

الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne Démocratique et Populaire
وزارة التعليم العالي و البحث العلمي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Mohamed Seddik Ben Yahia - Jijel
Faculté des Sciences et de la Technologie



جامعة محمد الصديق بن يحيى - جيجل
كلية العلوم والتكنولوجيا

Département D'Automatique

Mémoire

présenté en vue de l'obtention du diplôme

Master en Automatique

Option : Automatique et Informatique Industrielle

Thème

**Mise au point d'un système de
reconnaissance de visage basée Arduino**

Par :

Mr. El Joud Mohamed Yahye

Mr. Benamiour Ibrahim

Travail proposé et dirigé par :

Dr. S. Biad

Promotion 2019

Remerciements

*Tout d'abord nous remercions **ALLAH** le tout puissant
qui nous a éclairé le bon chemin*

Nous adressons nos profonds remerciements à :

*Nos très chers **parents** pour leur soutien et encouragement durant
toutes nos années d'études et sans lesquels on n'aurait jamais réussi.
Nos **frères** et **sœurs**, pour leur présence, leur soutien moral et leurs
encouragements.*

*Madame **S. Biad** d'avoir accepté de nous encadrer pour ce mémoire de fin
d'étude, de son aide et de sa disponibilité tout au long de cette période.*

*Nos remerciements et notre gratitude vont aux
professeurs et **enseignants** de département
d'Automatique ainsi que ses **étudiants** et son **personnel**
côtoyés tout au long de notre cursus universitaire.*

*Nous tenons aussi à remercier **mesdames** et **messieurs**
les membres du jury pour leur précieux temps accordé
à l'étude de notre mémoire.*

*Nos **amis** et toutes les **personnes** qui nous ont aidé de près
ou de loin à réaliser ce modeste travail.*

Dédicace

Je dédie ce modeste travail :

*A mes très chers **parents** pour leur soutien et encouragement durant toutes mes années d'études et sans lesquels je n'aurais jamais réussi et à ma **famille***

*A Ma **fiancée***

*A tous mes **professeurs** et **enseignants** que j'ai eu durant tout mon cursus scolaire et qui m'ont permis de réussir dans mes études.*

*A tous mes **amis***

*A toute **personne** ayant contribué à ce travail de près ou de loin.*

Benamiour Ibrahim

Dédicace

*Je dédie ce mémoire à ma famille
et à mes amis proches ...*

El Joud Mohamed Yahye

Table des matières

REMERCIEMENTS	I
DEDICACE	II
DEDICACE	III
TABLE DES MATIERES	IV
LISTES DES FIGURES	VII
LISTE DES TABLEAUX	IX
INTRODUCTION GENERALE	1
CHAPITRE I : GENERALITE SUR LA BIOMETRIE	1
I.1 Introduction	3
I.2 Définition	3
I.3 Différents modalités	3
I.3.1 Types de modalités biométriques	4
I.3.2 Modalité physiologique	4
I.3.3 Modalité comportementale	6
I.3.4 Combinaison de modalité physiologique et comportementale	7
I.3.5 Comparaison de différentes modalités	7
I.4 Architecture de base d'un système biométrique	8
I.5 Système de reconnaissance faciale	9
I.5.1 Définition	9
I.5.2 Architecture de base d'un système de reconnaissance faciale	9
I.5.3 Techniques de reconnaissance de visage	11
I.5.4 Mesure de la performance d'un système biométrique	12
I.6 Conclusion	14
CHAPITRE II : SYSTEME DE RECONNAISSANCE DE VISAGE	3
II.1 Introduction	15
II.2 Méthodes d'extraction de caractéristiques	15
II.2.1 Méthodes globales	15
II.2.2 Méthodes locales	16
II.2.3 Méthodes hybrides	16
II.3 Motifs Binaires Locaux (Local Binary Patterns)	16

II.4 Quantification de phase locale (Local Phase Quantization)	18
II.4.1 Invariance du flou lors de la phase de transformation de Fourier	18
II.4.2 Transformation de Fourier à court terme en LPQ	19
II.4.3 Analyse statistique des coefficients	20
II.4.4 Décorrélation et quantification	20
II.5 Médiane Robuste Etendu LBP (Median Robust Extended Local Binary Pattern)	21
II.5.1 Motif Binaire Local Etendu (Extended Local Binary Pattern)	22
II.5.2 Descripteur MRELBP	23
II.6 Classification	24
II.6.1 Classifieur k-NN	24
II.6.2 Algorithme de k-NN	24
II.6.3 Validation croisée	25
II.6.4 Matrice de confusion	27
II.7 Conclusion	28
CHAPITRE III : EVALUATION DU SYSTEME	15
III.1 Introduction	29
III.2 Bases des données	29
III.2.1 Base de données de FERET	29
III.2.2 Base de données de ORL	30
III.2.3 Base de données de FERET	30
III.3 Algorithme du système	31
III.3.1 Détection de visage	32
III.3.2 Prétraitement	33
III.3.3 Extraction de caractéristiques	34
III.4 Résultats expérimentales	35
III.4.1 Evaluation globales pour la Base de données FERET	35
III.4.2 Evaluation globales pour la base de données ORL	36
III.4.3 Evaluation globales pour la base de données FEI	36
III.4.4 Discussion des résultats	37
III.5 Conclusion	37
CHAPITRE IV : IMPLEMENTATION DU SYSTEME DEVELOPPEE	29
IV.1 Introduction	38
IV.2 Réalisation	38
IV.2.1 Arduino	39
IV.2.2 La connexion entre les équipements	40
IV.2.3 Interface (Matlab GUIDE)	41
IV.3 Méthodologie de travail	42
IV.4 Comment reconnaître une personne ?	43
IV.4.1 Première étape : Apprentissage	43
IV.4.2 Deuxième étape : Reconnaissance	43

IV.5 Résultats d'expérimentation	43
IV.5.1 Identifier quelqu'un qui cache une partie de visage	44
IV.5.2 Identifier quelqu'un qui porte des lunettes de vue	44
IV.5.3 Identifier quelqu'un dans des conditions d'illumination (éclairage) différentes	45
IV.5.4 Identifier une personne dans différentes postures	46
IV.6 Conclusion	46
CONCLUSION GENERALE	47
BIBLIOGRAPHIE	X

Listes des figures

Figure I.1 : Analyse de Zephyr : comparaison de différentes modalités selon quatre critères	7
Figure I.2 : Enrôlement d'une personne dans un système biométrique ^[10]	8
Figure I.3 : Authentification d'un individu dans un système biométrique	8
Figure I.4 : Identification d'un individu dans un système biométrique	9
Figure I.5 : schéma général de la reconnaissance faciale ^[12]	10
Figure I.6 : Caractéristiques géométriques du visage	11
Figure I.7 : Équilibre FAR et FRR	13
Figure I.8 : Un exemplaire d'un courbe ROC	14
Figure II.1 : Différents méthodes d'extraction de caractéristiques	15
Figure II.2 : Un exemple de l'opérateur de base LBP	16
Figure II.3 : Exemples d'opérateurs LBP étendus ^[20] : les voisinages circulaires (8,1), (16,2) et (24,3)	17
Figure II.4 : Vue d'ensemble de l'approche	22
Figure II.5 : La différence entre Underfit et Overfit	25
Figure II.6 : Train / test division ou Holdout (2 groupes)	26
Figure II.7 : Schéma illustrant la division en k sous-ensemble (k groupes)	26
Figure II.8 : Schéma illustrant comment fonctionne la méthode LOO	27
Figure III.1 : Aperçu de la base de données FERET	30
Figure III.2 : Aperçu de la base de données ORL	30
Figure III.3 : Aperçu de la base de données FEI	31
Figure III.4 : Schéma fonctionnel du système général de reconnaissance de visage	32
Figure III.5 : Exemples de caractéristique de Haar ^[29]	33
Figure III.6 : Différentes étapes du prétraitement	33
Figure III.7 : Exemple du prétraitement de l'image	33
Figure III.8 : Schéma illustrant la différence entre un histogramme égalisé et un histogramme non égalisé	34
Figure III.9 : Image égalisée (a), traitée par l'opérateur LBP (b) puis l'histogramme LBP (c)	34
Figure III.10 : Courbe ROC présentant les trois différents méthodes (MRELBP, LPQ et LBP)	35
Figure III.11 : Courbe ROC présentant les trois différents méthodes (MRELBP, LPQ et LBP)	36
Figure III.12 : Courbe ROC présentant les trois différents méthodes (MRELBP, LPQ et LBP)	37
Figure IV.1 : Application réalisée	38
Figure IV.2 : La carte Arduino	39
Figure IV.3 : Interface du projet réalisé	41
Figure IV.4 : Accuracy de la descripteur et base de données choisies	42
Figure IV.5 : Détection de visage (a), recadrage du visage (b), conversion en niveau de gris (c)	42
Figure IV.6 : Base de données enregistrée	44

Figure IV.7 : Image avec une partie du visage cachée	44
Figure IV.8 : Personne portant des lunettes	45
Figure IV.9 : Personne portant des lunettes	45
Figure IV.10 : Personne avec différentes poses	46

Liste des tableaux

Tableau II.1: <i>Tableau illustrant la matrice de confusion</i>	27
Tableau III.1 : <i>Résultat de la base de données FERET</i>	35
Tableau III.2 : <i>Résultat de la base de données ORL</i>	36
Tableau III.3 : <i>Résultat de la base de données FEI</i>	36

Introduction générale

La biométrie, est la technologie qui mesure les caractéristiques du vivant afin de l'authentifier. Il existe plusieurs caractéristiques biométriques (traits) chez l'être humain comme : l'empreinte digitale, l'iris et la rétine de l'œil, le visage, la voix, etc. Chacun de ces traits offre un niveau de précision particulier. Cependant le visage conserve la capacité d'identification à une distance de plusieurs mètres, ne nécessitant ni la connaissance ni la coopération du sujet.

Un système de contrôle basé sur les données biométriques et spatialement visage est un système fortement recommandé pour plusieurs processus et dans plusieurs domaines pour remplacer les systèmes classiques basés sur les mots de passe, cartes à puce, etc... Ceci est dû au fait qu'il offre un niveau élevé de sécurité et améliore la fiabilité du contrôle. Aujourd'hui, ce type de système est devenu réalisable à cause du développement des moyens informatiques et technologiques. Il est basé sur la transformation des particularités physiologiques ou comportementales uniques en *un exemplaire numérique*. Alors l'identification et l'authentification sont réalisées par une opération de comparaison statistique entre un exemplaire numérique de référence et un autre obtenu en temps réel.

Le passage du physiologique en numérique s'entoure principalement sur l'étape primordiale d'extraction de caractéristiques. Dans le cadre de cette étude, on a utilisé la méthode LBP (Local Binary Pattern) ^[1].

Les LBP ou motifs binaires locaux ont initialement été proposés par Ojala, Pietikäinen et Harwood en 1996 ^[1]. Son principe est basé sur l'assignation d'un code binaire à chaque pixel de l'image en fonction de son voisinage. Cette méthode a l'avantage d'être simple et efficace dans le cadre de la reconnaissance de visage. Nous avons utilisé deux variantes de méthodes LBP à savoir la méthode LPQ (Local Phase Quantization) ^[2] et MRELBP (Median Robust Extended LBP) ^[3].

Notre travail s'intéresse au problème général de la reconnaissance de visages en contexte de vidéosurveillance. Ainsi, dans ce mémoire, nous aurons à concevoir et à implémenter une application permettant la reconnaissance des visages des personnes en temps réel, basée sur Arduino et camera IP. La sortie du système est une valeur qui représente le score de comparaison des caractéristiques des visages extraits de la base avec celle qui existe dans la en temps réel sur camera. Cette sortie active l'allumage de LED reliées à la carte Arduino.

Introduction générale

Nous avons choisi d'articuler notre étude autour de quatre chapitres principaux :

Le premier chapitre est consacré à la présentation générale de la biométrie. Il décrit le principe de fonctionnement des systèmes biométriques puis définit les outils utilisés pour évaluer leurs performances. Ensuite, la place de la reconnaissance faciale parmi les autres techniques biométriques est analysée.

Le deuxième chapitre présente en détail l'approche proposée avec les différentes étapes et mesures d'évaluation.

Le troisième chapitre, nous présentons les résultats expérimentaux obtenus par chaque méthode en analysons leurs performances, suivi d'une discussion avec interprétation des résultats.

L'application réalisée est présentée en détail au cours du quatrième chapitre.

Enfin, la conclusion générale résumera les résultats obtenus par les différentes approches et donnera quelques perspectives sur les travaux futurs.

Chapitre I : Généralité sur la biométrie

I.1 Introduction

La reconnaissance biométrique est l'un des problèmes les plus étudiés en informatique. L'utilisation de techniques biométriques, telles que le visage, les empreintes digitales, l'iris, les oreilles, est une solution pour obtenir une identification personnelle sécurisée.

La biométrie utilise des méthodes de reconnaissance unique des humains basées sur un ou plusieurs traits physiques (modalité) ou comportementaux intrinsèques. En informatique, en particulier, la biométrie est utilisée comme une forme de gestion d'accès d'identité et de contrôle d'accès. Elle est également utilisée pour identifier les individus dans les groupes sous surveillance.

Ces dernières années, plusieurs systèmes de reconnaissance et d'authentification basés sur des mesures biométriques ont été proposés. Les algorithmes et les capteurs ont été développés pour acquérir et traiter de nombreux traits biométriques différents. De plus, La technologie biométrique est utilisée de manière innovante, avec un potentiel commercial et implications pratiques pour nos activités quotidiennes.

Dans ce chapitre, nous allons présenter un état d'art détaillé sur les modalités biométriques en donnant l'architecture de base d'un tel système, décrire ses deux modes de fonctionnement (vérification et authentification) ainsi que les différentes notions liées.

I.2 Définition

Le terme biométrie est composé de deux mots - Bio (mot grec pour la vie) et métrique (mesures). La biométrie est une branche de la technologie de l'information qui vise à établir son identité en se basant sur des traits personnels, est aussi une technologie utilisée pour identifier, analyser et mesurer les caractéristiques physiques et comportementales d'un individu.

La biométrie est actuellement un mot à la mode dans le domaine de la sécurité de l'information car elle offre un degré élevé de précision dans l'identification d'un individu.

I.3 Différents modalités

Une modalité biométrique n'est rien d'autre qu'une catégorie d'un système biométrique dépendant du type de trait humain qu'elle prend en entrée.

La biométrie est en grande partie statistique. Plus les données disponibles sur les échantillons sont nombreuses, plus le système sera probablement unique et fiable. Il peut travailler sur diverses modalités relatives à la mesure du corps et des caractéristiques d'un individu, ainsi qu'à des schémas comportementaux. Les modalités sont classées en fonction des traits biologiques de la personne.

Chaque être humain est unique en termes de caractéristiques, ce qui le rend différent de tous les autres. Les attributs physiques tels que les empreintes digitales, la couleur de l'iris, la couleur des

cheveux, la géométrie de la main et des caractéristiques comportementales telles que le ton et l'accent de la parole, la signature ou la manière de taper les touches du clavier de l'ordinateur, etc., distinguent les personnes le reste.

I.3.1 Types de modalités biométriques

Il existe divers caractères présents chez l'humain, qui peuvent être utilisés comme modalités biométriques. Les modalités biométriques relèvent de trois types ^[4] :

- Physiologique
- Comportementale
- Combinaison de modalité physiologique et comportementale

I.3.2 Modalité physiologique

Cette modalité concerne la forme et la taille du corps. Par exemple :

- **Reconnaissance des empreintes digitales**



La technologie de reconnaissance des empreintes digitales ^[5] a été réalisée en prenant une photo du bout des doigts et en enregistrant les caractéristiques, notamment les verticilles, les arcs et les boucles du bout des doigts. Il capture également les modèles de crêtes et de minuties pour une analyse précise.

L'empreinte digitale est une solution biométrique très sécurisée, fiable et stable. Les organismes chargés de l'application de la loi utilisent cette technologie depuis des décennies pour identifier les criminels. Actuellement, cette technologie est en train de devenir populaire dans les domaines de la sécurité domestique, des opérations bancaires, de la gestion de la main d'œuvre, etc.

- **Système de reconnaissance faciale**



La technique de reconnaissance faciale ^[6] enregistre les images de visage à l'aide d'une caméra vidéo numérique et analyse les caractéristiques faciales telles que la distance entre les yeux, le nez, la bouche et les bords de la mâchoire. Ces mesures sont décomposées en plans du visage et conservées dans une base de

données, utilisée ensuite à fins de comparaison.

Ensuite, le système crée un modèle sur la base de données pour permettre à cette personne de comparer les données pour d'autres utilisations.

- **Système de reconnaissance de l'iris**



Beaucoup reconnaissent la reconnaissance de l'Iris [7] comme la meilleure technologie biométrique d'identification. Il analyse les caractéristiques de l'iris, notamment les anneaux, les sillons et les taches de rousseur, situés dans le tissu coloré autour de la pupille. Le scanner d'iris contient une caméra

vidéo et fonctionne à travers des lunettes et des lentilles de contact. La reconnaissance de l'Iris est utilisée par de nombreux pays dans des endroits cruciaux tels que les frontières, les banques, les entreprises privées, les instituts, les forces de l'ordre, etc.

- **Système de reconnaissance de la géométrie de la main**



La reconnaissance de la géométrie de la main fonctionne avec la forme des caractéristiques de la main d'une personne. Le lecteur de géométrie de la main mesure la main d'un individu dans plusieurs dimensions. Ensuite, il stocke les données pour une comparaison et une mesure ultérieures.

Il est principalement apprécié pour son confort, sa facilité et son acceptation par le public. Néanmoins, ce système n'est pas très unique, tout comme la reconnaissance des visages ou des empreintes digitales.

- **Système de balayage rétinien**



La reconnaissance rétinienne est une modalité biométrique qui utilise la technologie infrarouge pour capturer les modèles uniques des vaisseaux sanguins rétiniens d'un individu. En tant qu'organe interne de l'œil et protégé des environnements

extérieurs, la reconnaissance de la rétine est reconnue comme un système d'authentification biométrique fiable.

- **Système de reconnaissance de l'ADN**



L'ADN biométrique est assez différent des modalités biométriques standard. Cela nécessite un échantillon physique tangible et ne peut être effectué en temps réel. C'est une technologie de reconnaissance avec une très grande précision.

I.3.3 Modalité comportementale

Cette modalité est liée au changement de comportement humain au cours du temps. Par exemple :

- **Reconnaissance de la démarche (la façon dont on marche)**



La reconnaissance de la démarche consiste à identifier les humains en fonction de leurs caractéristiques de démarche. Comparées à d'autres éléments biométriques tels que le visage et les empreintes digitales, les caractéristiques de la démarche peuvent toujours être obtenues et

reconnaissables à distance avec une vidéo à faible résolution. Par conséquent, avec des caractéristiques de plage de reconnaissance sans contact, longue distance (50 mètres), à vision croisée (360 °) et difficile à dissimuler, la reconnaissance de la marche comble le vide du marché de l'identification longue distance dans l'industrie de la sécurité publique.

- **Système de reconnaissance de frappe**



Cette analyse biométrique analyse le schéma de frappe du candidat, son rythme et sa vitesse de frappe au clavier. Les mesures du temps de passage et du temps de vol sont utilisées dans la reconnaissance de frappe.

Temporisation : Il s'agit de la durée pendant laquelle une touche est enfoncée.

Temps de vol : C'est le temps écoulé entre le relâchement d'une touche et l'appui sur la touche suivante.

- **Reconnaissance de la signature**



La reconnaissance des signatures est l'un des types de comportement de la biométrie. Cela fonctionne de deux manières, statique et dynamique. Dans ce système de reconnaissance, la manière dont une personne signe son nom est considérée comme une caractéristique de cette personne. Il est basé sur des

mesures telles que le nombre de contours intérieurs et le nombre de composantes de la pente verticale.

I.3.4 Combinaison de modalité physiologique et comportementale

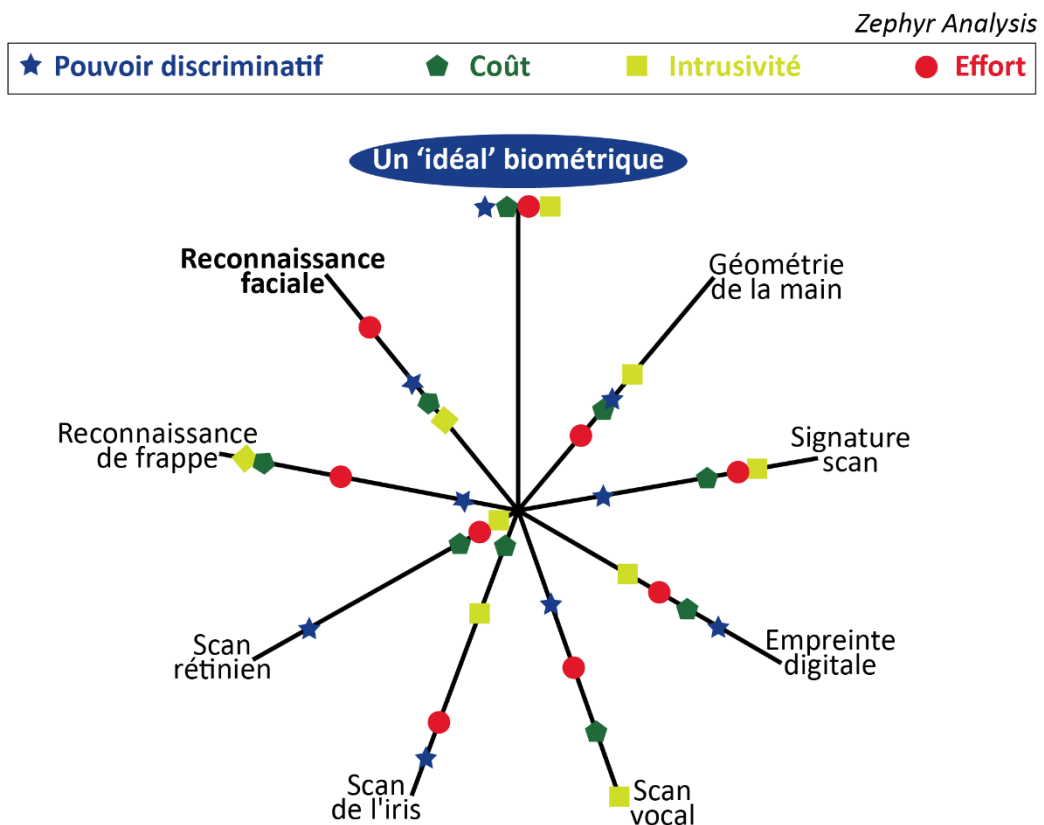
Cette modalité inclut les deux traits, ceux-ci dépendant de changements physiques et comportementaux. Par exemple le cas de la reconnaissance vocal où cela dépend de la santé, de la taille et de la forme de la corde vocale, des cavités nasales, de la bouche, des lèvres, etc., ainsi que de l'état émotionnel, de l'âge, de la maladie (comportement) d'une personne.

I.3.5 Comparaison de différentes modalités

Le succès d'un système biométrique dépend souvent du choix de la modalité biométrique appropriée, mais ce n'est pas facile. Une recherche minutieuse incluant des comparaisons rigoureuses des forces et des faiblesses de la modalité est un élément important pour aider à choisir le bon matériel. Les facteurs à prendre en compte dans la comparaison sont les suivants : l'intrusivité, le pouvoir discriminant, le coût et l'effort. Zephyr a résumé le concept dans la figure (I.1) [8].

Il est important de réaliser qu'il n'existe pas une modalité biométrique optimale pour toutes les conditions et pour toutes les implémentations. De nombreux facteurs doivent être pris en compte lors de l'implémentation d'un dispositif biométrique, notamment l'emplacement, la sécurité, l'acceptabilité et la facilité d'utilisation. Toutefois, les performances et les coûts peuvent varier si vous prenez en compte les exigences de déploiement et l'environnement.

Figure I.1 : Analyse de Zephyr : comparaison de différentes modalités selon quatre critères



I.4 Architecture de base d'un système biométrique

Les systèmes biométriques ont eu un impact significatif sur les pratiques d'identification personnelle et d'authentification à l'échelle mondiale. Cette technologie a non seulement changé la façon dont les personnes sont identifiées, mais a également réduit considérablement le temps nécessaire aux processus d'identification et de vérification. La vérification d'une identité revendiquée ne prend pas plus de quelques secondes avec la biométrie, alors qu'avec les méthodes traditionnelles, cela pourrait même prendre plusieurs jours. L'exécution d'une requête d'identification sur une base de données biométrique avec des millions d'enregistrements est également devenue beaucoup plus rapide avec le développement de machines informatiques avancées. Dans certains secteurs d'activité tels que la banque, les finances, les télécommunications, etc., connaître le client est un aspect important de la protection des services contre une utilisation abusive potentielle. Un système de reconnaissance biométrique comporte deux étapes ^[9] :

- **Enrôlement** : les données biométriques d'une personne sont enregistrées dans la base de données biométrique du système (*figure I.2*).
- **Reconnaissance** : les données biométriques nouvellement acquises d'une personne (que nous appelons une sonde) sont comparées aux données biométriques inscrites (que nous appelons un modèle) et un score de correspondance est généré. Le score de correspondance nous indique à quel point le modèle et la sonde sont similaires. Sur la base des scores de correspondance, nous décidons ensuite si le modèle et la sonde proviennent de la même personne (**vérification**) (*figure I.3*). Ou de l'identité de la galerie à attribuer à l'entrée biométrique (**identification**) (*figure I.4*).

Figure I.2 : Enrôlement d'une personne dans un système biométrique ^[10]

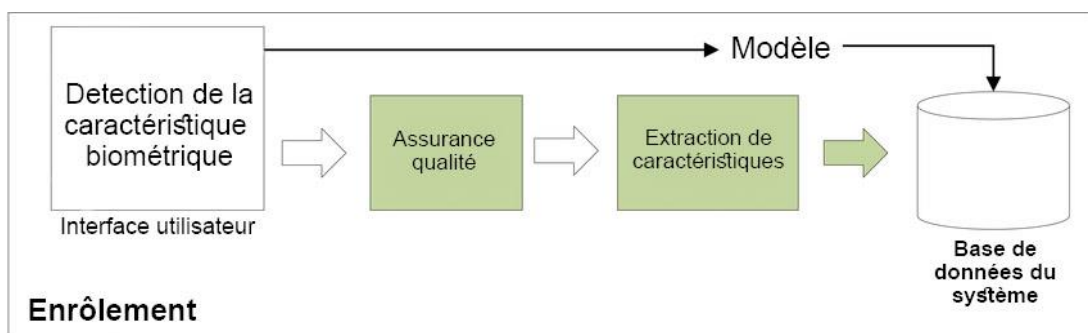


Figure I.3 : Authentification d'un individu dans un système biométrique

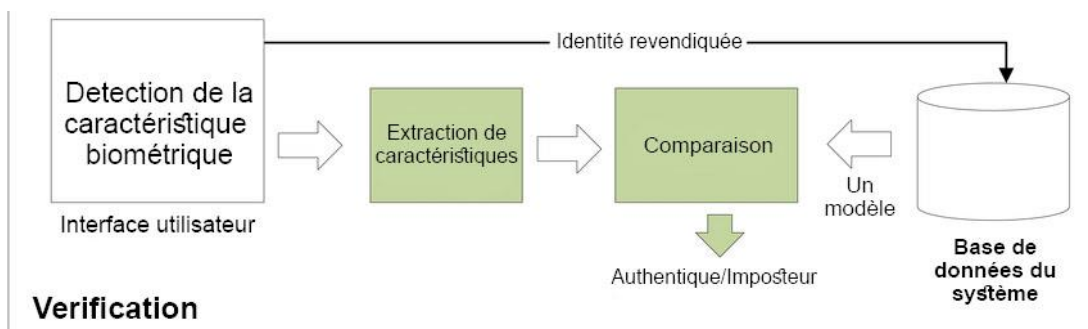
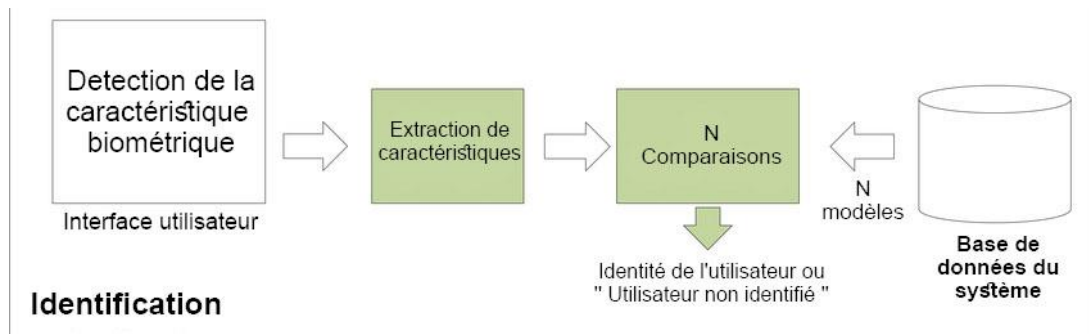


Figure I.4 : Identification d'un individu dans un système biométrique



I.5 Système de reconnaissance faciale

En raison de la diversité de ses applications réelles, allant de l'authentification de l'utilisateur (accès contrôle, ATM^[11]) à la vidéosurveillance et à l'application de la loi, la reconnaissance faciale^[6] a été l'un des sujets de recherche les plus actifs en vision par ordinateur et en reconnaissance de formes. En outre, il a l'avantage évident par rapport aux autres techniques biométriques, car il est naturel, socialement bien accepté, et notamment non intrusif. En réalité, plusieurs techniques d'authentification biométrique fiables sont disponibles et largement utilisés de nos jours (tels que l'iris^[7] ou les empreintes digitales^[5]), mais ils reposent principalement sur une participation active de l'utilisateur. Au contraire, la biométrie faciale exige très peu coopération de l'utilisateur ; grâce à cette fonctionnalité conviviale, la reconnaissance faciale est réputée être non intrusif.

Au cours des dernières décennies, des progrès importants ont été réalisés dans le domaine de la reconnaissance faciale. Néanmoins, la reconnaissance faciale, notamment dans des scénarios non contrôlés, reste active et non résolu. Parmi les nombreux facteurs affectant la performance des systèmes de reconnaissance faciale, le fait que c'est une technologie sensible à l'environnement (éclairage, position, expression du visage...), en plus on trouve : les vrais jumeaux ne sont pas différenciés, sensibilité aux changements (barbe, moustache, lunette, chirurgie...)

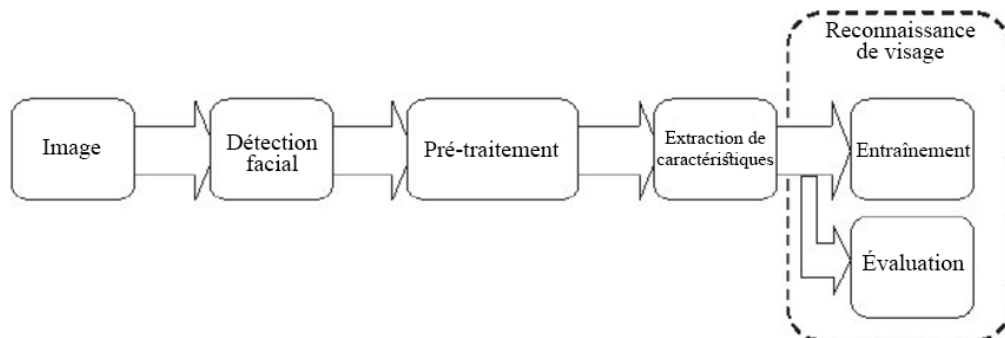
I.5.1 Définition

La reconnaissance faciale est une méthode d'identification ou de vérification de l'identité d'un individu en utilisant son visage. Elle peut être utilisée pour identifier des personnes sur des photos, des vidéos ou en temps réel.

I.5.2 Architecture de base d'un système de reconnaissance faciale

Le système de reconnaissance de visage est composé des principales étapes^[12] illustrées sur le schéma de la *figure I.5*.

Figure I.5 : schéma général de la reconnaissance faciale ^[12]



a. Bloc de détection de visage

Il s'agit de la première étape de tout système de reconnaissance de visage et de la différence essentielle entre une reconnaissance de visage semi-automatique et une reconnaissance de visage entièrement automatique. Afin de rendre le système de reconnaissance entièrement automatique, la détection et l'extraction de visages à partir d'une image doivent également être automatiques. Cette étape représente une phase très importante avant la reconnaissance des visages, car la précision du processus de reconnaissance dépend directement de la précision du processus de détection.

b. Bloc de prétraitement

L'image du visage peut être traitée avec une série de techniques de prétraitement afin de minimiser l'effet de facteurs pouvant influencer négativement l'algorithme de reconnaissance de visage. Les plus critiques sont la pose et l'éclairage du visage.

c. Bloc d'extraction de caractéristiques

Dans cette étape, les caractéristiques utilisées dans la phase de reconnaissance sont calculées. Ces fonctionnalités varient en fonction du système de reconnaissance automatique du visage utilisé. Par exemple, les premières caractéristiques les plus simples utilisées dans la reconnaissance des visages étaient les relations géométriques et les distances entre les points importants d'un visage, et l'algorithme de reconnaissance correspondant à ces distances ; La fonctionnalité que nous allons utiliser dans ce travail est le LBP ^[1].

d. Bloc de reconnaissance de visage

Il comprend deux étapes distinctes : un processus d'entraînement, dans lequel l'algorithme fournit des échantillons des sujets à apprendre et un modèle distinct pour chaque sujet est déterminé ; et un processus d'évaluation dans lequel un modèle d'un sujet de test nouvellement acquis est comparé à tous les modèles existants dans la base de données et le modèle le plus étroitement correspondant est déterminé. L'algorithme de reconnaissance standard utilise la distance euclidienne ou Mahalanobis pour faire correspondre les caractéristiques. Si ceux-ci sont suffisamment proches, un événement de reconnaissance est déclenché.

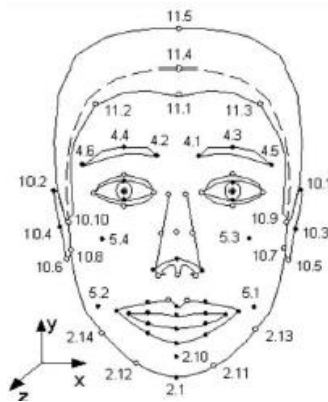
I.5.3 Techniques de reconnaissance de visage

Les algorithmes de reconnaissance de visage peuvent être classés en deux grandes catégories selon les schémas d'extraction de caractéristiques utilisés pour la représentation de visage : les méthodes basées sur les caractéristiques et les méthodes basées sur l'apparence. Les propriétés et les relations géométriques, telles que les zones, les distances et les angles entre les points caractéristiques du visage, sont utilisés comme descripteurs pour la reconnaissance des visages. D'autre part, les méthodes basées sur l'apparence considèrent les propriétés globales du motif d'intensité de l'image du visage. Ces algorithmes utilisent généralement des vecteurs de base pour représenter efficacement les données de visage. Les algorithmes populaires tels que PCA ^[13], LDA ^[14], ...etc.

I.5.3.1 Technique basée sur la géométrie (*Geometry-based Technique*)

Dans cette technique, les caractéristiques géométriques sont extraites à l'aide de la taille et de la position relative d'importants composants d'images. Alors, la direction et les arêtes d'un composant important sont d'abord détectées, puis des vecteurs de caractéristiques sont construits à partir de ces arêtes de cette direction. Le résultat de cette opération est la caractérisation du visage par des distances et des proportions entre des points particuliers comme les yeux, le nez les coins de la bouche. Dans cette catégorie, on peut citer les travaux de ^[15] ^[16].

Figure I.6 : Caractéristiques géométriques du visage



I.5.3.2 Techniques basées sur des modèles (*Template Based Techniques*)

Cette technique permet d'extraire les caractéristiques faciales basées sur des modèles précédemment conçus à l'aide de la fonction d'énergie appropriée. La meilleure correspondance entre les modèles dans l'image faciale produit le minimum d'énergie. Yuille et ses collaborateurs ^[17] ont proposé des méthodes permettant de détecter et de décrire les caractéristiques des visages à l'aide de modèles déformables. Dans les modèles déformables, la caractéristique intéressante, un œil par exemple, est décrit par un modèle paramétré. Ces modèles paramétrés permettent a priori de connaître la forme attendue des caractéristiques pour guider le processus de détection.

Une fonction d'énergie est définie pour lier les sommets, les arêtes et les creux de l'intensité de l'image aux propriétés correspondantes du modèle. Ensuite, la correspondance du modèle avec l'image est effectuée en modifiant les valeurs de ses paramètres afin de minimiser la fonction d'énergie, se déformant de ce fait pour trouver le meilleur ajustement. Pour les besoins du descripteur, la valeur finale du paramètre est utilisée. Dans la détection des yeux et de la bouche basée sur un modèle, un modèle oculaire est utilisé pour détecter l'œil à partir d'une image. Ensuite, une corrélation est établie entre les modèles d'œil et diverses régions superposées de l'image du visage. La région des yeux a une corrélation maximale avec le modèle.

1.5.3.3 Approche basée sur l'apparence (Appearance-based approach)

Cette approche traite l'image comme un motif bidimensionnel. Le concept de « caractéristique » dans cette approche est différent des simples traits du visage tels que les yeux et la bouche. Toute caractéristique extraite de l'image est référée à une entité. Ce groupe de méthodes a obtenu les meilleurs résultats lors de l'extraction de caractéristiques faciales, car il conserve les informations importantes de l'image et rejette les informations redondantes. Des méthodes telles que l'Analyse en Composantes Principales ACP ^[13] (Principal Component Analysis PCA) et l'Analyse en Composantes Indépendantes ACI ^[18] (Independent Component Analysis ICA) sont utilisées pour extraire le vecteur de caractéristiques.

1.5.3.4 Approche basée sur la couleur (Color-based approach)

Cette approche utilise la couleur de la peau pour isoler la zone du visage de la zone non-visage d'une image. Toute région non colorée dans le visage est considérée comme un candidat pour les yeux ou la bouche. La performance de telles techniques sur les bases de données d'images faciales est plutôt limitée en raison de la diversité des origines ethniques ^[15].

1.5.4 Mesure de la performance d'un système biométrique

La popularité croissante de la biométrie dans l'identification et l'authentification classiques a rendu extrêmement important d'assurer que les performances des systèmes, solutions et applications biométriques atteignent un niveau acceptable. Dans tout système ou solution, l'évaluation des performances et les métriques renforcent la confiance des futurs utilisateurs. L'évaluation des performances devient particulièrement importante pour les systèmes en cours d'utilisation dans des applications cruciales ou hautement sécurisées.

Différentes métriques peuvent être utilisées à cette fin. Les mesures de performance Les plus communs sont le FAR (taux de fausse acceptation), le FRR (taux de faux rejet), le taux d'erreur égal (EER) et la courbe ROC ^[19].

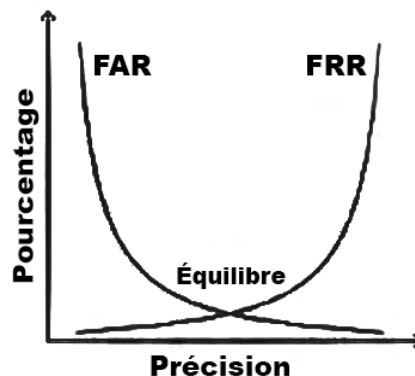
1.5.4.1 Taux de fausse acceptation (False Accept Rate FAR)

Le FAR est la probabilité de cas dans lesquels un système biométrique autorise par erreur une personne non autorisée. Cela se produit lorsqu'un système, une solution ou une application biométrique met en correspondance de manière erronée une entrée biométrique avec un modèle enregistré, renvoyant par erreur une correspondance et accordant l'accès à une personne non autorisée. C'est l'un des paramètres couramment utilisés dans les systèmes de reconnaissance biométrique pour évaluer les performances du système. La fausse acceptation est un résultat indésirable d'un système biométrique. Il est exprimé en pourcentage d'instances dans lesquelles le système autorisera une personne non autorisée. Par exemple : si $FAR = 0,1\%$, cela signifie que dans 1 cas sur 1 000, un système biométrique, une solution d'application ont une probabilité d'accorder l'accès à une personne non autorisée.

1.5.4.2 Taux de faux rejet (False Reject Rate FRR)

Le FRR (taux de faux rejet), au contraire, est la probabilité de cas pour lesquels un système biométrique refuse faussement l'accès à une personne autorisée. Cela se produit lorsqu'un système, une solution ou une application biométrique ne parvient pas à faire correspondre l'entrée biométrique à un modèle stocké, renvoyant par erreur une non-correspondance et refusant l'accès à une personne autorisée. Le taux de faux rejets (FRR) est l'un des paramètres importants aux côtés de la FAR et est couramment utilisé pour évaluer les performances d'un système, de solutions et d'applications biométriques. Comme les FAR, il est également exprimé en pourcentage de probabilité, dans lequel un système refusera faussement l'accès à une personne autorisée. Par exemple, si $FRR = 0,01\%$, cela signifie que 1 cas sur 10 000, un système biométrique, une solution d'application ont une probabilité de refuser l'accès à une personne autorisée.

Figure I.7 : Équilibre FAR et FRR



1.5.4.3 Taux d'erreur égal (Equal Error Rate EER)

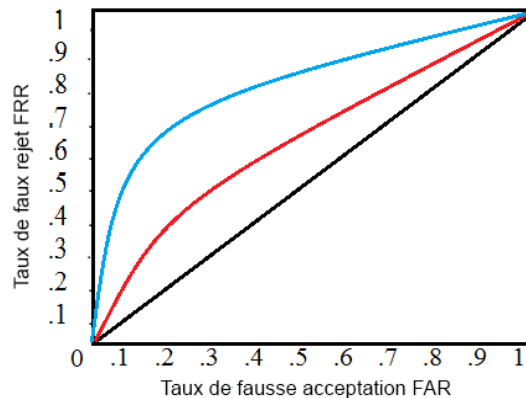
Le taux d'erreur égal (EER) est utilisé pour prédéterminer les valeurs de seuil pour son taux d'acceptation faux et son taux de rejet faux. Lorsque les taux sont égaux à $FAR = FRR$, la valeur commune est appelée taux d'erreur égal. La valeur indique que la proportion de fausses acceptations est égale à la proportion de faux rejets. Plus la valeur du taux d'erreur égal est faible, plus la précision du système biométrique est élevée.

I.5.4.4 Courbe ROC (Receiver Operating Characteristic Curve)

Une courbe ROC trace le FRR (en ordonnée) par rapport à la FAR (en abscisse). Plus cette courbe tend à épouser la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé.

La courbe ROC suivant montre deux tests. Le test rouge est plus proche de la diagonale est donc moins précis que le test bleu.

Figure I.8 : Un exemplaire d'une courbe ROC



I.6 Conclusion

La biométrie est la reconnaissance automatisée des individus en fonction de leurs caractéristiques comportementales et biologiques. Il repose sur la présomption que les individus se distinguent physiquement et comportementalement de plusieurs manières.

L'objectif principal de cet état d'art est de donner un aperçu sur la biométrie et ses propriétés les plus importantes. La reconnaissance du visage, les algorithmes utilisés et les différentes mesures de la performance d'un tel système sont présentés en détails.

Dans le chapitre suivant nous allons décrire en détail les méthodes d'extraction de caractéristiques utilisées dans la conception du système de reconnaissance de visage proposé dans cette étude.

Chapitre II : Système de reconnaissance de visage

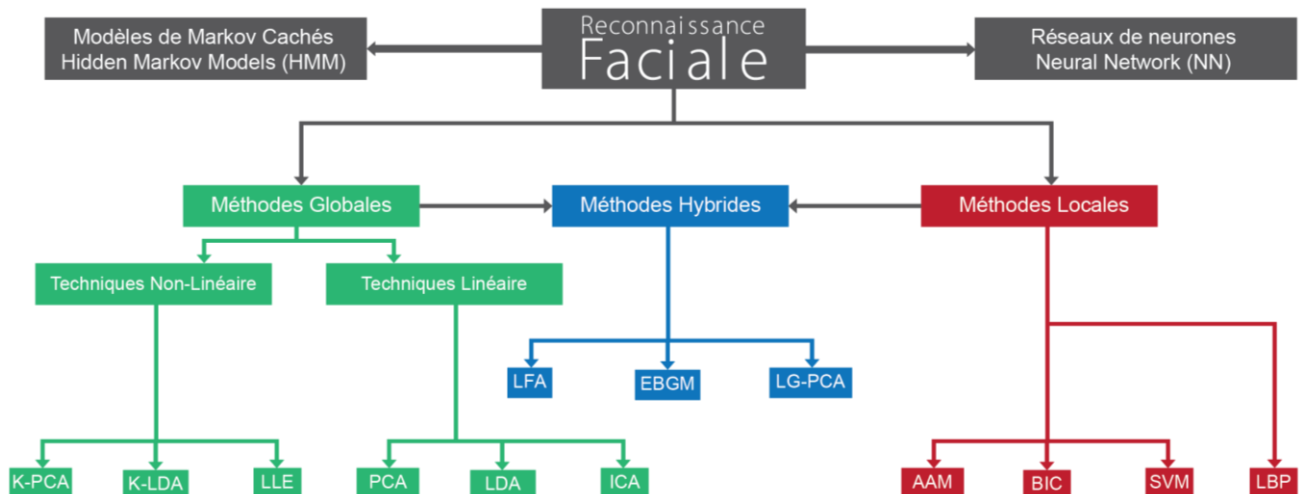
II.1 Introduction

La reconnaissance des visages est l'une des technologies biométriques les plus utilisées et les plus adaptées. De nombreuses méthodes de reconnaissance de visages ont été proposées au cours dernières années. L'étape fondamentale dans tout système de reconnaissance faciale est celle d'extraction de caractéristique. Dans ce chapitre nous allons premièrement présenter en détail cette étape fondamentale. Puis on expliquera les trois méthodes utilisées dans ce travail, à savoir la méthode les motifs binaires locaux (LBP) ^[1] LBP (Local Binary Pattern) et ses deux variantes LPQ ^[2] (Local Phase Quantization) et MRELBP ^[3] (Median Robust Extended Local Binary Pattern). Ensuite on abordera le problème d'évaluation d'un tel système par la présentation des différentes métriques utilisées dans ce domaine.

II.2 Méthodes d'extraction de caractéristiques

L'extraction de caractéristique est une étape fondamentale dans un système de reconnaissance biométrique. Il s'agit d'extraire les caractéristiques du visage qui peuvent le rendre à la fois différent de celui des autres personnes et robuste aux variations de la personne elle-même. C'est l'information nécessaire pour que le visage d'une personne ne ressemble pas à celui d'une autre personne et en même temps qu'il ressemble à lui-même dans d'autres conditions d'acquisition. On distingue trois catégories de méthodes : les *méthodes globales*, les *méthodes locales* et les *méthodes hybrides* ^[10]. Le schéma de la *figure II.1* représente une classification détaillée de ces trois groupes.

Figure II.1 : Différents méthodes d'extraction de caractéristiques



II.2.1 Méthodes globales

Ces méthodes sont basées sur l'utilisation de la surface entière du visage pour l'extraction de caractéristiques sans prendre en compte ses points caractéristiques (comme les centres des yeux, les narines, le centre de la bouche, etc.). Leurs avantages principaux sont qu'elles sont relativement rapides à mettre en œuvre. En revanche, elles sont très sensibles aux variations d'éclaircement, de pose et

d'expression faciale. Parmi les approches les plus importantes réunies au sein de cette classe on trouve: l'Analyse en Composantes Principales (ACP ou *Eigen Faces*) [13], l'Analyse Discriminante Linéaire (ADL) [14].

II.2.2 Méthodes locales

Le principe de base consiste à construire un espace de caractéristiques local et à utiliser des filtres d'images appropriés, de manière à ce que les distributions des visages soient moins affectées par divers changements. L'avantage principal dans ce type de méthodes est de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Les méthodes LBP^[1] étudiées dans ce travail font partie de cette catégorie.

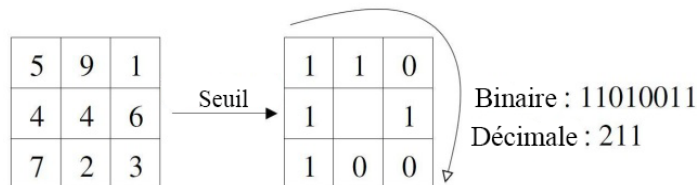
II.2.3 Méthodes hybrides

Les méthodes hybrides combinent les avantages des méthodes globales et locales en associant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairage et d'expressions faciales.

II.3 Motifs Binaires Locaux (Local Binary Patterns)

L'opérateur LBP^[1] d'origine étiquette les pixels d'une image avec des nombres décimaux, appelés motifs binaires locaux ou codes LBP, qui codent la structure locale autour de chaque pixel. Il procède ainsi, comme illustré à la *figure II.2* : Chaque pixel est comparé à ses huit voisins situés dans un voisinage 3x3 en soustrayant la valeur du pixel central ; Les valeurs strictement négatives qui en résultent sont codées avec 0 et les autres avec 1 ; Un nombre binaire est obtenu en concaténant tous ces codes binaires dans le sens des aiguilles d'une montre en commençant par celui en haut à gauche et la valeur décimale correspondante est utilisée pour l'étiquetage. Les nombres binaires dérivés sont appelés motifs binaires locaux ou codes LBP.

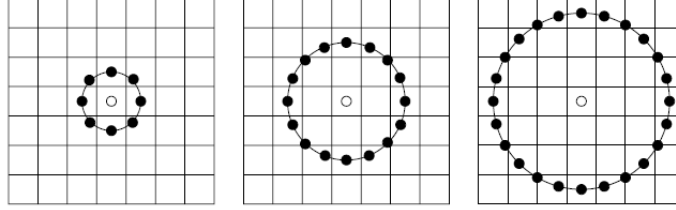
Figure II.2 : Un exemple de l'opérateur de base LBP



Une des limites de l'opérateur LBP de base est que son petit voisinage 3x3 ne peut pas capturer les caractéristiques dominantes avec des structures à grande échelle. Pour traiter la texture à différentes échelles, l'opérateur a ensuite été généralisé pour utiliser des voisinages de tailles différentes.

Un voisinage local est défini comme un ensemble de points d'échantillonnage régulièrement espacés sur un cercle centré sur le pixel à étiqueter. Les points d'échantillonnage ne faisant pas partie des pixels sont interpolés à l'aide d'une interpolation bilinéaire. Ainsi, en tenant compte de tout rayon et de tout nombre de points d'échantillonnage dans le voisinage. La *figure II.3* montre quelques exemples d'opérateur LBP étendu ^[20], où la notation (P, R) indique un voisinage de P points d'échantillonnage sur un cercle de rayon R .

Figure II.3 : Exemples d'opérateurs LBP étendus ^[20]: les voisinages circulaires (8,1), (16,2) et (24,3)



Formellement, étant donné un pixel situé en (x_c, y_c) , la LBP résultante peut être exprimée sous forme décimale de la manière suivante:

$$LBP_{P,R}(x_c, y_c) = \sum_{P=0}^{P-1} s(i_P - i_c) 2^P \quad 2.1$$

Où i_c et i_p sont respectivement les valeurs de niveau de gris du pixel central et P les pixels environnants dans le voisinage du cercle de rayon R , et la fonction $s(x)$ est définie comme suit:

$$s(x) = \begin{cases} 1 & \text{si } x \geq 0 \\ 0 & \text{si } x < 0 \end{cases} \quad 2.2$$

Selon la définition ci-dessus, l'opérateur LBP de base est invariant des transformations monotones en niveaux de gris préservant l'ordre d'intensité des pixels dans les voisinages locaux. L'histogramme des étiquettes LBP calculé sur une région peut être exploité en tant que descripteur de texture.

L'opérateur LBP (P, R) produit 2^P valeurs de sortie différentes, correspondant à 2^P motifs binaires différents formés par P pixels dans le voisinage. Si vous faites pivoter l'image, les pixels environnants de chaque voisinage se déplaceront de manière correspondante le long du périmètre du cercle, ce qui donnera une valeur LBP différente, à l'exception des motifs comportant uniquement des 1 et des 0. Afin de supprimer l'effet de rotation, une LBP invariante à la rotation est proposée dans :

$$LBP_{P,R}^i = \min\{ROR(LBP_{P,R}, i) | i = 0, 1, \dots, P - 1\} \quad 2.3$$

Où $ROR(x, i)$ effectue un décalage circulaire à droite sur le nombre de P -bits x , i fois. L'opérateur $LBP_{P,R}^i$ quantifie les statistiques d'occurrence de motifs invariants de rotation individuels correspondant à certaines micro-caractéristiques de l'image. Par conséquent, les motifs peuvent être

considérés comme un détecteur de caractéristiques. Cependant, il a été démontré qu'un tel opérateur LBP à invariance par rotation ne fournit pas nécessairement une information discriminante, car les fréquences d'apparition des motifs individuels incorporés dans $LBP_{P,R}^{ri}$ varient considérablement et la quantification brute des espaces angulaires à 45° .

Il a été démontré que certains modèles contiennent plus d'informations que d'autres. Il est possible d'utiliser uniquement un sous-ensemble de motifs binaires 2^P pour décrire la texture des images. Ojala et al. Nommé ces motifs '*motifs uniformes*'^[1], notés $LBP_{P,R}^{U2}$. Un modèle binaire local est appelé uniforme s'il contient au plus deux transitions de 0 à 1, ou inversement, lorsque la chaîne de bits correspondante est considérée comme circulaire. Par exemple, 00000000 (0 transitions) et 01110000 (2 transitions) sont uniformes alors que 11001001 (4 transitions) et 01010011 (6 transitions) ne le sont pas. On observe que les motifs uniformes représentent environ 90% de tous les motifs dans un voisinage $(8,1)$ et environ 70% dans un voisinage $(16,2)$ en images de texture.

II.4 Quantification de phase locale (Local Phase Quantization)

La deuxième méthode choisie pour l'extraction de caractéristique est la méthode LPQ^[2]. Son apport principal est son invariance au flou. Le flou est un problème courant dans un système de reconnaissance de visage. C'est une dégradation dû au mouvement de capture. Il est alors toujours souhaitable de pouvoir analyser le système de manière insensible au flou.

Cette méthode est basée sur la phase quantifiée de la Transformée de Fourier discrète (**D**iscrete **F**ourier **T**ransform **DFT**) calculée dans des fenêtres d'image locale, d'où son nom quantification de phase locale (LPQ).

Les codes produits par l'opérateur LPQ sont insensibles au flou symétrique central. L'opérateur LPQ s'applique à l'identification de la texture en la calculant localement à chaque emplacement de pixel et en présentant les codes obtenus sous forme d'histogramme. La génération des codes et de leurs histogrammes est similaire à la méthode LBP^[1]

II.4.1 Invariance du flou lors de la phase de transformation de Fourier

Dans le traitement numérique de l'image, le modèle discret de flou spatialement invariant d'une image originale $f(x)$ donnant une image observée $g(x)$ peut être exprimé par une convolution^[21], donnée par :

$$g(x) = (f * h)(x) \quad 2.4$$

Où $h(x)$ est la fonction d'étalement du point (Point Spread Function PSF) du flou, * désigne une convolution 2-D et x est un vecteur de coordonnées $[x, y]^T$. Dans le domaine de Fourier, cela correspond à :

$$G(u) = F(u).H(u) \quad 2.5$$

Où $G(u)$, $F(u)$ et $H(u)$ sont les transformées de Fourier discrètes (DFT) de l'image floue $g(x)$, de l'image d'origine $f(x)$ et de la PSF $h(x)$, et u est un vecteur de coordonnées $[u, v]^T$. On peut séparer les parties magnitude et phase de l'équation (2.5), ce qui entraîne :

$$|G(u)| = |F(u)| \cdot |H(u)| \quad \text{et} \quad \angle G(u) = \angle F(u) + \angle H(u) \quad 2.6$$

Si nous supposons que le flou PSF $h(x)$ est symétrique central, à savoir $h(x) = h(-x)$, sa transformée de Fourier a toujours une valeur réelle et par conséquent, sa phase n'est qu'une fonction à deux valeurs, donné par :

$$\angle H(u) = \begin{cases} 0 & \text{si } H(u) \geq 0 \\ \pi & \text{si } H(u) < 0 \end{cases} \quad 2.7$$

Cela signifie que :

$$\angle G(u) = \angle F(u) \quad \text{pour tout } H(u) \geq 0 \quad 2.8$$

En d'autres termes, la phase de l'image observée $\angle G(u)$ aux fréquences, où $H(u)$ est positif, est invariante du flou à symétrie centrale.

II.4.2 Transformation de Fourier à court terme en LPQ

La méthode de quantification de phase locale (LPQ) est basée sur la propriété d'invariance de flou du spectre de phase de Fourier décrite dans la Section passé. Il utilise les informations de phase locale extraites à l'aide de la 2-D DFT (Transformée de Fourier Discrète bidimensionnelle) ou, plus précisément, d'une transformée de Fourier à court terme (**Short-Term Fourier Transform STFT**) calculée sur un voisinage M -par- M \mathcal{N}_x rectangulaire à chaque position de pixel x de l'image $f(x)$ défini par :

$$F(u, x) = \sum_{y \in \mathcal{N}_x} f(x - y) e^{-j2\pi u^T y} = w_u^T f_x \quad 2.9$$

Où w_u est le vecteur de base de la 2-D DFT à la fréquence u , et f_x est un autre vecteur contenant tous les échantillons d'image M^2 de \mathcal{N}_x .

A partir de l'équation (6), un moyen efficace de mettre en œuvre le STFT consiste à utiliser des convolutions bidimensionnelle $f(x) * e^{-\pi j u^T x}$ pour tout u [23]. Puisque les fonctions de base sont séparables, le calcul peut être effectué en utilisant des convolutions unidimensionnelles pour les lignes et les colonnes successivement.

Dans LPQ, seuls quatre coefficients complexes sont pris en compte, correspondant aux fréquences bidimensionnelle $u_1 = [a, 0]^T$, $u_2 = [0, a]^T$, $u_3 = [a, a]^T$ et $u_4 = [a, -a]^T$, où a est une fréquence scalaire inférieure au premier passage à zéro de $H(u)$ qui satisfait à la condition (2.8). Laisser :

$$F_x^c = [F(u_1, x), F(u_2, x), F(u_3, x), F(u_4, x)], \quad \text{et} \quad 2.10$$

$$F_x = [Re\{F_x^c\}, Im\{F_x^c\}]^T \quad 2.11$$

Où $Re\{\cdot\}$ et $Im\{\cdot\}$ renvoient respectivement les parties réelle et imaginaire d'un nombre complexe. La matrice de transformation δ -par- M^2 correspondante est :

$$W = [Re\{w_{u1}, w_{u2}, w_{u3}, w_{u4}\}, Im\{w_{u1}, w_{u2}, w_{u3}, w_{u4}\}]^T \quad 2.12$$

Pour que :

$$F_x = Wf_x \quad 2.13$$

II.4.3 Analyse statistique des coefficients

Supposons que la fonction image $f(x)$ résulte d'un processus de Markov du premier ordre, dans lequel le coefficient de corrélation entre les valeurs de pixels adjacentes est ρ et la variance de chaque échantillon est σ^2 . Sans perte de généralité, on peut supposer que $\sigma^2 = 1$. En conséquence, la covariance entre les positions x_i et x_j devient :

$$\sigma_{ij} = \rho^{\|x_i - x_j\|} \quad 2.14$$

Où $\|\cdot\|$ désigne la norme L_2 , et la matrice de covariance de tous les M échantillons de \mathcal{N}_x peut être exprimée par

$$C = \begin{bmatrix} 1 & \sigma_{12} & \cdots & \sigma_{1M} \\ \sigma_{21} & 1 & \cdots & \sigma_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{M1} & \sigma_{M2} & \cdots & 1 \end{bmatrix} \quad 2.15$$

Par conséquent, la matrice de covariance du vecteur de coefficient de transformation F_x peut être obtenue à partir de :

$$D = WCW^T \quad 2.16$$

D n'est pas une matrice diagonale pour $\rho > 0$, ce qui signifie que les coefficients sont corrélés.

II.4.4 Décorrélation et quantification

Avant la quantification, les coefficients sont décorrélés, car les informations sont préservées de manière maximale dans la quantification scalaire si les échantillons à quantifier sont statistiquement indépendants ^[24]. En supposant une distribution gaussienne, l'indépendance peut être obtenue à l'aide d'une transformation de blanchiment :

$$G_x = V^T F_x \quad 2.17$$

Où V est une matrice orthonormée dérivée de la décomposition en valeurs singulières (Singular Value Decomposition **SVD**) de la matrice D qui est :

$$D = U \sum V^T \quad 2.18$$

Notez que V peut être résolu à l'avance pour une valeur fixe de ρ .

Ensuite, G_x est calculé pour toutes les positions d'image, c'est-à-dire $x \in \{x_1, x_2, \dots, x_N\}$, et les vecteurs résultants sont quantifiés à l'aide d'un simple quantificateur scalaire :

$$q_j = \begin{cases} 1, & \text{si } g_j \geq 0 \\ 0, & \text{autrement} \end{cases} \quad 2.19$$

Où g_j est la $j^{\text{ième}}$ composante de G_x . Les coefficients quantifiés sont représentés sous forme de valeurs entières comprises entre 0 et 255 à l'aide d'un codage binaire :

$$b = \sum_{j=1}^8 q_j 2^{j-1} \quad 2.20$$

Enfin, un histogramme de ces valeurs entières provenant de toutes les positions de l'image est composé et utilisé comme vecteur de caractéristiques à 256 dimensions dans la classification.

II.5 Médiane Robuste Etendu LBP (Median Robust Extended Local Binary Pattern)

Les motifs binaires locaux (LBP) ^[1] sont considérés parmi les caractéristiques de texture haute performance les plus efficaces en termes de calcul. Cependant, la méthode LBP est très sensible au bruit d'image et incapable de capturer les informations de macrostructure. Pour résoudre au mieux ces inconvénients, dans cette section, nous introduisons un autre descripteur pour la classification de la texture, la Médiane Robuste Etendu LBP (**Median Robust Extended LBP**). Différent de la LBP traditionnelle et de nombreuses variantes de la LBP, le MRELBP ^[3] compare les médianes d'image régionales plutôt que les intensités d'image brutes. Un descripteur de type LBP multi-échelle est calculé en comparant efficacement les médianes d'image sur un nouveau schème d'échantillonnage, capable de capturer des informations de texture de microstructure et de macrostructure. Une évaluation complète des ensembles de données de référence révèle les hautes performances du MRELBP - robustes aux variations d'échelle de gris, aux changements de rotation et au bruit - mais à un faible coût en calcul ^[3]. Plus important encore, il est démontré que MRELBP est très résistant au bruit d'image, y compris le bruit gaussien, le flou gaussien, le bruit sel et poivre (Salt-and-Pepper noise) et la corruption aléatoire de pixels.

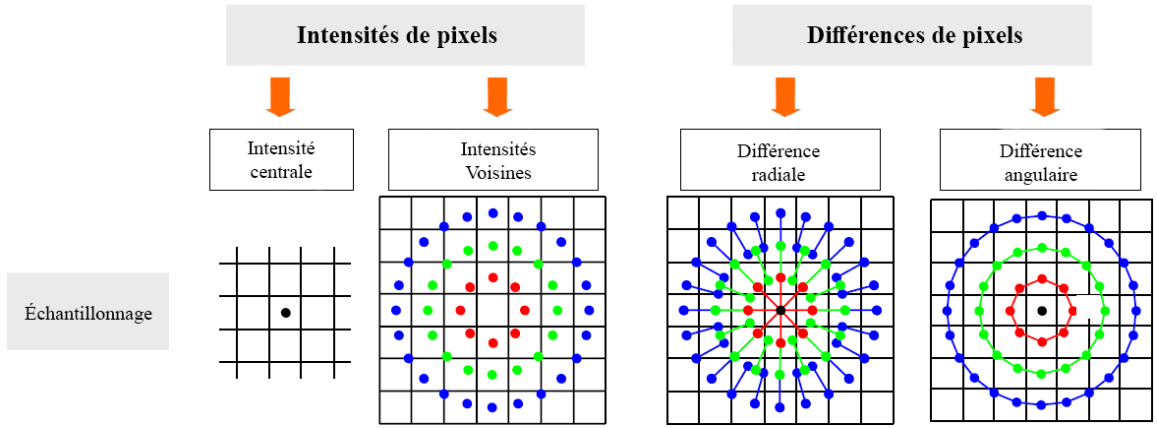
Tout d'abord, nous devons parler du descripteur ELBP (**Extended Local Binary Pattern**) ^[20]. Qui est la base du MRELBP.

II.5.1 Motif Binaire Local Étendu (Extended Local Binary Pattern)

Quatre différents descripteurs de type LBP (illustrés à la *Figure II.4*) sont utilisés :

- LBP basé sur l'Intensité Centrale (LBP-CI - Center Intensity)
- LBP basé sur l'Intensité Voisines (LBP-NI - Neighborhood Intensity)
- LBP basée sur la Différence Radiale (LBP-RD - Radial Difference)
- LBP basée sur la Différence Angulaire (LBP-AD - Angular Difference).

Figure II.4 : Vue d'ensemble de l'approche



Avec la même forme que les codes LBP conventionnels, ils peuvent donc être facilement combinés pour former des histogrammes conjoints afin de représenter des images texturées.

Les proportions des motifs uniformes de LBP-AD étaient trop petites et inadéquates pour fournir une description fiable et significative des images de texture. C'est pour cela qu'il n'a pas été utilisé.

a. ELBP-CI (LBP basé sur l'Intensité Centrale)

$$ELBP_CI(x_c) = s(x_c - \beta) \tag{2.21}$$

$$\beta = \frac{1}{N} \sum_{c=0}^N x_c \tag{2.22}$$

b. ELBP-NI (LBP basé sur l'Intensité Voisines)

$$ELBP_NI_{r_2,8}(x_c) = \sum_{n=0}^7 s(x_{r_2,8,n} - \beta_{r_2,8}) 2^n \tag{2.23}$$

$$\beta_{r_2,8} = \frac{1}{8} \sum_{n=0}^7 x_{r_2,8,n} \tag{2.24}$$

c. *ELBP-RD (LBP basée sur la Différence Radiale)*

$$ELBP_{RD_{r_2, r_1, 8}}(x_c) = \sum_{n=0}^7 s(x_{r_2, 8, n} - x_{r_1, 8, n})2^n \quad 2.25$$

Il a été montré que la distribution de probabilité conjointe de ELBP-CI, ELBP-NI et ELBP-RD (collectivement désignées ELBP) produit de bonnes performances de classification de la texture, avec toutefois les inconvénients de :

- Sensibilité au flou et au bruit de l'image
- Échec de capture de la macrostructure de texture
- Avoir une dimensionnalité de fonctionnalité élevée.

II.5.2 Descripteur MRELBP

Afin de surmonter les faiblesses de l'ELBP, nous proposons une approche multirésolution théoriquement très simple, de grande qualité et efficace, le motif binaire médiane robuste étendu (MRELBP).

Le descripteur ELBP est maintenant modifié pour que les intensités de pixels individuelles aux points échantillonnés soient remplacées par des valeurs médianes, où $\emptyset(X_{r,p,w_r,n})$ est la médiane de tous les pixels du patch local $X_{r,p,w_r,n}$ centré sur $x_{r,p,n}$. Toutes les autres étapes de prétraitement et de post-traitement sont maintenues cohérentes avec ELBP.

Formellement, les nouveaux descripteurs proposés MRELBP-CI, MRELBP-NI et MRELBP-RD sont définis comme suit :

a. *MRELBP-CI (MRELBP basé sur l'Intensité Centrale)*

$$MRELBP_CI(x_c) = s(\emptyset(X_{c,w}) - \mu_w) \quad 2.26$$

Où $X_{c,w}$ désigne le pièce local de taille $w \times w$ centré sur le pixel central x_c considéré, la fonction $\emptyset(X)$ est la valeur médiane sur X , et μ_w est la moyenne de $\emptyset(X_{c,w})$ sur toute l'image.

b. *MRELBP-NI (MRELBP basé sur l'Intensité Voisines)*

$$MRELBP_NI_{r,p}(x_c) = \sum_{n=0}^{P-1} s(\emptyset(X_{r,p,w_r,n}) - \mu_{r,p,w_r})2^n \quad 2.27$$

$$\mu_{r,p,w_r} = \frac{1}{P} \sum_{n=0}^{P-1} X_{r,p,w_r,n} \quad 2.28$$

Où $x_{r,p,w_r,n}$ désigne le pièce de taille $w_r \times w_r$ centré sur le pixel voisin $x_{r,p,n}$.

c. **MRELBP-RD (MRELBP basée sur la Différence Radiale)**

$$MRELBP_{RD,r,r-1,p,w_r,w_{r-1}}(x_c) = \sum_{n=0}^{P-1} s(\phi(X_{r,p,w_r,n}) - \phi(X_{r-1,p,w_{r-1},n}))2^n \quad 2.29$$

Où $X_{r,p,w_r,n}$ désigne les zones centrées sur les pixels voisins $x_{r,p,n}$, qui sont les voisins espacés de manière circulaire et uniforme du pixel central x_c sur le rayon r .

II.6 Classification

La classification constitue la dernière étape dans le processus de reconnaissance. Son objectif dans un système de reconnaissance consiste à identifier à quelle classe appartient chaque visage en faisant une comparaison entre les caractéristiques extraites du visage actuel et de celui enregistré dans la base de données.

II.6.1 Classifieur k-NN

Le classifieur k -NN convient mieux à la classification des personnes en fonction de leurs images en raison de son temps d'exécution et de sa précision plus courts que ceux des méthodes couramment utilisées, notamment le HMM (Hidden Markov Model) et les méthodes Kernel [25]. Bien que des méthodes telles que les algorithmes SVM (Support Vector Machine) et Adaboost soient plus précises que le classifieur k -NN, le classifieur k -NN possède un temps d'exécution plus court donc dominant par rapport au SVM.

Dans ce type de classifieur, une image dans l'ensemble de test est reconnue en lui attribuant l'étiquette du point le plus proche dans l'apprentissage. La métrique de distance euclidienne est souvent choisie pour déterminer la proximité entre les points de données en k -NN. La distance euclidienne est donnée par :

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2} \quad 2.30$$

Cette distance euclidienne est définie par défaut pour un classifieur k -NN.

II.6.2 Algorithme de k-NN

L'algorithme de k-voisin le plus proche (k -NN) est une méthode de classification des objets basée sur des exemples d'apprentissage les plus proches dans l'espace des fonctions. k -NN est un type d'apprentissage basé sur une instance, ou apprentissage paresseux (lazy learning), dans lequel la fonction est uniquement approximée localement et tous les calculs sont différés jusqu'à la classification.

L'algorithme k-voisin le plus proche est l'un des plus simples de tous les algorithmes d'apprentissage automatique : un objet est classé par le vote majoritaire de ses voisins, l'objet étant

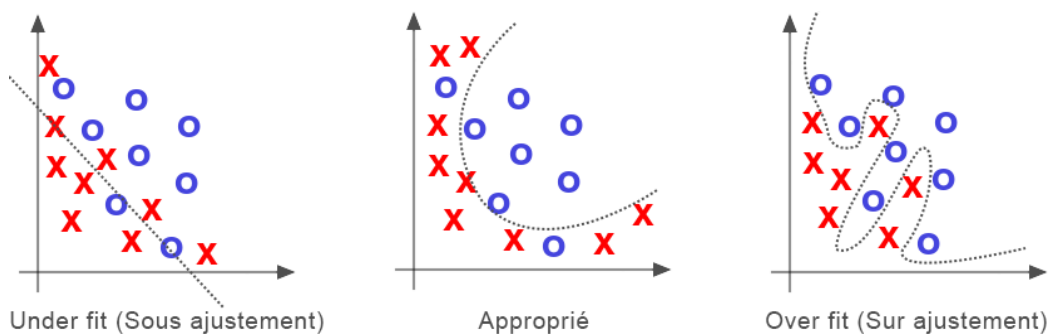
affecté à la classe la plus courante parmi ses k plus proches voisins (k est un entier positif, typiquement petit). Si $k = 1$, l'objet est simplement affecté à la classe de son plus proche voisin.

- a. Chaque valeur de pixel de données dans l'ensemble de données a une étiquette de classe dans l'ensemble, Classe = $\{c_1 \dots c_n\}$.
- b. Les k points les plus proches voisins (k étant le nombre de voisins) sont ensuite trouvés en analysant la matrice de distance.
- c. Les points k de données les plus proches sont ensuite analysés pour déterminer quelle étiquette de classe est la plus courante parmi l'ensemble.
- d. L'étiquette de classe la plus courante est ensuite affectée au point de données en cours d'analyse.

II.6.3 Validation croisée

La validation croisée est une technique de validation de modèle permettant d'évaluer la manière dont les résultats d'une analyse statistique (modèle) se généraliseront à un ensemble de données indépendant. Elle est principalement utilisée dans des contextes où l'objectif est la prédiction et on souhaite estimer la précision avec laquelle un modèle prédictif fonctionnera. Alors son objectif consiste à définir un jeu de données pour tester le modèle en phase d'apprentissage (c'est-à-dire un jeu de données de validation) afin de limiter les problèmes tels que sur-ajustement, sous-ajustement (*figure II.5*). En d'autre terme elle permet d'évaluer la qualité du modèle.

Figure II.5 : La différence entre Underfit et Overfit



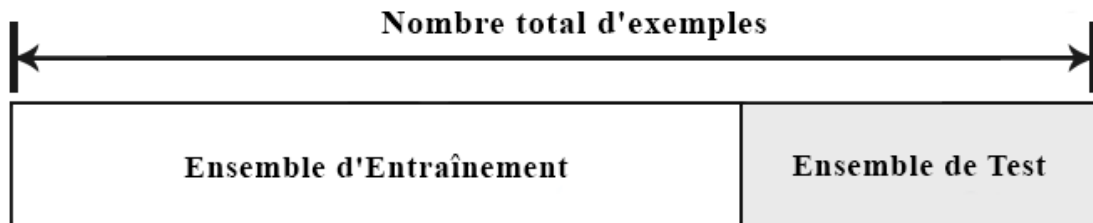
II.6.3.1 Différentes stratégies de validation

En règle générale, différentes stratégies de validation existent en fonction du nombre de divisions effectuées dans l'ensemble de données.

A. Holdout : La méthode du Holdout est le type le plus simple de validation croisée. L'ensemble de données est séparé en deux ensembles, appelés ensemble d'entraînement et ensemble d'essai. L'approximation de la fonction s'adapte à une fonction à l'aide de l'ensemble d'entraînement uniquement. Ensuite, il est demandé à l'approximation de prédire les valeurs de sortie pour les données

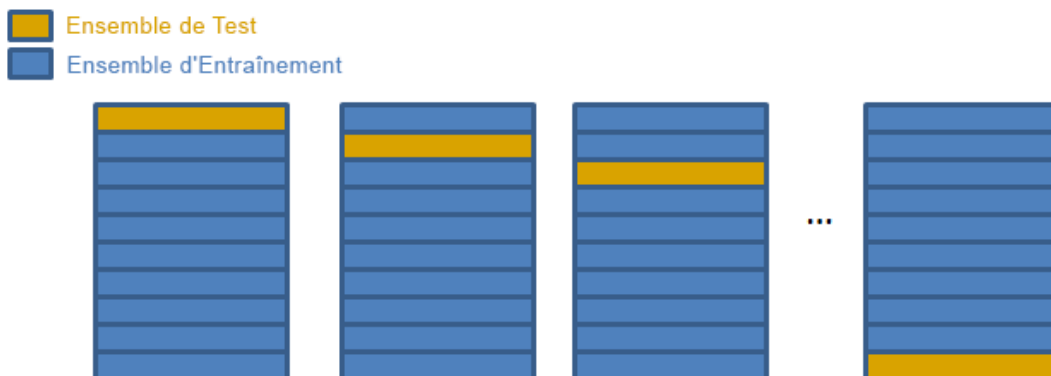
de l'ensemble de test (il n'a jamais vu ces valeurs de sortie avant). Les erreurs qu'il commet s'accumulent comme auparavant pour donner l'erreur moyenne absolue du jeu d'essais, qui est utilisée pour évaluer le modèle.

Figure II.6 : Train / test division ou Holdout (2 groupes)



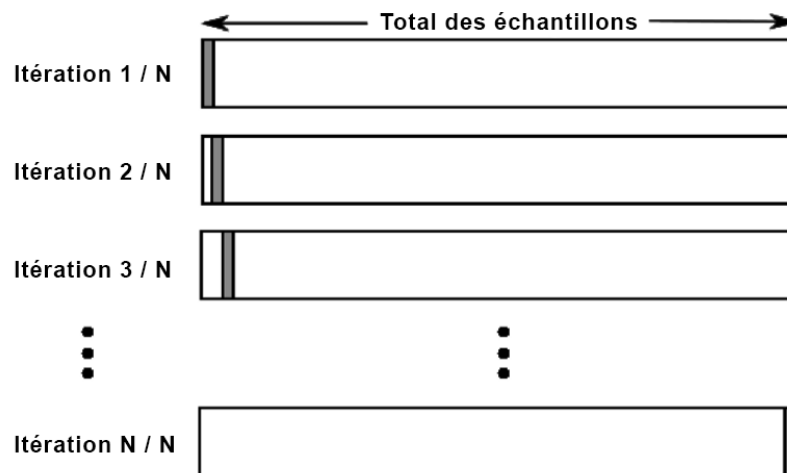
B. K-fold : La validation croisée de K-fold est un moyen d'améliorer la méthode du Holdout. L'ensemble de données est divisé en k sous-ensembles et la méthode de Holdout est répétée k fois. À chaque fois, l'un des k sous-ensembles est utilisé comme ensemble de test et les $k-1$ autres sous-ensembles sont regroupés pour former un ensemble d'entraînement. Ensuite, l'erreur moyenne sur tous les k essais est calculée. Chaque point de données doit être dans un ensemble de test exactement une fois, et doit être dans un ensemble d'entraînement $k-1$ fois. La variance de l'estimation résultante est réduite lorsque k augmente.

Figure II.7 : Schéma illustrant la division en k sous-ensemble (k groupes)



C. Leave-One-Out (LOO) : La validation croisée LOO est la validation croisée K-fold à son extrême logique, avec K égal à N , le nombre de points des données dans l'ensemble. Cela signifie que N fois séparés, l'approximation de la fonction est entraînée sur toutes les données à l'exception d'un point et une prédiction est faite pour ce point. Comme auparavant, l'erreur moyenne est calculée et utilisée pour évaluer le modèle. L'évaluation donnée par une erreur de validation croisée (Leave-One-Out Cross Validation 'LOO-XVE') est bonne, mais au premier passage, elle semble très coûteuse à calculer.

Figure II.8 : Schéma illustrant comment fonctionne la méthode LOO



II.6.4 Matrice de confusion

La matrice de confusion est utilisée pour résumer, décrire ou évaluer les performances d'une tâche ou d'un modèle de classification binaire.

Le concept clé de la matrice de confusion est qu'elle calcule le nombre de prédictions correctes et incorrectes, qui est ensuite résumée avec le nombre de valeurs de comptage et leur répartition dans chaque classe. Il montre finalement la voie dans laquelle le modèle de classification est confus lorsqu'il fait des prédictions. On peut l'appeler également une matrice d'erreur.

On trouve ci-dessous la disposition des paramètres de la matrice de confusion :

Tableau II.1: Tableau illustrant la matrice de confusion

Matrice de Confusion		Réelle	
		P	N
Prédit	P	TP	FP
	N	FN	TN

- *Positive (P)* : le réel est positif.
- *Negative (N)* : la réalité n'est pas positive.
- *True Positive (TP)* : la valeur réelle est positive et devrait être positive.
- *False Negative (FN)* : la valeur réelle est positive, mais prédite négative.
- *True Negative (TN)* : le nombre réel est négatif et il est prévu que ce soit négatif.
- *Faux Positif (FP)* : le nombre réel est négatif, mais il est prédit positif.

La liste des taux qui sont calculés à partir d'une matrice de confusion pour un classifieur :

- *Taux d'erreur de classification ou taux d'erreur* : Dans l'ensemble, combien de fois c'est faux ?

$$\frac{FN + FP}{total} \quad 2.31$$

- *Sensibilité* : Quand c'est effectivement le cas, à quelle fréquence le prédit-il ?

$$\frac{TP}{TP + FN} \quad 2.32$$

- *Spécificité* : Quand c'est en fait non, à quelle fréquence le prédit-il ?

$$\frac{TN}{TN + FP} \quad 2.33$$

II.7 Conclusion

Dans ce chapitre, nous avons présenté le problème d'extraction de caractéristiques pour un système de reconnaissance de visage ainsi que les moyens d'évaluation de ce dernier. On a énuméré les trois méthodes d'extraction utilisés dans ce mémoire à savoir la méthode LBP et ses deux variantes LPQ et MRELBP. Dans le chapitre suivant, nous allons passer à la présentation des résultats de la mise au point du système proposé.

Chapitre III : Evaluation du système

III.1 Introduction

Afin de mesurer les performances d'un système de reconnaissance de visages, les scientifiques ont établi un certain nombre de règles communes permettant de disposer les mêmes critères d'évaluation. Ces critères s'appliquent sur des bases de données également communes et partagées par l'ensemble de la communauté scientifique.

Dans ce chapitre, nous présenterons les différents tests du système de reconnaissance proposé et détaillé dans le chapitre 2 effectués sur les bases de données sélectionnées. Cela va nous permettre de montrer la puissance des méthodes d'extraction de caractéristiques et si la méthode peut représenter le contenu de l'image de la manière la plus pertinente possible. La puissance de ces méthodes sera déterminée par les performances du système déjà discuté au chapitre 2.

III.2 Bases des données

Lors de l'analyse comparative d'un algorithme, il est recommandé d'utiliser un ensemble de données de test standard. Cet ensemble standard permet de comparer directement les différents résultats obtenus par les chercheurs. Bien que de nombreuses bases de données soient actuellement utilisées, le choix de la base de données appropriée à utiliser doit être effectué en fonction de la tâche donnée (vieillesse, expressions, éclairage, etc.). Ce travail utilise trois bases de données : FERET, ORL et FEI.

III.2.1 Base de données de FERET

Le programme FERET visait à établir une grande base de données d'images faciales, recueillies indépendamment des développeurs de l'algorithme. Dr Harry Wechsler de l'Université George Mason a été choisi pour diriger la collecte de cette base de données. Les images ont été collectées dans un environnement semi-contrôlé. Afin de maintenir un certain degré de cohérence dans la base de données, la même configuration physique a été utilisée lors de chaque session de photographie. La base de données FERET a été constituée en 15 sessions entre août 1993 et juillet 1996. Elle contient 1564 ensembles d'images pour un total de 14 126 images comprenant 1199 personnes et 365 séries d'images en double. Pour certaines personnes, plus de deux ans s'étaient écoulés entre la première et la dernière séance, certains sujets ayant été photographiés à plusieurs reprises. Ce laps de temps était important car il permettait d'étudier, pour la première fois, les changements d'apparence d'un sujet sur une année^[26].

Pour le cas de notre travail, on s'est limité à un total de 300 images comprenant 100 personnes, chacune avec 3 images.

Figure III.1 : Aperçu de la base de données FERET



III.2.2 Base de données de ORL

Base de données ORL des visages, contient une série d'images de visages prises entre avril 1992 et avril 1994 au laboratoire. Elle a été utilisée dans le cadre d'un projet de reconnaissance de visage réalisé en collaboration avec le groupe de discours, vision et robotique du département d'ingénierie de l'université de Cambridge.

Dix images différentes de chacun des 40 sujets distincts. Pour certains sujets, les images ont été prises à des moments différents, en modifiant l'éclairage, les expressions du visage (yeux ouverts / fermés, souriant / pas souriant) et les détails du visage (lunettes / pas de lunettes). Toutes les images ont été prises sur un fond sombre et homogène, les sujets étant dans une position verticale et frontale (avec une tolérance pour certains mouvements latéraux). Une image d'aperçu de la base de données de visages de la *figure III.2* ^[27].

Figure III.2 : Aperçu de la base de données ORL



III.2.3 Base de données de FERET

La base de données de visages FEI est une base de données de visages brésilienne contenant un ensemble d'images de visages prises entre juin 2005 et mars 2006 au Laboratoire d'intelligence artificielle de FEI, situé à São Bernardo do Campo, à São Paulo, au Brésil. Il y a 14 images pour 200 personnes, soit un total de 2800 images.

Toutes les images sont colorées et prises sur un fond blanc et homogène dans une position frontale verticale avec une rotation du profil d'environ 180 degrés. L'échelle peut varier d'environ 10% et la taille d'origine de chaque image est de 640x480 pixels.

Tous les visages sont principalement représentés par les étudiants et le personnel de FEI, âgés de 19 à 40 ans, avec une apparence et une coiffure distinctes. Le nombre de sujets masculins et féminins est exactement le même et égal à 100. La figure III. 3 quelques exemples de variations d'image de la base de données de visages FEI^[28].

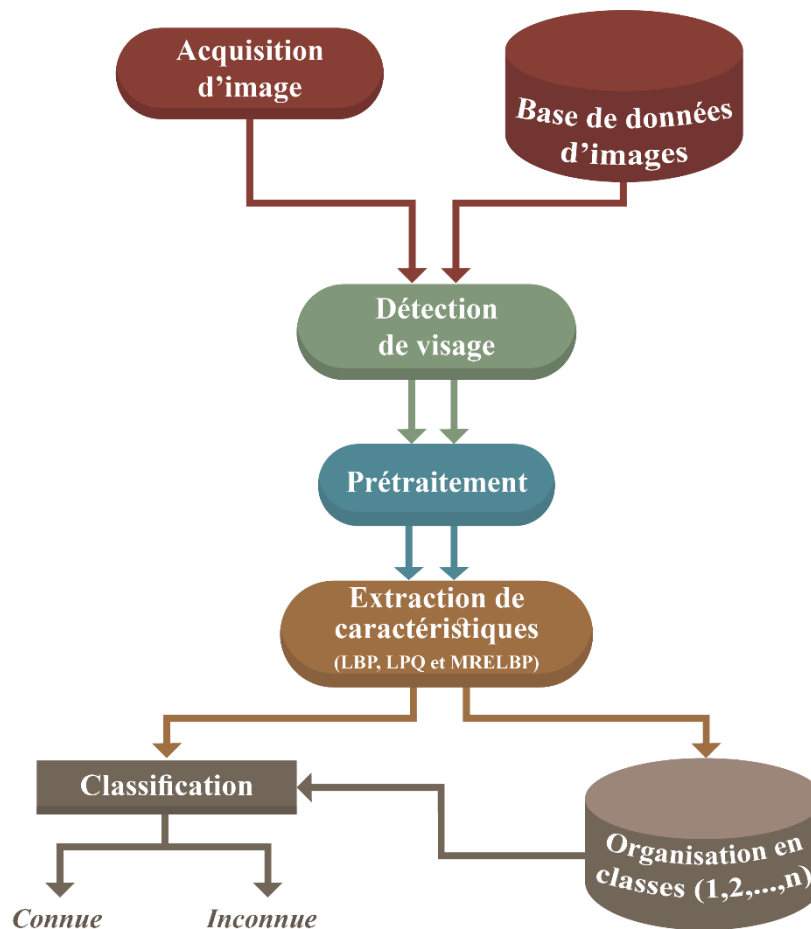
Figure III.3 : Aperçu de la base de données FEI



III.3 Algorithme du système

Un système de reconnaissance faciale ce passe par plusieurs étapes. L'algorithme de la reconnaissance faciale dans notre travail est illustré sur la *figure III.4*. Notons que cette algorithme est évalué théoriquement sur les bases de données déjà citées, puis utilisé dans une réalisation pratique à base d'Arduino. Au départ l'image initiale est soit capturée à l'aide d'une caméra (le cas de la réalisation pratique détaillée au chapitre 4) soit elle appartient à la base de données pour évaluation du système (le cas du chapitre en cours). La phase suivante est celle de prétraitement dont l'objectif est amélioration de sa qualité (accentuation du contraste ...). Les caractéristiques sont ensuite extraites en utilisant des méthodes appropriées. Ces caractéristiques sont ensuite classées à l'aide d'un algorithme de classification approprié. Dans la section 4, nous discuterons les résultats des trois méthodes d'extraction de caractéristiques utilisées.

Figure III.4 : Schéma fonctionnel du système général de reconnaissance de visage



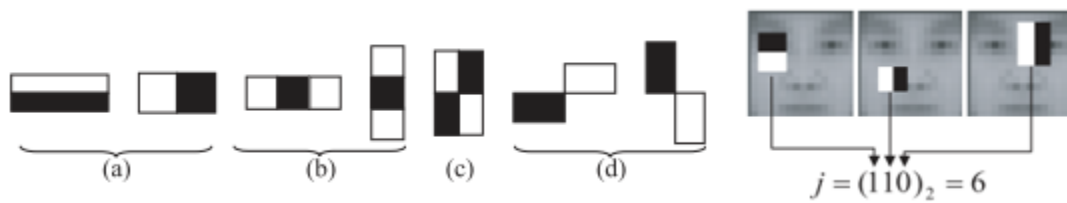
III.3.1 Détection de visage

La détection des objets et spécialement des visages est l'une des technologies informatiques reliées au traitement de l'image et à la vision par ordinateur. Son utilité se manifeste dans différents domaines tel que de la vidéosurveillance qui fait l'objectif de l'application proposée. Le principal objectif dans ce cas est de déterminer s'il y a un visage dans une image ou non. Les premières difficultés rencontrées consistent à détecter les visages sont les variations de pose (vue de profil, de face), d'expression, de rotation du visage et d'illumination

De nombreux travaux d'étude ont été proposés dans le domaine de la reconnaissance faciale et de la détection des visages. Le détecteur de Viola-Jones a révolutionné ce domaine de la faite qu'il est capable de détecter les visages en temps réel et avec une grande précision.

La détection VJ consiste à appliquer plusieurs faibles classifieurs en cascade (d'où le nom alternatif *cascade classifier* de l'algorithme) qui ont été entraînés à progressivement valider avec de plus en plus de rigueur la présence de caractéristiques Haar bien précises et qui représentent la réponse typique d'un visage. Des exemples de ce type de caractéristiques Haar sont présentés à la *figure III.5*. Plus de détails peuvent se trouver dans la référence [29].

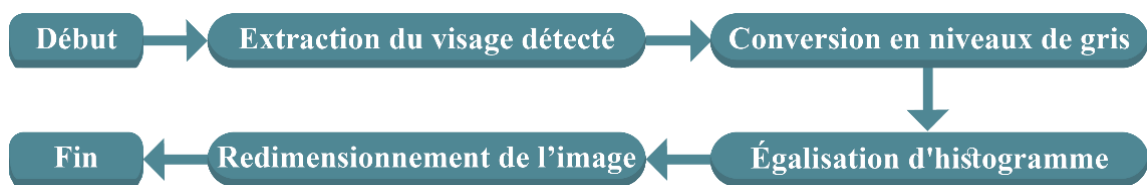
Figure III.5 : Exemples de caractéristique de Haar [29]



III.3.2 Prétraitement

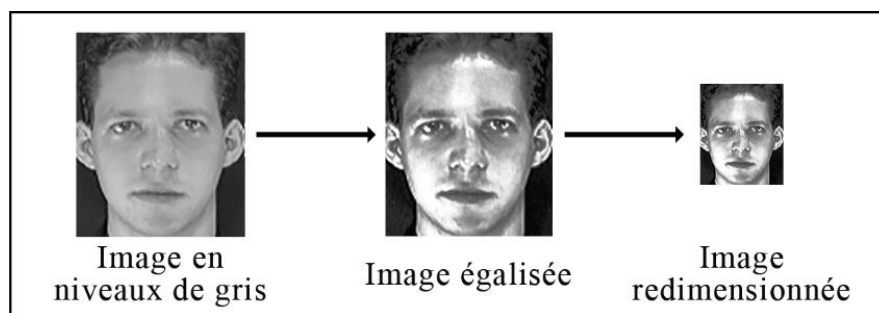
La qualité de l'image joue un rôle essentiel dans l'augmentation du taux de reconnaissance des visages. Une image de bonne qualité donne un meilleur taux de reconnaissance que les images bruitées. Il est plus difficile d'extraire des caractéristiques d'images aussi bruitées, ce qui réduit le taux de reconnaissance des visages. Pour surmonter les problèmes dus à une image de mauvaise qualité, un prétraitement est toujours effectué avant d'extraire les caractéristiques de l'image.

Figure III.6 : Différentes étapes du prétraitement



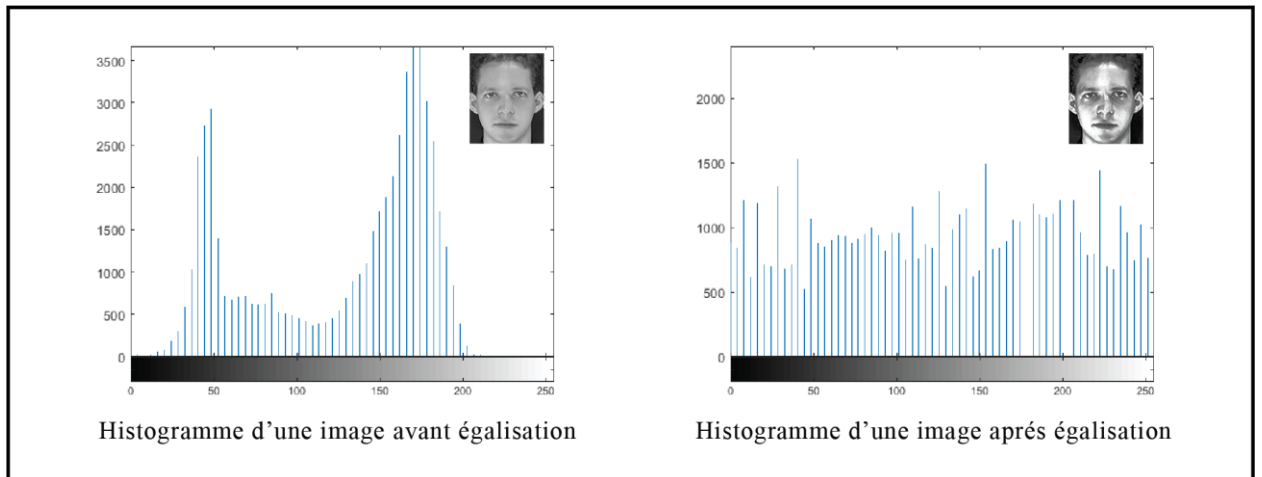
La *figure III.6* montre les approches de base de prétraitement utilisées dans nos simulations. L'extraction du visage détecté dans la partie précédente, puis l'image d'entrée en couleur est convertie en image à niveau de gris. À l'aide de la fonction MATLAB 'histeq', nous effectuons l'égalisation de l'histogramme. L'image est ensuite redimensionnée pour répondre à l'exigence (figure III.7)

Figure III.7 : Exemple du prétraitement de l'image



La *figure III.8* montre l'apport de l'opération d'égalisation d'histogramme sur la qualité de l'image.

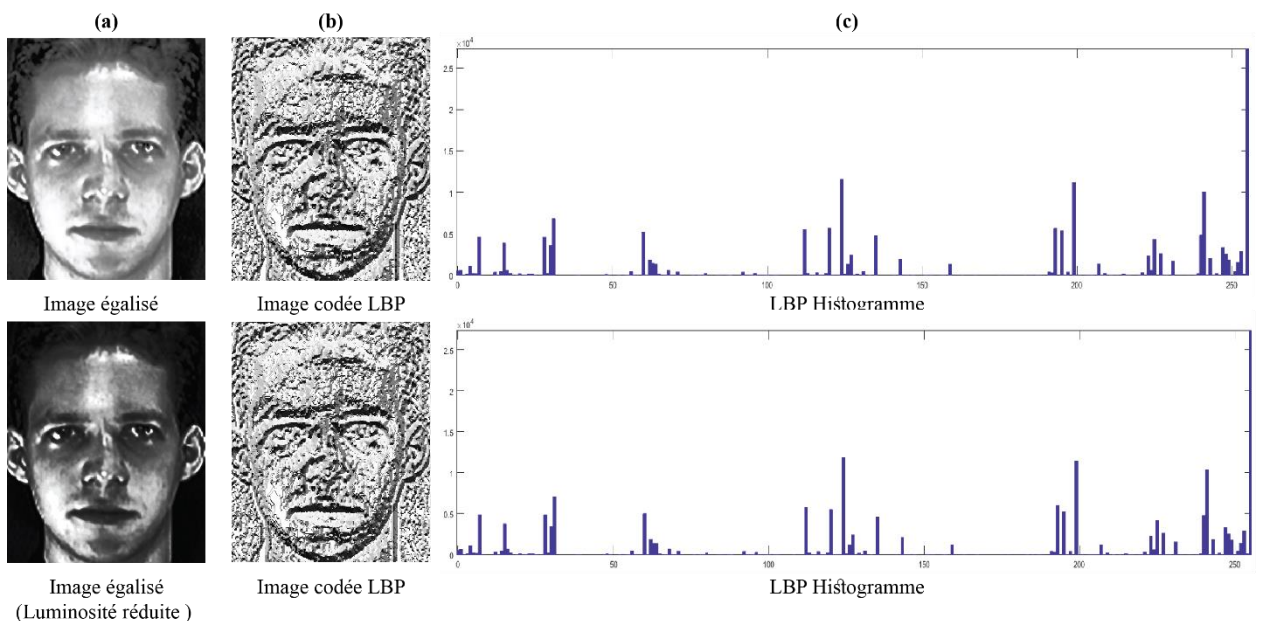
Figure III.8 : Schéma illustrant la différence entre un histogramme égalisé et un histogramme non égalisé



III.3.3 Extraction de caractéristiques

L'étape clé d'un système de reconnaissance de visages est bien celle d'extraction de caractéristiques. En fait il est fort nécessaire de représenter ces visages dans un hyper-espace augmenté de caractéristiques, dont des classifieurs entraînés à partir d'exemples appropriés pourraient classifier adéquatement. Dans ce travail, nous avons utilisé trois extracteurs comme déjà cité au chapitre 2 (LBP, LPQ, et MRELBP). Sur la *figure III.9*, on donne un exemple sur l'obtention du vecteur de caractéristique par LBP ainsi que sa résistance à l'illumination. On obtient le même histogramme après le changement d'illumination. Chose qui confirme la robustesse de la méthode LBP à l'illumination.

Figure III.9 : Image égalisée (a), traitée par l'opérateur LBP (b) puis l'histogramme LBP (c)



III.4 Résultats expérimentales

Les sous-sections qui suivront par la suite présentent les mesures de performances qui sont employées dans cette étude et les résultats obtenus afin d'évaluer la qualité de la reconnaissance de visages des systèmes à travers les méthodes LBP, LPQ et MRELBP. L'implémentation a été effectuée sous **MATLAB R2019a** sur différents types d'images issues des différentes bases de données. On s'est basé sur le calcul du taux de reconnaissance, FPR (**F**alse **P**ositive **R**ate), FNR (**F**alse **N**egative **R**ate), TPR (**T**ru **P**ositive **R**ate) et TNR (**T**ru **N**egative **R**ate) et les courbes ROC correspondantes à chaque méthode d'extraction.

III.4.1 Evaluation globales pour la Base de données FERET

Nous avons modifié cette très grande base de données en fonction de nos besoins, en la limitant à un total de 300 images comprenant 100 personnes, chacune avec 3 images. Ensuite, nous verrons les résultats lors de l'application de différentes méthodes d'extraction de caractéristiques. On a effectué cette modification de la base de données pour tester ces méthodes d'extraction avec un petit ensemble d'images par personne.

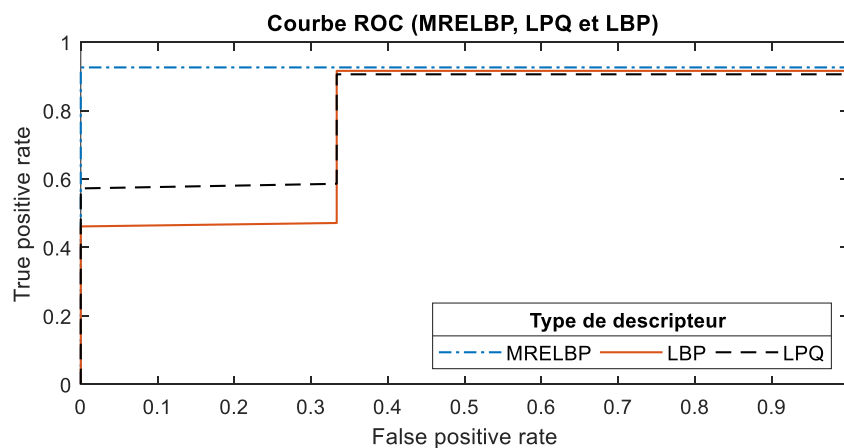
Dans le *tableau III.1* on a présenté les différents taux calculés de la base de données.

Tableau III.1 : Résultat de la base de données FERET

	TPR (%)	FPR (%)	TNR (%)	FNR (%)	Taux de reconnaissance (%)
LBP	30.6099	0.5639	99.4361	69.3901	65.0230
LPQ	58.7028	0.3753	99.6247	41.2972	79.1638
MRELBP	60.5716	0.3710	99.6290	39.4284	80.1003

Pour visualiser les performances globales de ces méthodes, nous avons tracé la courbe ROC pour différentes méthodes (MRE LBP, LPQ et LBP), comme indiqué dans la figure suivante.

Figure III.10 : Courbe ROC présentant les trois différents méthodes (MRELBP, LPQ et LBP)



III.4.2 Evaluation globales pour la base de données ORL

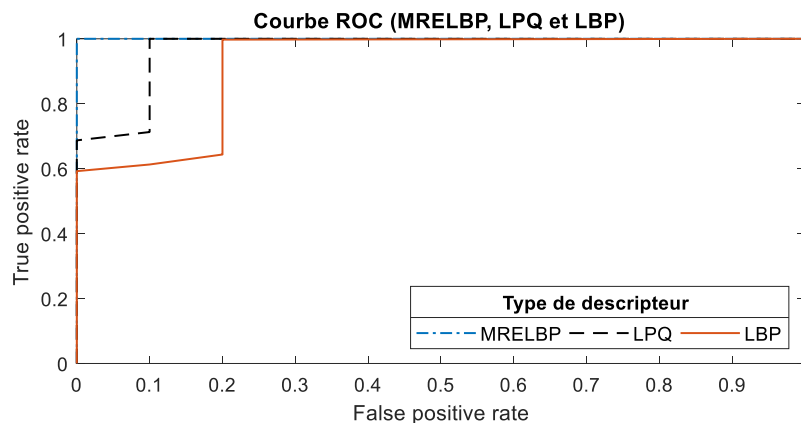
La base de donnée ORL présente 10 images pour chaque individu, au contraire de la base de donnée FERET le nombre d'images par personne est assez élevé et ces différentes images présente une légère variation de position ce qui aide l'algorithme à mieux apprendre et par conséquent améliore les résultats de la classification. Le *tableau III.2* présente les différents taux calculés de cette base de données.

Tableau III.2 : Résultat de la base de données ORL

	TPR (%)	FPR (%)	TNR (%)	FNR (%)	Taux de reconnaissance (%)
LBP	91.4533	0.1233	99.8767	8.5467	95.6650
LPQ	97.8244	0.0821	99.9179	2.1756	98.8712
MRELBP	99.4907	0.0157	99.9843	0.5093	99.7375

La prochaine courbe ROC nous aide à voir la performance globale du système avec chaque méthode utilisée

Figure III.11 : Courbe ROC présentant les trois différents méthodes (MRELBP, LPQ et LBP)



III.4.3 Evaluation globales pour la base de données FEI

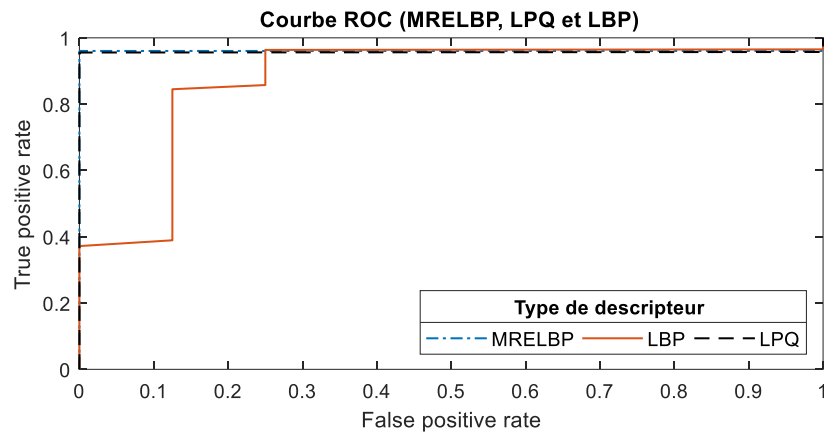
La base de données FEI a été modifiée pour prendre un ensemble des images qui présente un changement des poses remarquable, mais avec ensembles d'image par personne inférieurs que celle de la base de donnée ORL. La base de données comprend 80 individus, 8 images pour chacun, ce qui donne un total de 640 images en total. Les taux calculés sont présentés dans le *tableau III.3* :

Tableau III.3 : Résultat de la base de données FEI

	TPR (%)	FPR (%)	TNR (%)	FNR (%)	Taux de reconnaissance (%)
LBP	84.2051	0.1940	99.8060	15.7949	92.0055
LPQ	92.0385	0.0712	99.9288	7.9615	95.9837
MRELBP	93.4236	0.0644	99.9356	6.5764	96.6796

Pour accomplir la performance globale de ces méthodes sur cette base de données, on a tracé le courbe ROC suivant : illustrant la différence entre la performance de chaque méthode.

Figure III.12 : Courbe ROC présentant les trois différents méthodes (MRELBP, LPQ et LBP)



III.4.4 Discussion des résultats

Après la collection des résultats précédents, on peut tirer les points suivants :

- ❖ La base de données choisies influe d'une façon directe sur les taux de reconnaissance du système. Le nombre d'images par personnes améliore fortement les taux de reconnaissances. La base FERET qui contient trois images par personne présente les plus faibles taux.
- ❖ Le descripteur MRELBP donne les meilleurs taux de reconnaissances par rapport aux deux autres (LBP et LPQ) pour les trois bases de données utilisés. Ceci est dû à son vecteur de caractéristique qui est composé de la concaténation de trois vecteurs de caractéristiques celle de (NI-MRELBP, CI-MRELBP et RD-MRELBP) (voir la section II.5.2).
- ❖ Le temps d'exécution de la reconnaissance basée sur le MRELBP est relativement long par rapport à celle basée LPQ et LBP.

III.5 Conclusion

Dans ce chapitre, nous avons fait la présentation des résultats de la mise au point du système proposé. En suivant un protocole de test et d'évaluation précis, nous avons exploré trois méthodes d'extraction des caractéristiques LBP, LPQ et MRELBP sur trois bases de données différents FERET, ORL et FEI. Ces méthodes ont donné des résultats prometteurs. La méthode MRELBP, a montré à travers une étude comparative, qu'elle pouvait fournir d'excellents résultats en termes de taux de reconnaissance et les courbe ROC. Dans le chapitre suivant, nous allons faire une application en temps réel dans laquelle nous implémentons l'approche proposée pour la reconnaissance faciale.

Chapitre IV : Implémentation du système développée

IV.1 Introduction

De nos jours, la vidéosurveillance est omni présente et on la retrouve dans de nombreux secteurs d'activité (banque, transports, industrie, grande distribution, ...) ou lieux de vie (villes, immeubles de bureau, équipements collectifs, ...).

Le nombre croissant de menaces de vol ou autre a fait que la plupart des responsables d'entreprise, souhaitent accroître la s'écurité, en protégeant les biens et les personnes par de la vidéosurveillance. C'est pourquoi, notre travail consiste à mettre en place un système de vidéosurveillance intelligente, en intégrant un système de reconnaissance faciale qui permettra l'authentification du personnel et la reconnaissance des personnes.

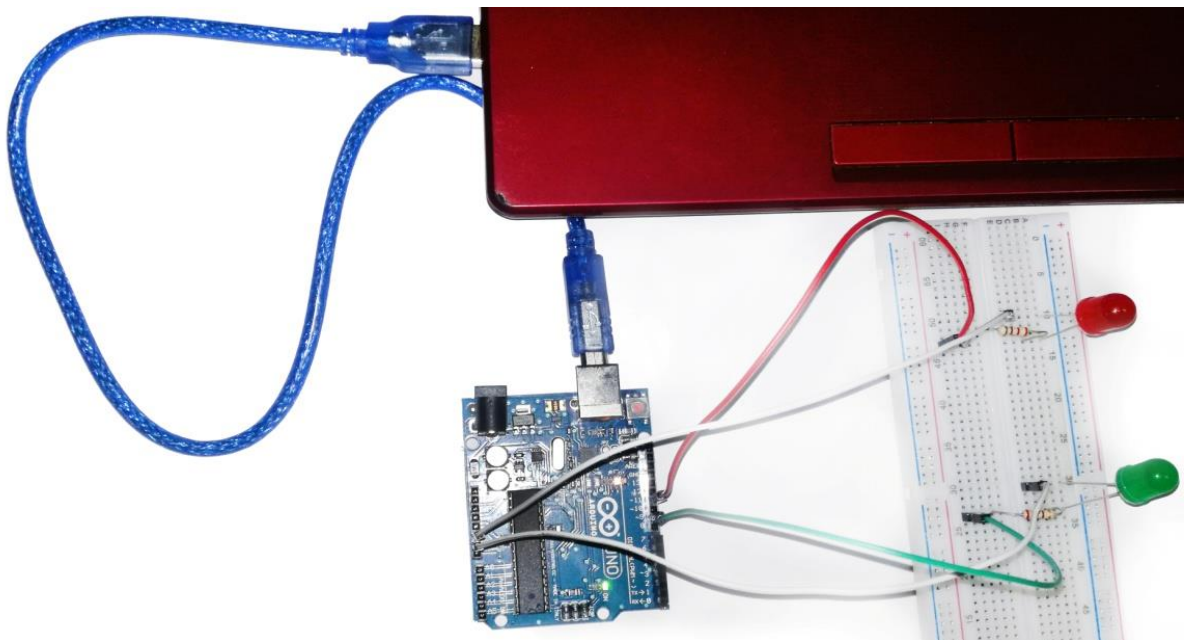
Ce chapitre est consacré à la présentation des différents aspects de l'application qui permettra d'identifier des personnes par la reconnaissance de visage en utilisant la capture par un camera IP wifi.

IV.2 Réalisation

Nous allons décrire en détail le système réalisée (*figure IV.1*), qui nous a permis de passer de la théorie à la pratique. A cet effet nous avons utilisé :

- Un Arduino
- Un ordinateur avec les caractéristiques suivantes : Processeur : Intel® Core™ i7-6500U CPU @ 2.50GHz (4 CPUs), Mémoire : 16 Gb.
- Une caméra IP wifi.
- Led et plaque d'essai.

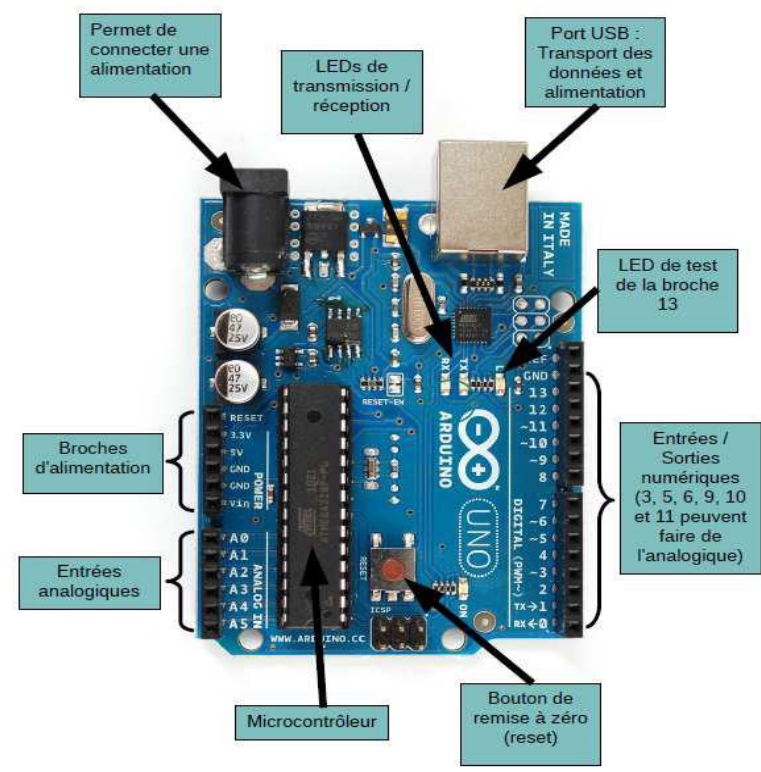
Figure IV.1 : Application réalisée



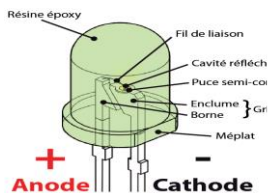
IV.2.1 Arduino

L'Arduino est une plate-forme de prototypage d'objets interactifs indépendants, ou connecté à un ordinateur pour communiquer avec différents logiciels. Il est constitué d'une carte électronique et d'un environnement de programmation. La carte électronique Arduino qui est un circuit imprimé en matériel libre (*c'est à dire que les plans de la carte elle-même sont publiés en licence libre*) sur lequel se trouve un microcontrôleur qui peut être programmé pour analyser et produire des signaux électriques. En d'une interface entrée/sortie simple. Au cours de notre projet, nous avons utilisé une carte Arduino UNO : La Arduino UNO est le modèle de référence de la série de cartes Arduino USB.

Figure IV.2 : La carte Arduino



IV.2.1.1 Led



Une diode électroluminescente (DEL ou LED) est un composant optoélectronique capable d'émettre de la lumière lorsqu'il est parcouru par un courant électrique.

IV.2.1.2 Résistance



Une résistance est un composant électronique ou électrique dont la principale caractéristique est d'opposer une plus ou moins grande résistance (mesurée en ohms) à la circulation du courant électrique. Dans notre application, elles sont utilisées pour la Protection des LEDs.

IV.2.1.3 Des Câble électriques



Un câble électrique est un regroupement de fils conducteurs avec parfois un, ou plusieurs, blindage électromagnétique intérieurs/extérieur. Un câble électrique peut être utilisé pour le transport d'énergie électrique mais aussi pour la transmission de données (téléphone, informatique, télévision, etc.).

IV.2.1.4 Breadboard (Planche à pain ... pour le prototypage)



Élément essentiel pour le prototypage et essai en tout genre.

IV.2.1.5 Smartphone (Utilisé comme camera IP) :



Une application (IP Webcam) installé sur Smartphone pour transforme le Smartphone en une caméra IP.

IV.2.1.6 Ordinateur



Un ordinateur est un système de traitement de l'information programmable tel que défini par Turing et qui fonctionne par la lecture séquentielle d'un ensemble d'instructions,

IV.2.2 La connexion entre les équipements

La connexion entre les différents équipements a été faite avec la façon suivante :

IV.2.2.1 Connexion entre Smartphone et ordinateur (Application hotspot)

Portable Wi-Fi hotspot est une application qui, comme son nom le suggère, permet de transformer l'appareil Android en un point d'accès Wifi. Cette application permet principalement de partager la connexion à Internet du système Android avec d'autres utilisateurs. En plus, elle permet de renommer la connexion et même la protéger par un mot de passe.

IV.2.2.2 Connexion entre IP camera et Matlab :

La connexion entre la camera IP et Matlab se fait à travers la création de l'objet suivant :
Cam = ipcam ("URL") crée l'objet **ipcam**, où **URL** est une valeur vectorielle de caractère qui identifie une caméra particulière par son **URL** et la connecte à la caméra avec cette adresse. **L'URL** doit correspondre à un flux **HTTP**, **RTSP** ou Motion JPEG (**mjpeg**).

Cette façon de créer l'objet ne nécessite aucune authentification de l'utilisateur. Lorsque l'objet *ipcam* est créé, il se connecte à la caméra et permet d'acquérir les images.

Pour notre application l'url utilisée est : `url = 'http://192.168.43.1:8080/shot.jpg';`

Sous MATLAB, le Support Package pour IP Cameras doit être déjà installé. Les images peuvent être prises depuis n'importe quelle caméra IP prenant en charge le flux *MJPEG* via *HTTP* et *RTSP* avec un support d'authentification de base.

IV.2.2.3 Connexion entre Arduino et Matlab :

Cette connexion est réalisée via le câble USB Arduino branché directement sur l'ordinateur. D'abord le *MATLAB* Support Package pour *Arduino* Hardware est installé pour permettre d'utiliser *MATLAB* et communiquer avec la carte *Arduino*.

IV.2.3 Interface (Matlab GUIDE)

GUIDE (Graphical User Interface Development Environment) est un environnement de travail intégré à *MATLAB* qui permet une conception et un développement accélérés, simples et intuitifs de l'interface graphique pour les applications orientées utilisateur. La *figure IV.3* représente l'interface utilisée pour l'application réalisée. Les différents boutons réalisés sont :

Figure IV.3 : Interface du projet réalisé



- 1) **Accuracy** : L'Accuracy est le taux de reconnaissance d'un descripteur sur une base de donnée spécifié.
- 2) **Affichage** : C'est un afficheur qui affiche le taux de reconnaissance (Accuracy) en (%)
- 3) **Descripteur** : C'est un panneau dont on sélectionne le descripteur qui extrait les vecteurs des caractéristiques de la base de donnée choisie.

- 4) **Les bases de données** : C'est un panneau qui nous permet de choisir une base de données pour le traitement.
- 5) **N° Classe** : C'est une entrée pour laquelle on choisit le label (n° de classe) pour l'enrôlement.
- 6) **Enrôlement** : L'enrôlement est l'action d'ajouter une nouvelle personne dans une base de données.
- 7) **Check ID** : pour décider est ce que la personne capturée en temps réelle appartient à la base de donnée ou non.
- 8) **Sortir** : Quitter le programme.

IV.3 Méthodologie de travail

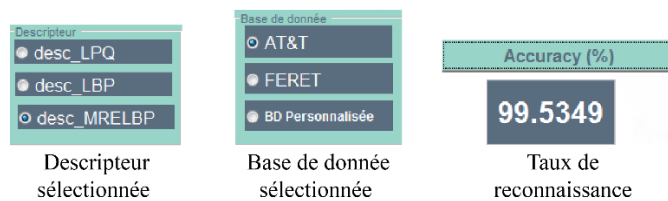
Pour la réalisation de notre travail, nous avons suivi les étapes d'un processus de reconnaissance des formes à savoir :

- Enrôlement
- Accuracy
- Détection du visage
- Reconnaissance et identification de la personne (Check ID).
- Faire l'action

Enrôlement : Pour faire la reconnaissance, nous avons besoin d'enregistrer les images des personnes à reconnaître dans notre base de données qui sera utilisée pour l'identification.

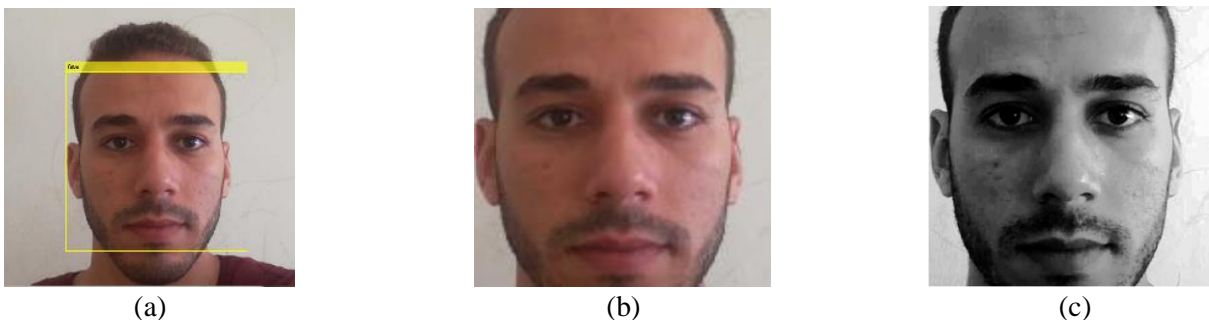
Accuracy : quand on clique sur le bouton Accuracy le programme commence à calculer le taux de reconnaissance de la base de données sélectionné avec le descripteur sélectionné

Figure IV.4 : Accuracy de la descripteur et base de données choisis



Détection du visage : une fois que la base de données est créée, nous allons passer à la détection de visage et pour cela, nous avons exploité la méthode de Viola-Jones. La **figure IV.5** montres la détection du visage en utilisant la méthode de Viola-Jones

Figure IV.5 : Détection de visage (a), recadrage du visage (b), conversion en niveau de gris (c)



Reconnaissance et identification de la personne (Check ID) : une fois le visage détecté, il reste à l'identifier. Pour la reconnaissance faciale nous avons décidé, d'utiliser le descripteur sélectionné avant, qui permet de déterminer les caractéristiques d'un visage. Ces caractéristiques seront ensuite exploitées pour la recherche de l'individu dans la base de données.

Faire l'action : une fois l'identification est faite, Matlab envoie l'ordre à l'Arduino une LED verte s'allume si la personne est autorisée, une LED rouge s'allume si la personne n'a pas l'accès. L'autorisation d'accès est faite par le programme réalisé.

IV.4 Comment reconnaître une personne ?

Pour reconnaître une personne, nous procédons en deux étapes :

IV.4.1 Première étape : Apprentissage

Dans cette phase, chaque personne est identifiée par son label (numéro affecté à le dossier de chaque personne dans la base de données) et sa photo. En premier lieu nous allons créer un modèle training Features par la suite nous allons appliquer l'apprentissage sur ce modèle en utilisant la fonction de descripteur utilisé (MRELBP). Les résultats contiennent les caractéristiques des visages qui seront utilisées pour l'identification.

IV.4.2 Deuxième étape : Reconnaissance

Une fois l'apprentissage fait, nous chargeons les résultats de trainingFeatures (nous rappelons que ces résultats contiennent les caractéristiques MRELBP – chapitre 3 - des personnes qui se trouvent dans la base de données), par la suite nous allons faire la classification Fit k-Nearest Neighbor classifier. On prend alors une photo en temps réel et extraites les vecteurs de caractéristique de visage et avec la fonction *predict* renvoie un vecteur d'étiquettes de classe prédites pour les données de prédicteur dans trainingFeatures, en fonction du modèle de classification formé du voisin le plus proche k. On retourne la valeur de label trouvé pour identifier la personne trouvée après tout ça, le programme fait des actions dans l'afficheur de l'interface de l'Arduino tel que (accès refusé, bienvenue, des sonne, des LEDs s'allume) selon notre programmation.

IV.5 Résultats d'expérimentation

Avant de présenter les résultats que nous avons obtenus, nous allons tout d'abord présenter la base de données que nous avons utilisé, c-à-d les personnes qu'on essaiera d'identifier grâce au programme.

Dans le but de tester le programme de reconnaissance faciale nous avons pris deux personnes pour les tests, nous avons enregistré dix photos de profil de deux personnes différentes. Ces images vont nous servir comme base de données d'apprentissage. La *figure IV.6* représente un exemple des images d'une personne que nous avons prise.

Figure IV.6 : Base de données enregistrée



Les images doivent être prises sous différents angles, et avec différentes postures. Nous avons expérimenté notre travail sur différents types d'image pour tester sa capacité à identifier les personnes. Notre travail a été donc testé sur des images de personnes sans et avec artifices.

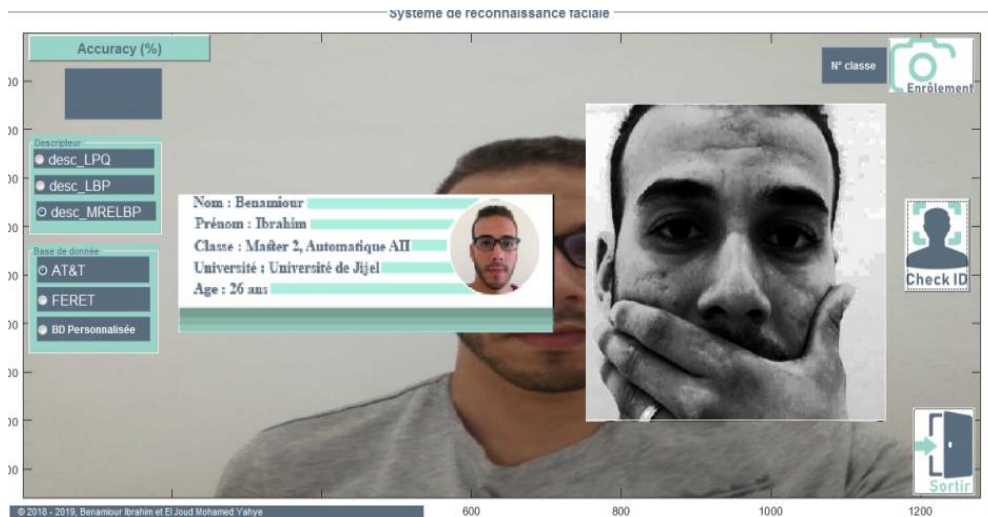
L'expérimentation a été sur des images :

- De personnes caché une partie de visage.
- De personnes avec lunettes.
- De personnes dans différentes conditions d'illumination.
- De personnes selon différentes postures.

IV.5.1 Identifier quelqu'un qui cache une partie de visage

Pour notre premier test, nous allons identifier une personne caché une partie de visage. Les résultats sont représentés sur la *figure IV.7*.

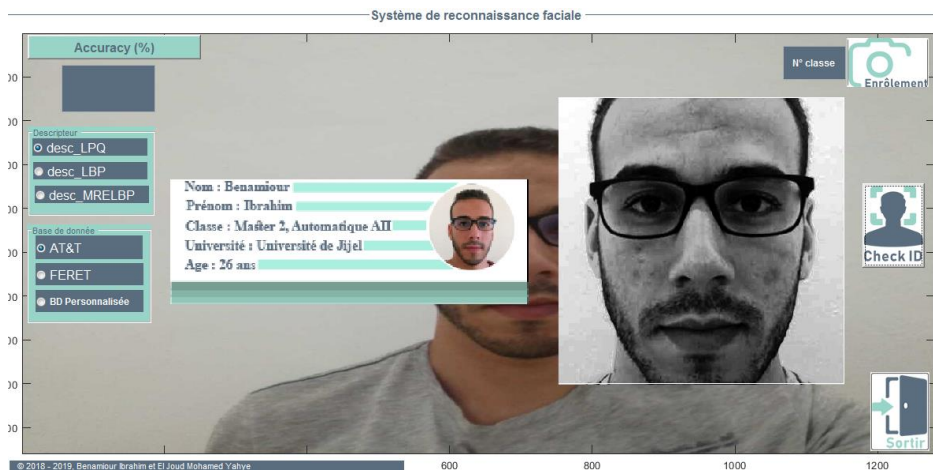
Figure IV.7 : Image avec une partie du visage cachée



IV.5.2 Identifier quelqu'un qui porte des lunettes de vue

Pour le deuxième test, nous allons essayer d'identifier un individu sans et avec lunettes de vue. La *figure IV.8*, montre le résultat du test. Nous remarquons sur la figure que le programme l'a bien reconnu avec des lunettes et sans lunettes. Le programme a identifié une personne qui porte un artifice.

Figure IV.8 : Personne portant des lunettes



IV.5.3 Identifier quelqu'un dans des conditions d'illumination (éclairage) différentes

Le troisième test est consacré au niveau d'éclairage dans la pièce, nous avons essayé d'identifier deux personnes différentes en faisant varier le niveau de luminosité, et pour cela on procède en quatre étapes :

- Éclairer le visage de personne de front.
- Éclairer le visage de personne du côté gauche.
- Éclairer le visage de personne du côté droit.

La figure IV. 9 représente les résultats des trois premiers tests, nous constatons que la personne a été mal identifiée. Le test a échoué

Figure IV.9 : Personne portant des lunettes



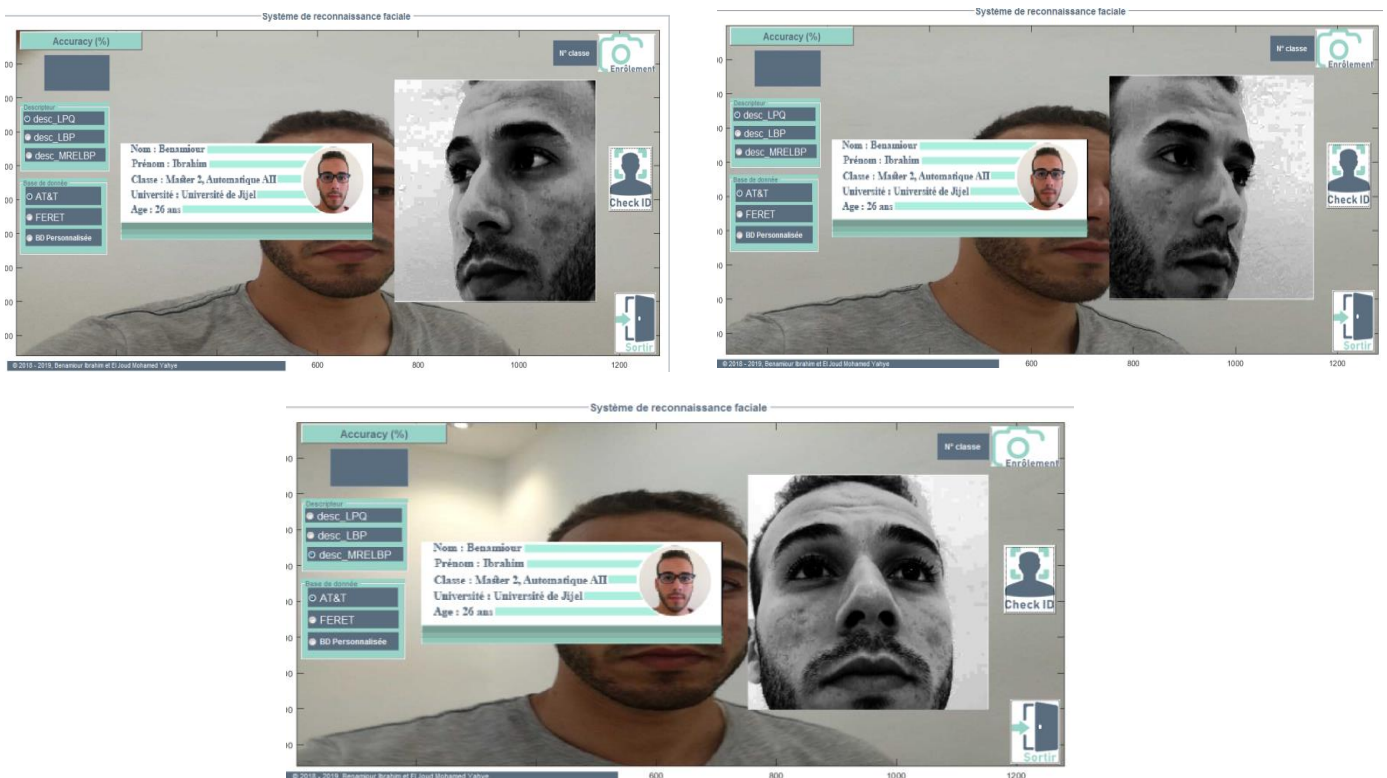
IV.5.4 Identifier une personne dans différentes postures

Dans le quatrième test nous allons nous intéresser aux différentes postures que prend l'individu, et pour cela nous allons essayer d'identifier l'individu sous trois postures différentes.

- Identifier une personne qui lève la tête.
- Identifier une personne qui tourne la tête à droite.
- Identifier une personne qui tourne la tête à gauche.

La **figure IV.10** montre les résultats des trois tests, nous constatons que la personne a bien été identifiée, le programme réagit bien aux différentes poses.

Figure IV.10 : Personne avec différentes poses



IV.6 Conclusion

Les différents tests effectués ont montré l'efficacité de l'algorithme proposé sous différentes conditions de capture d'image à part le test d'éclairage. On peut conclure qu'il est sensible aux conditions d'illumination.

Conclusion générale

La mise en œuvre d'une application de reconnaissance de visage en temps réel est une exigence à l'heure actuelle non discutable à cause des besoins sécuritaire dans plusieurs domaines. Vu la quantité de logiciels potentiels (sécurité, réseaux sociaux,) pouvant se baser sur cette application, celle-ci doit répondre à des exigences de robustesse et de rapidité des résultats. Notre projet est une tentative de réalisation d'une telle application.

Pour ce faire, cette application possède plusieurs aspects et repose sur plusieurs outils et notions. La première étape est celle de la détection de visage où on a utilisé l'algorithme standard de Viola and Jones, largement reconnu comme méthode fonctionnant en temps réel et fournissant des résultats robustes et fiables. Pour l'extraction de caractéristiques, nous avons utilisé trois méthodes LBP dans l'afin de profiter de leurs simplicités sur le plan implémentation et efficacité du point de vue robustesse. La classification par apprentissage par la méthode k-NN a permis d'obtenir des taux élevés de reconnaissances.

Nous estimons avoir réalisé un système répondant à l'objectif que nous avons fixé au départ, à savoir la mise en œuvre d'un système permettant la reconnaissance d'individus et le contrôle d'accès. Les problèmes de pose et d'éclairage pour l'identification dans des environnements extérieurs restent des challenges qui susciteront plus d'efforts.

En guise de perspectives, dans un premier temps une extension de ce travail peut être envisagée par l'étude et la réalisation d'un système de détection et de localisation du visage avec des performances assez hautes, une autre consiste à appliquer ce système sur d'autres bases de données des visages présentant des fortes variations dans l'éclairage et de la pose ainsi que d'envisager la possibilité d'employer une approche basée sur les éléments locaux du visage.

Ensuite, un des grands challenges serait de pouvoir mieux maîtriser les variations d'environnement, qui perturbent encore trop les systèmes de reconnaissance, Les dernières avancées de la technologie de capture 3D des images de visage ont permis de mettre en place des systèmes de reconnaissance assez robustes par rapport à la 2D.

Si la biométrie est un enjeu important au niveau économique, la recherche, en particulier dans le domaine de la reconnaissance des visages offre encore un champ d'investigations très ouvert avec de large perspectives tels que :

- Intégrer l'outil développé dans une application réelle de la reconnaissance pour l'authentification.
- Adjonction des systèmes de télésurveillance à un centre de contrôle de sécurité.

Bibliographie

- [1] T. Ojala, M. Pietikainen, and T. Maenpaa, Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on pattern analysis and machine intelligence* 24 (2002) 971-987.
- [2] V. Ojansivu, and J. Heikkilä, Blur insensitive texture classification using local phase quantization, *International conference on image and signal processing*, Springer, 2008, pp. 236-243.
- [3] L. Liu, S. Lao, P.W. Fieguth, Y. Guo, X. Wang, and M. Pietikäinen, Median robust extended local binary pattern for texture classification. *IEEE Transactions on Image Processing* 25 (2016) 1368-1381.
- [4] J. L. Wayman, A. Jain, D. Maltoni, and D. Maio, Eds., *Biometric Systems: Technology, Design and Performance Evaluation*. London: Springer-Verlag, 2005.
- [5] J. Yang, S. J. Xie, D. S. Park, S. Yoon, and J. Shin, "Fingerprint Quality Analysis and Estimation Approach for Fingerprint Matching," *State of the art in Biometrics*, Jul. 2011.
- [6] N.-S. Vu and A. Caplier, "Biologically Inspired Processing for Lighting Robust Face Recognition," *State of the art in Biometrics*, Jul. 2011.
- [7] Q. Tian, H. Qu, L. Zhang, and R. Zong, "Personal Identity Recognition Approach Based on Iris Pattern," *State of the art in Biometrics*, Jul. 2011.
- [8] N. MORIZET, "Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris," École Doctorale d'Informatique, Télécommunications et Électronique de Paris, Paris, 2009.
- [9] L. C. Jain, U. Halici, I. Hayashi, S. B. Lee, and S. Tsutsui, Eds., *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, 1 edition. Boca Raton, Fla: CRC Press, 1999.
- [10] Damer, Naser. (2018). Application-driven Advances in Multi-biometric Fusion.
- [11] M. Onyesolu and I. Ezeani, "ATM Security Using Fingerprint Biometric Identifier: An Investigative Study," *International Journal of Advanced Computer Science and Applications*, vol. 3, Apr. 2012.
- [12] P. Corcoran and C. Iancu, "Automatic Face Recognition System for Hidden Markov Model Techniques," *Face Recognition Volume 2, Intech Publishing*, Jun. 2019.
- [13] Kwang In Kim, Keechul Jung, and Hang Joon Kim, "Face recognition using kernel principal component analysis," *IEEE Signal Processing Letters*, vol. 9, no. 2, pp. 40–42, Feb. 2002.
- [14] Wangmeng Zuo, D. Zhang, Jian Yang, and Kuanquan Wang, "BDPCA plus LDA: a novel fast feature extraction technique for face recognition," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 36, no. 4, pp. 946–953, Aug. 2006.

- [15] Zhengyou Zhang, M. Lyons, M. Schuster, and S. Akamatsu, "Comparison between geometry-based and Gabor-wavelets-based facial expression recognition using multi-layer perceptron," in *Proceedings Third IEEE International Conference on Automatic Face and Gesture Recognition*, 1998, pp. 454–459.
- [16] R. S and Y. P Gowramma, "Face Recognition Techniques: A Survey," *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, vol. 3, pp. 630–635, Apr. 2015.
- [17] R. H. Abiyev, "Facial Feature Extraction Techniques for Face Recognition," *JCS*, vol. 10, pp. 2360–2365, 2014.
- [18] M. S. Bartlett, J. R. Movellan, and T. J. Sejnowski, "Face recognition by independent component analysis," *IEEE Transactions on Neural Networks*, vol. 13, no. 6, pp. 1450–1464, Nov. 2002.
- [19] K. P Tripathi, "A Comparative Study of Biometric Technologies with Reference to Human Interface," *International Journal of Computer Applications*, vol. 14, Jan. 2011.
- [20] L. Liu, P. Fieguth, G. Zhao, and M. Pietikainen, "Extended local binary pattern fusion for face recognition," *2014 IEEE International Conference on Image Processing, ICIP 2014*, pp. 718–722, Jan. 2015.
- [21] Banham, M.R., Katsaggelos, A.K.: Digital image restoration. *IEEE Signal Processing Mag.* 14(2), 24–41 (1997)
- [22] Nagarajaiah, S. "Adaptive passive, semiactive, smart tuned mass dampers: identification and control using empirical mode decomposition, hilbert transform, and short-term Fourier transform." *Structural Control and Health Monitoring: The Official Journal of the International Association for Structural Control and Monitoring and of the European Association for the Control of Structures* 16.7-8 (2009): 800-841.
- [23] K. Nasser, "Frequency Domain Processing," in *Digital Signal Processing System Design*, Second Edition. Academic Press, 2008, pp. 175–196.
- [24] Heikkila, J., Ojansivu, V., & Rahtu, E. (2010, August). Improved blur insensitivity for decorrelated local phase quantization. In *2010 20th International Conference on Pattern Recognition* (pp. 818-821). IEEE.
- [25] Vaidehi, S.Vasuhi et.al, "Person authentication using face detection", *Proceedings of the World Congress on Engineering and Computer Science*, pp 222-224, 2008.
- [26] Flanagan, Patricia A. "Face Recognition Technology (FERET)." NIST. July 13, 2017. Accessed July 13, 2019. <https://www.nist.gov/programs-projects/face-recognition-technology-feret>.

Bibliographie

- [27] " The ORL Database of Faces." The Database of Faces. Accessed July 13, 2019. <https://www.cl.cam.ac.uk/research/dtg/attarchive/facedatabase.html>.
- [28] Flanagan, Patricia A. "Face Recognition Technology (FERET)." NIST. July 13, 2017. Accessed July 13, 2019. <https://www.nist.gov/programs-projects/face-recognition-technology-feret>.
- [29] R. Rizki Damanik, D. Sitanggang, H. Pasaribu, H. Siagian, and F. Gulo, "An application of viola jones method for face recognition for absence process efficiency," *Journal of Physics: Conference Series*, vol. 1007, p. 012013, Apr. 2018.