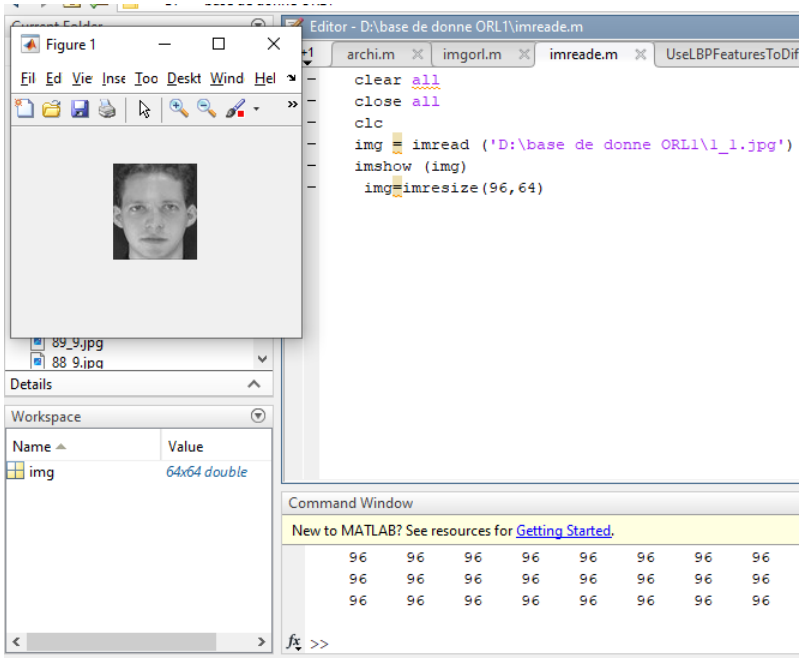

Figure 4. 3: Image de changement de taille.

IV.3. L'interpolation bicubique

L'interpolation bicubique est une méthode d'interpolation utilisée en traitement d'images pour estimer les valeurs de nouveaux pixels lorsqu'une image est agrandie ou réduite. Contrairement à l'interpolation linéaire, qui prend en compte uniquement les pixels voisins, l'interpolation bicubique utilise une approche plus complexe en considérant un voisinage plus large de pixels. Elle utilise des fonctions cubiques pour ajuster les valeurs des pixels, ce qui

permet généralement d'obtenir des résultats plus lisses et plus précis. Cependant, cette méthode nécessite également un calcul plus intensif que l'interpolation bilinéaire. En résumé, l'interpolation bicubique est une méthode avancée pour ajuster la taille des images tout en conservant les détails et en minimisant les artefacts.

IV.4. Les expériences

IV.4.1. Expériences 1

Dans cette expérience, nous avons appliqué la méthode LBP avec les paramètres (P = 8) et (R = 2). Ensuite, nous avons variée la taille de l'image (64 × 64) et (128 × 128), et on a utilisé le nombre de train 2 (le nombre minimale) et le nombre de teste 8.

Figure 4. 4: La représentation LBP.

IV.4.2. Expériences 2

Dans cette expérience, nous avons utilisé la méthode LPQ et avons modifié la taille des images à (32 × 32), (64 × 64) et (128 × 128).

Figure 4. 5: La représentation LPQ.

IV.4.3. Expériences 3

Lors de la dernière expérience, nous avons utilisé la méthode BSIF, à travers laquelle nous avons changé le filtre à 17×17, 12 bit de la taille (32 × 32), 64 × 64) et (128 × 128).

IV.5. Les résultats

Après l'exécution du programme, nous avons obtenu les résultats suivants :

a) LBP avec LDA

Tableau 4. 1:l.es résultats de LBP.

LBP	FRR	FAR	EER	Taux de vérification	Taux de reconnaissance
64× 64	0	0	0	100%	100%
128×128	24.24242	20.35985	22.30114	75%	51%

Nous avons atteint un taux de reconnaissance de 100 % avec une taille d'image de 64 × 64, en utilisant seulement deux exemples d'entraînement (le nombre minimal).

La figure 4.6 montre le FAR en fonction du FRR pour le descripteur LBP et la méthode de réduction LDA, avec une taille d'image de 64 × 64.

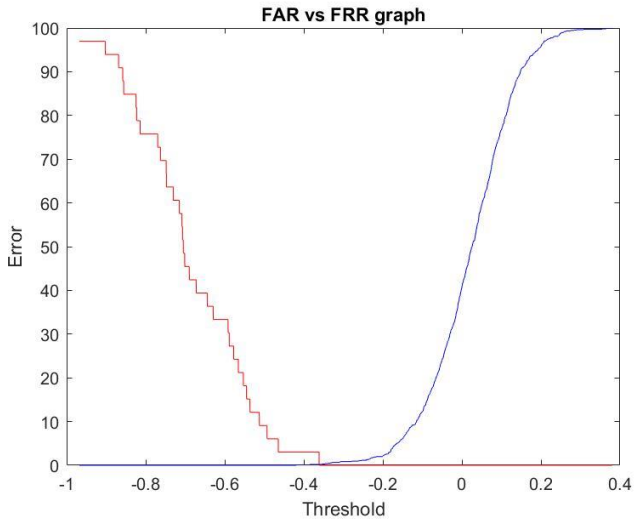

Figure 4. 6: Illustre FRR et FAR avec descripteur LBP.

La figure monter que la zone d'une intersection entre FAR et FRR est très réduite est ça exprime la performance de notre système.

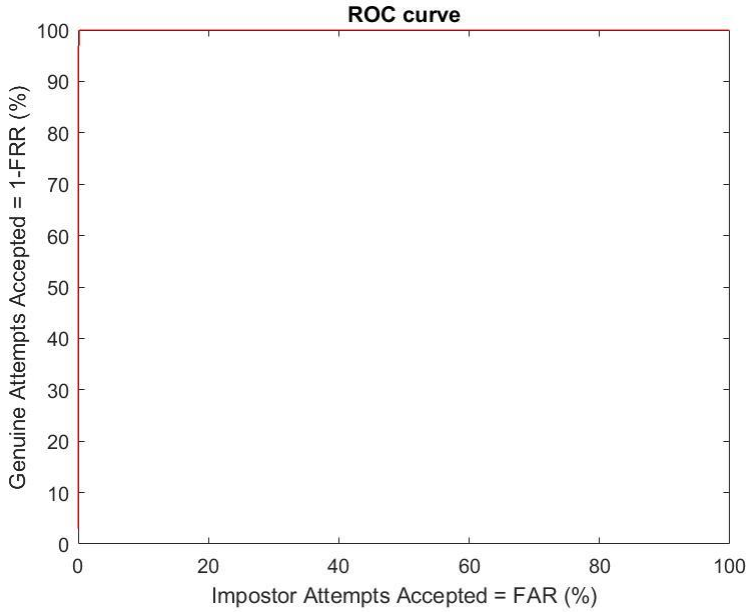

Figure 4. 7: Représente ROC, LDA.

Remarque

Nous avons obtenu un taux de reconnaissance 100% juste au Rank 1

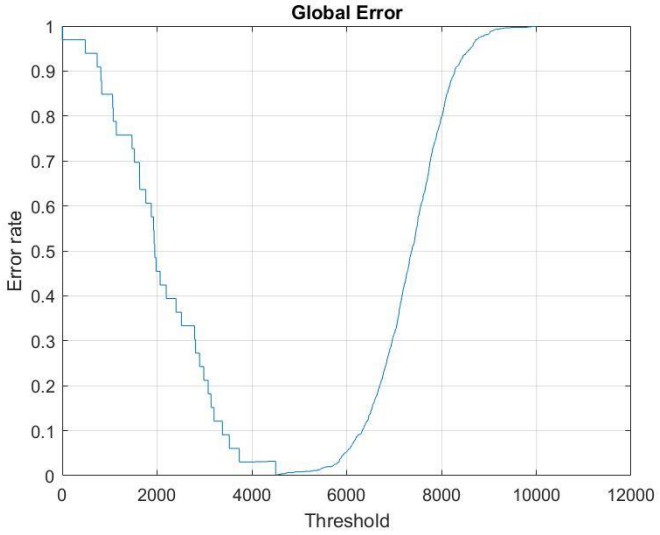

Figure 4. 8: Globale d'erreur.

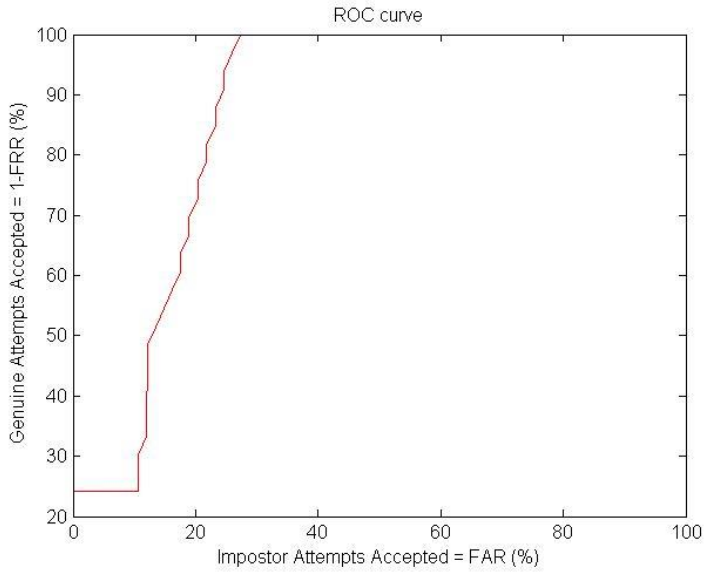

Figure 4. 9: Représente ROC.

Remarque

Nous avons obtenu un taux de reconnaissance 51% au Rank 28.

b) LPQ 13 avec LDA

Tableau 4. 2: Les résultats de LPQ.

LPQ 13	FRR	FAR	EER	Taux de vérification	Taux de reconnaissance
32× 32	3.030303	0.1893939	1.609848	97%	100%
64× 64	3.030303	0.3787879	1.704545	97%	100%
128×128	3.030303	0.3787879	1.704545e	97%	100%

Les résultats obtenus grâce au descripteur LPQ révèlent que ce système produit des performances exceptionnelles même avec une résolution d'image réduite.

c) BSIF taille (17 × 17) 12 bit avec LDA

Tableau 4. 3: Les résultats de BSIF.

BSIF (17× 17)12 bit	FRR	FAR	EER	Taux de vérification	Taux de reconnaissance
32× 32	0	0	0	100%	100%
64× 64	3.030303	0.1893939	1.609848	97%	100%
128×128	3.030303	0.3787879	1.704545	97%	100%

Les résultats obtenus via le descripteur BSIF indiquent que ce système produit de meilleures performances dans les deux modes (identification et vérification), même avec une résolution d'image réduite.

IV.6. Comparaison

Tableau 4. 4: La comparaison des résultats.

Bibliographiques	**Les méthodes qui utilisent**	**Taux de reconnaissance**
[32] année 2018	PCA	99,2%
[33] année 2020	CNN	97.5%
[34] année 2018	TPLBP et FPLBP	95%
Nous	BSIF 17 17 12bit avec LDA	100%

Dans ce tableau, nous avons comparé nos résultats avec certains résultats des autres comme indiqué dans le tableau 4.4.

IV.7. Conclusion

Dans ce chapitre, nous avons présenté les résultats obtenus de la détection des personnes en utilisant les algorithmes LPQ, LBP et BSIF, en les associant à une base de données utilisée pour obtenir des résultats expérimentaux et confirmer notre méthode proposée. De plus, nous avons présenté les résultats, les analyses et les discussions avec des remarques sur notre travail. Nous avons constaté que tous les résultats étaient bons, en particulier ceux obtenus avec l'algorithme BSIF.

Conclusion générale

Ce mémoire a exploré de manière approfondie la biométrie, avec un accent particulier sur la reconnaissance faciale, en abordant ses principes fondamentaux, ses applications et les défis associés. Chaque chapitre a apporté des éclairages spécifiques, consolidant notre compréhension de cette technologie en pleine expansion.

Dans le premier chapitre, nous avons introduit la biométrie en général, en décrivant ses caractéristiques, domaines d'application et diverses modalités. Nous avons expliqué le fonctionnement des systèmes biométriques pour la vérification et l'identification, et présenté les méthodes d'évaluation des performances, notamment les mesures FAR (False Acceptance Rate), FRR (False Rejection Rate), EER (Equal Error Rate) et GAR (Genuine Acceptance Rate). Cette introduction a posé les bases nécessaires pour appréhender les enjeux et les capacités des technologies biométriques.

Le deuxième chapitre a mis en lumière la reconnaissance faciale, une technologie biométrique de plus en plus prévalente. Nous avons discuté de ses applications dans des secteurs variés tels que la santé, la sécurité, la défense, la médecine légale et les transports, tout en soulignant les défis persistants, comme la gestion des variations de poses, d'éclairage, d'expressions faciales, et la présence ou l'absence de composants structuraux. Ces défis représentent des axes de recherche essentiels pour améliorer la précision et l'efficacité des systèmes de reconnaissance faciale.

Le troisième chapitre a exploré en profondeur les techniques utilisées pour la reconnaissance faciale, notamment les méthodes d'extraction des caractéristiques telles que les Local Binary Patterns (LBP), Local Phase Quantization (LPQ) et Binary Robust Independent Elementary Features (BSIF). Il a également abordé les algorithmes de classification comme les SVM (Support Vector Machines) et KNN (K-Nearest Neighbors), ainsi que les techniques de réduction de dimensionnalité comme la LDA (Linear Discriminant Analysis) et la PCA (Principal Component Analysis). Ces approches constituent un cadre solide pour la reconnaissance faciale, permettant de capturer les caractéristiques discriminantes tout en réduisant la redondance et la complexité des données. L'intégration judicieuse de ces techniques améliore les performances des algorithmes de classification, en diminuant le sur ajustement et en renforçant la généralisation.

Le quatrième chapitre a présenté les résultats obtenus à partir de la base de données ORL, démontrant l'efficacité des approches théoriques et méthodologiques discutées dans les chapitres précédents. Ces résultats valident les techniques employées et montrent la faisabilité de développer des systèmes de reconnaissance faciale précis et fiables.

En conclusion, ce mémoire souligne le potentiel significatif de la biométrie, en particulier de la reconnaissance faciale, pour répondre aux besoins croissants de sécurité et de gestion de l'identité. Les avancées technologiques dans ce domaine, bien que prometteuses, doivent encore surmonter divers défis techniques pour atteindre une précision et une robustesse optimales. En combinant différentes méthodes et en comprenant les forces et limites de chaque approche, les praticiens peuvent développer des systèmes de reconnaissance faciale efficaces et précis, ouvrant la voie à des applications toujours plus vastes et sophistiquées. Les futures recherches et innovations continueront à faire évoluer ce domaine, offrant des solutions de plus en plus robustes et adaptées aux besoins contemporains

REFERENCES

- *[1] N. Morizet, 'Reconnaissance biométrique par fusion multimodale du visage et de l'iris', PhD Thesis, Télécom ParisTech, 2009.*
- *[2] Biométrie : des dispositifs sensibles soumis à autorisation de la CNIL, (Avril 2011)*
- *[3] R. Belguechi, 'Contribution a la reconnaissance d'empreintes digitales par une approche hybride', PhD Thesis, ESI, 2006*
- *[4] Anil. K. Jain, P. Flynn, A. Ross, « Handbook of Biometrics », Springer, 2007*
- *[5] Djamel SAIGAA, " Contribution à l'authentification d'individus par reconnaissance de visages", THESE Présentée pour obtenir le Diplôme de Doctorat d"Etat en Automatique, Faculté des Sciences et Sciences de l"ingénieur, Université Mohamed Kheider, Biskra, 2006*
- *[6] These-Pierre-Buyssens (Fusion de differents modes de capture pour la ´ reconnaissance du visage appliquee aux transactions) , 2011.]*
  - [7] Youbi, Zineb, et al. "Novel Approach of Face Identification Based on Multi-scale Local Binary Pattern." 2018 International Conference on Signal, Image, Vision and their Applications (SIVA). IEEE, *2018.*
  - [8] Griouz, Badreddine, et al. "A spatial pyramidal decomposition method for *finger vein recognition using local descriptors." International Journal of Biometrics 12.2 (2020): 131-146.*
- *[9] Anil K. Jain, Stan Z. Li, « Encyclopedia Of Biometrics », Springer 2009*
- *[10] É. Freyssinet and G. Desgens-Pasanau, 'L'identité à l'ère numérique'. Dalloz, 2009.*
- *[11] LOUIBA Fadia et HADJ ALI Ryma "Système de contrôle d'accès physique basé sur le visage" .pp.19 ; 2010.*
- *[12] EURODAC "Information and communication" unit, Directorate-General Justice, Freedom*
- *Security, B-1049 Brussels – August 2004. Retrieved October 22 2013*
- *[13] C. L. Giles "Méthodes d'authentification vocale d'utilisateurs dans les systèmes informatique" thème d'ingénieur C.N.A.M. en informatique, centre régional associe de Strasbourg, 2000.*
- *[14] M. Boutelba Adem et M. Boumeliha Hemza "Reconnaissance de visages par les formes locales binaires LBP" Projet de fin d'études, Université de Jijel, 2018.*

- *[15] M. Aldjia Messaili et M. LydiaSi Hadj Mohand "Conception et réalisation d'un système automatique de reconnaissance faciale" mémoire de fin d'études, Université Mouloud Mammeri Tizi Ouzou, 2012.*
- *[16] Souhila Guerfi Ababsa "Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D" mémoire de fin d'études, UNIVERSITE D'EVRY VAL D'ESSONNE, 2008.*
- *[17] H. Mouna et T. Mohammed Taha et M. Abdel Ouahab "Reconnaissance de visage" thème de fin d'études Université Kasdi Merbah OUARGLA, 2020.*
- *[18] Z.Abdel Aziz & B. Mohamed Taki ALLAH " Etude et réalisation d'un système de reconnaissance de faces humaines par la méthode des faces propres" mémoire de Master, Université SAAD DAHLAB de BLIDA, 2016.*
- *[19] Amine Nait ali & Régis Fournier "traitement du signal et de l'image pour la biométrie" Lavoisier, page 37, 45, 2012*
- *[20] Ardabilian, M., Szeptycki, P., Ouji, K., & Chen, L. (2009, January). Biométrie faciale 3D-Acquisition, prétraitement et reconnaissance. In WISG'09-Workshop Interdisciplinaire sur la Sécurité Globale 2009 (p. inconnue).*
- *[21] Capcha Huaman, A. (2021). Sistema de reconocimiento facial basado en los algoritmos Haar Cascade, DeepFace Y Luxand FaceSDK.*
- *[22] Rahim, M. A., Hossain, M. N., Wahid, T., & Azam, M. S. (2013). Face recognition using local binary patterns (LBP). Global Journal of Computer Science and Technology, 13(4), 1-8.*
- *[23] Dhall, A., Asthana, A., Goecke, R., & Gedeon, T. (2011, March). Emotion recognition using PHOG and LPQ features. In 2011 IEEE International Conference on Automatic Face & Gesture Recognition (FG) (pp. 878-883). IEEE.*
- *[24] Kannala, J., & Rahtu, E. (2012, November). Bsif: Binarized statistical image features. In Proceedings of the 21st international conference on pattern recognition (ICPR2012) (pp. 1363-1366). IEEE.*
- *[25] Liu Ming & Wu Zhaoxia. (2018). Theory and application of support vector machine. Horizon of Science and Technology (23), 68-69.*
- *[26] Mathieu-Dupas, E. (2010). Algorithme des k plus proches voisins pondérés et application en diagnostic. In 42èmes Journées de Statistique.*

- *[27] Wang Zhiyang, Liu Jinlong & Tang Zixian. (2016). Application Research on PCA algorithm in Face Recognition. Horizon of Science and Technology (01), 19-20.*
- *[28] Zhao, W., Krishnaswamy, A., Chellappa, R., Swets, D. L., & Weng, J. (1998). Discriminant analysis of principal components for face recognition. Face recognition: From theory to applications, 73-85.*
- *[29] L. Sirovich and M. Kirby, Low-Dimensional Procedure for the Characterization of Human Faces, Journal of the Optical Society of America, A 4 (1987) 519-524.*
- *[30] M. Turk and A. Pentland, "Eigenfaces for Recognition," Journal of Cognitive Neuroscience, Vol. 3, No. 1 (1991) 71-86.*
- *[31] Chahrazed Rouabhia & Hicham Tebbikh "Mesure de similarité pondérée dans l'espace 2D: Application à la reconnaissance de visages' Article ' Université 8 mai 45 de Guelma.*
- *[32] G. Bencherki, B. Moustafa. "Implémentation d'un système de reconnaissance de visages à base de PCA." (2018).*
- *[33] Gooya, Ehsan Sedgh, et Dominique Pastor. "Première application du réseau de neurones cliques dédiéea la reconnaissance faciale."*
- *[34] B.Adem, B.Hemza, et B. Sabrina Encadreur. "Reconnaissance de visages par les formes locales binaires LBP". 2018. Thèse de doctorat. Université de Jijel.*

Résumé

Dans ce projet, notre objectif est de réaliser un système de reconnaissance faciale et de trouver des solutions pour les contraintes d'acquisition tels que : faible résolution et sombre. Pour trouver la meilleure solution nous avons étudié déférents algorithme (LBP, LPQ et BSIF) afin d'évaluer leur performance dans la reconnaissance faciale.

Cette évaluation repose sur l'utilisation des méthodes de réduction de paramètres (LDA, PCA, K-LDA) aussi k nearest Neighbors K-NN pour classifier les résultats obtenus.

Les tests ont été effectués sur différentes bases de données, et nos résultats montrent un taux de reconnaissance faciale de 100 % sur la base de données ORL

Mots clés : système de reconnaissance faciale, LBP, LPQ, BSIF, LDA, PCA, K-LDA, KNN, ORL.

Abstract

In this project, our goal is to develop a facial recognition system and find solutions for acquisition constraints such as low resolution and darkness.

To find the best solution, we studied different algorithms (LBP, LPQ, and BSIF) to evaluate their performance in facial recognition.

This evaluation relies on the use of parameter reduction methods (LDA, PCA, K-LDA) as well as k-nearest neighbor (K-NN) for classifying the obtained results.

Tests were conducted on various databases, and our results show a facial recognition rate of 100% on the ORL database.

Keywords: facial recognition system, LBP, LPQ, BSIF, LDA, PCA, K-LDA, KNN, ORL.

ملخص

.في هذا المشروع، هدفنا هو تطوير نظام لتعرف الوجوه وإيجاد حلول لقيود الحصول مثل الدقة المنخفضة والظلام

للعثور على أفضل حل، قمنا بدراسة خوارزميات مختلفة BSIF و LBP, LPQ . لتقييم أدائها في التعرف على الوجوه

لتقييم أدائها في التعرف على الوجوه. يستند هذا التقييم إلى استخدام طرق تقليل المعلمات (LDA ،PCA ،K-LDA)

وأيضًا الجار الأقرب (K-NN)

تصنيف النتائج التي تم الحصول عليها. تم إجراء الاختبارات على قواعد بيانات مختلفة، وأظهرت نتائجنا معدل دقة 100٪ في التعرف على الوجوه باستخدام قاعدة بيانات ORL

الكلمات الدالة : LBP, LPQ, BSIF, LDA, PCA, K-LDA, KNN, ORL.