



Université Mohamed Khider de Biskra
Faculté des Sciences et de la Technologie
Département de génie électrique

MÉMOIRE DE MASTER

Sciences et Technologies
Télécommunications
Réseaux et Télécommunications

Réf. : Entrez la référence du document

Présenté et soutenu par :
Farhi Imane, Gouicem Aya

Le : [Click here to enter a date.](#)

Application des paramètres de haralick à la reconnaissance de visage

Jury :

Dr.	Fedias Meriem	MCB	Université de Biskra	Encadreur
Pr.	Sbaa Salim	Pr	Université de Biskra	Président
Pr.	BENAKCHA Abdelhamid	Pr	Université de Biskra	Examineur

Année universitaire : 2024/2025

Remerciement

*Louange à « Allah » par Sa grâce les bonnes œuvres s'accomplissent.
C'est avec Son aide que j'ai pu achever.
Ce parcours scientifique. À Lui la louange en premier et en dernier.
J'exprime ma profonde gratitude et mes sincères remerciements à
toutes les personnes qui m'ont soutenu et accompagné jusqu'à la
réalisation de cet accomplissement.*

*Ceux dont les prières ont été mon appui, et dont le soutien a nourri
l'âme de mon accomplissement... Je dédie ce diplôme à mes chers
parents, vous êtes la source et la motivation première.*

*Je tiens à exprimer toute ma reconnaissance à ma respectable
encadrante, la Docteure "Fedias Meriem", qui n'a jamais ménagé ses
efforts pour m'apporter son savoir, ses orientations, et qui a été un
véritable soutien scientifique et moral à toutes les étapes de ce travail.*

*J'aimerais également exprimer ma considération la plus sincère aux
membres du jury.*

Résumé :

Cette recherche s'inscrit dans le domaine de la biométrie, et vise à vérifier l'identité des personnes à partir d'images faciales. Les systèmes de vérification du visage reposent généralement sur des images en niveaux de gris, approche que nous avons adoptée dans ce travail afin d'évaluer l'efficacité des techniques d'analyse de texture dans ce contexte. Nous avons concentré nos efforts sur l'extraction des caractéristiques distinctives du visage à l'aide de la **matrice de cooccurrence**, une méthode d'analyse de texture performante. À partir de cette matrice, nous avons extrait les **paramètres de Haralick**, qui capturent des informations statistiques fines sur la répartition de la texture dans l'image, ce qui les rend particulièrement adaptés à la distinction des traits faciaux.

Le système proposé a été évalué à l'aide de la base de données **XM2VTS**, en suivant le **protocole de Lausanne**. Les résultats ont montré une grande efficacité en termes de précision et de rapidité d'exécution, en particulier lors du traitement de bases de données de grande taille. Ces résultats démontrent que l'utilisation des descripteurs de Haralick pour la représentation des images faciales contribue de manière significative à l'amélioration des performances des systèmes de vérification d'identité.

Mots-clés : Biométrie, Couleur, authentification de visage, Analyse de texture, extraction de caractéristiques.

ملخص:

هذا البحث يندرج في إطار المقاييس الحيوية بهدف التحقق من هوية الأشخاص من خلال صورة الوجه. تعتمد أنظمة التحقق من الوجه عادةً على الصور بالأبيض والأسود، وهو ما اعتمدناه في هذا العمل لتقييم فعالية تقنيات تحليل النسيج في هذا السياق. ركزنا في هذا البحث على استخراج الخصائص المميزة للوجه من خلال مصفوفة التشارك (Co-occurrence Matrix) وهي تقنية تحليل نسيجي فعالة. ومن هذه المصفوفة استخرجنا معاملات هاراليك (Haralick features). هذه المعاملات تلتقط المعلومات الإحصائية الدقيقة حول توزيع النسيج في الصورة، مما يجعلها مناسبة لتمييز ملامح الوجه.

تم اختبار النظام المقترح على قاعدة البيانات **XM2VTS** باستخدام (بروتوكول لوزان)، وأظهرت النتائج فعالية عالية من حيث الدقة وسرعة التنفيذ، خاصة عند التعامل مع قواعد بيانات ذات حجم كبير. تُبين هذه النتائج أن استخدام معاملات هاراليك في تمثيل صور الوجه يساهم بشكل ملحوظ في تحسين أداء أنظمة التحقق.

الكلمات المفتاحية: القياسات الحيوية، اللون، مصادقة الوجه، تحليل الملمس، استخراج الميزات.

Abstract:

This research falls within the field of biometrics and aims to verify individuals' identities using facial images. Facial verification systems generally rely on grayscale images—an approach we adopted in this work in order to assess the effectiveness of texture analysis techniques in this context. We focused our efforts on extracting distinctive facial features using the co-occurrence matrix, a powerful texture analysis method. From this matrix, we extracted Haralick parameters, which capture fine statistical information about the texture distribution in the image, making them particularly well-suited for distinguishing facial traits.

The proposed system was evaluated using the XM2VTS database, following the Lausanne protocol. The results demonstrated high efficiency in terms of both accuracy and processing speed, especially when handling large databases. These results show that using Haralick descriptors for facial image representation significantly contributes to improving the performance of identity verification systems

Keywords: Biometrics, Color, Face Authentication, Texture Analysis, Feature Extraction.

Table des matières

INTRODUCTION GENERALE	1
------------------------------------	----------

Chapitre 1 : La biométrie et la reconnaissance faciale.

1.1 Introduction.....	4
1.2 Les principales techniques biométriques	4
1.3 Les avantages et les inconvénients de la reconnaissance de visage..	8
1.4 Processus de la reconnaissance faciale	9
1.5 Les défis de la reconnaissance faciale	13
1.6 Mesure de la performance des systèmes de reconnaissance de visages.....	14
1.7 Conclusion.....	18

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage.

2.1 Introduction	20
2.2 Les méthodes de reconnaissance de visage	20
2.3 La Technique utilisé.....	24
2.4 Conclusion	31

Chapitre 3 : Environnement de Travail.

3.1 Introduction.....	33
3.2 Présentation de la base de données XM2VTS.....	33
3.3 Le protocole de Lausanne.....	35

3.4 Conclusion	37
----------------------	----

Chapitre 4 : Mise en œuvre et Résultats.

4.1 Introduction.....	39
4.2 Prétraitement.....	39
4.3 Extraction des caractéristiques.....	40
4.4 Classification.....	40
4.5 Mesure de similitude.....	41
4.6 Présentation des résultats de la technique utilisée.....	41
4.7 Conclusion.....	43
CONCLUSION GENERALE.....	44
REFERENCES.....	46

Listes des figures

Figure 1.1 : Classification d'un certain nombre de modalités biométries.....	5
Figure 1.2 : Photo de signature	5
Figure 1.3 : Spectre d'un signal voix	6
Figure 1.4 : Photo de marche	6
Figure 1.5 : Photo de rétine	6
Figure 1.6 : Photo d'iris	7
Figure 1.7 : Photo de visage.....	7
Figure 1.8 : Photo analyse de l'ADN.....	8
Figure 1.9 : Photo de l'empreinte digitale.....	8
Figure1.10 : Variation de pose, changement d'illumination.....	9
Figure1.11 : Système de reconnaissance de visage.....	9
Figure1.12 : Détection de visage.....	10
Figure1.13 : Processus de reconnaissance faciale par l'intelligence artificielle.....	11
Figure1.14 : Schéma général d'un système de reconnaissance des visages.....	12
Figure1.15 : Variations faciales et défis de la reconnaissance biométrie.....	14
Figure1.16 : Illustration du TFR et du TFA.....	15
Figure 1.17 : Courbe ROC.....	16
Figure 2.1 : Classification des méthodes principales utilisées en reconnaissance faciale.....	20
Figure 2.2 : Le principe des méthodes globales.....	21
Figure 2. 3 : Formation de la matrice de cooccurrence GLCM.....	26

Figure 2 .4: Exemple sur deux images de visages (b) matrice de cooccurrence avec 64 niveaux de gris (c) avec 256 niveaux de gris.....	26
Figure 3.1 : Images typiques de la base de données XM2VTS.....	35
Figure 3.2 : Répartition des images de la base de données selon la configuration I...	36
Figure 3.3 : Répartition des images de la base de données selon la configuration II..	37
Figure 4.1 : Quelques exemples d'images de visages de la base de données XM2VTS.....	39
Figure 4.2 : a) image d'entrée, b) image après découpage et c) image après décimation.....	40

Liste des tableaux

Tableau 1.1 : Les avantages et les inconvénients de la reconnaissance de visage.....	9
Tableau 2.1 : Comparaison des méthodes basées sur les caractéristiques locales et les caractéristiques globales en fonction des critères de variation.....	24
Tableau 2.2 : Les 14 paramètres de Haralick.....	27
Tableau 3.1 : Répartition des photos dans les différents ensembles.....	37
Tableau 4.1 : Les résultats de 14 paramètres de Haralick avec 16 niveaux de gris et différents angles : 0° , 45° , 90° , 135°	42

INTRODUCTION GENERALE :

Les communications à l'échelle internationale connaissent un essor considérable, tant sur le plan du volume que de la diversité (déplacements physiques, transactions financières, accès aux services, etc.), ce qui rend indispensable la nécessité de vérifier l'identité des individus. En effet, l'importance des enjeux associés à ces échanges peut inciter les fraudeurs à tenter de contourner les dispositifs de sécurité existants. Dans ce contexte, un intérêt croissant se manifeste pour les systèmes électroniques d'identification et de vérification d'identité. Ces systèmes partagent tous le besoin commun de disposer d'un moyen simple, pratique, fiable et peu coûteux pour confirmer l'identité d'une personne, sans nécessiter l'intervention d'un tiers. Le marché du contrôle d'accès a connu une large expansion avec la multiplication des dispositifs, mais aucun ne s'est révélé infaillible face à la fraude. Cela s'explique par le fait qu'ils reposent essentiellement sur des identifiants externes (badge, carte, code, clé...), qui peuvent être oubliés, perdus, copiés ou volés. Ce défaut commun l'authentification d'un objet plutôt que de l'individu lui-même constitue une faille majeure dans ces systèmes. Face à cette problématique, la biométrie apparaît comme une alternative prometteuse. Elle offre à la fois simplicité, confort d'usage et sécurité accrue. La biométrie s'appuie sur l'étude des caractéristiques physiques ou comportementales propres à chaque individu, en utilisant des approches mathématiques comme les statistiques ou les probabilités. Cette discipline vise à identifier les personnes à partir de leurs traits biologiques (empreintes digitales, iris, visage...) ou comportementaux (voix, démarche, signature...). Parmi ces différentes modalités, la reconnaissance faciale a été retenue dans ce travail, car elle repose sur un indice biologique riche en informations et qui peut être capturé de manière non intrusive. Cette technique est l'une des plus répandues et acceptées dans le domaine de la biométrie, notamment en raison de la possibilité de capturer une image du visage à distance, sans contact direct avec l'individu. À l'aide d'une caméra, il est possible d'extraire des caractéristiques clés du visage telles que les yeux, la bouche, le contour du visage ou encore le nez. Ces données sont ensuite comparées à une base de référence afin de vérifier l'identité de la personne. Le système doit être en mesure d'identifier l'individu même en présence de modifications physiques telles que le port de lunettes, la présence d'une barbe ou d'une moustache. Cependant, malgré sa popularité, la reconnaissance faciale présente certaines limites. Elle est

particulièrement sensible aux variations d'éclairage, aux expressions faciales, à la position du visage, à l'usage de maquillage ou encore aux effets du vieillissement. Le signal biométrique facial est donc sujet à de nombreuses fluctuations, ce qui rend l'authentification plus complexe. Ce mémoire s'inscrit dans le cadre de l'étude de l'authentification par le visage, dont l'objectif principal est de confirmer l'identité d'un utilisateur déjà connu du système (authentification) et non d'en découvrir l'identité (identification).

Dans notre travail, nous avons choisi une méthode pour l'extraction des caractéristiques faciales en utilisant les paramètres de Haralick. Cette méthode se base sur le calcul d'une matrice de cooccurrence dit GLCM (Grey Level Co-occurrence Matrix).

Plan de mémoire de fin d'études :

Le chapitre 1 présentera quelques techniques biométriques qui existent dans la littérature, ses applications, les détails sur la technique biométrique basée sur le visage, les différents avantages et inconvénients de la reconnaissance faciale, le processus de la reconnaissance de visage, les défis de la reconnaissance faciale et mesure de la performance des systèmes de reconnaissance de visages.

Dans le chapitre 2, nous mettrons en évidence les méthodes de reconnaissance de visage et la Technique utilisé pour la reconnaissance de visage.

En chapitre 3, nous allons présenter la base de données des visages qui a été choisie pour nos expériences. Ainsi le protocole expérimental qui a été soigneusement conçu pour cette base de données.

Le chapitre 4 présentera les améliorations possibles en utilisant l'information pour améliorer les résultats obtenus par l'algorithme décrits en chapitre 2.

Nous terminons enfin par une conclusion générale et perspective.

Chapitre 1 :
La biométrie et la reconnaissance faciale

Chapitre 1 : la biométrie et la reconnaissance faciale

1.1 Introduction :

Dans tous les domaines de sécurité et de contrôle d'accès, on utilise des mots de passe ou des clés qui se compose de chiffres ou de lettres. Mais, dans ces derniers temps avec l'avancement de la technologie ces mots de passe sont devenus facilement falsifiables et franchissable. C'est pour ça, que les chercheurs de différents domaines ont orientés leurs travaux sur des clés et mots de passe impossible à falsifier, sûr et surtout efficace. La biométrie est devenue à la mode dans les domaines qui requiert un niveau élevé de sécurité et de contrôle Et parmi toutes les technologies biométriques qui existent, la reconnaissance des visages et l'une des technologies les plus utilisées et les plus adaptées car elle nous permet d'exploiter de nombreuses informations relatives à une personne. La reconnaissance du visage est un domaine très actif dans la vision par ordinateur et dans la biométrie. Elle a été étudiée vigoureusement il y a déjà 25 ans et sa finalité est de produire des homme-machine, applications pour les appareils photo numériques, jeux et divertissement. [1]

Dans ce chapitre, nous donnons un aperçu des différentes méthodes biométriques et nous mettons en lumière le processus de reconnaissance faciale.

1.2 Les principales techniques biométriques :

La biométrie est une mesure des caractéristiques biologiques pour l'identification ou l'authentification d'un individu à partir de certaines de ses caractéristiques : comportementales (exemple de la dynamique de frappe au clavier), physiques, ou physiologiques (exemple de l'ADN). Cette technique est utilisée de plus en plus aujourd'hui pour établir la reconnaissance des personnes dans un grand nombre d'applications divers.[2]

Chapitre 1 : la biométrie et la reconnaissance faciale

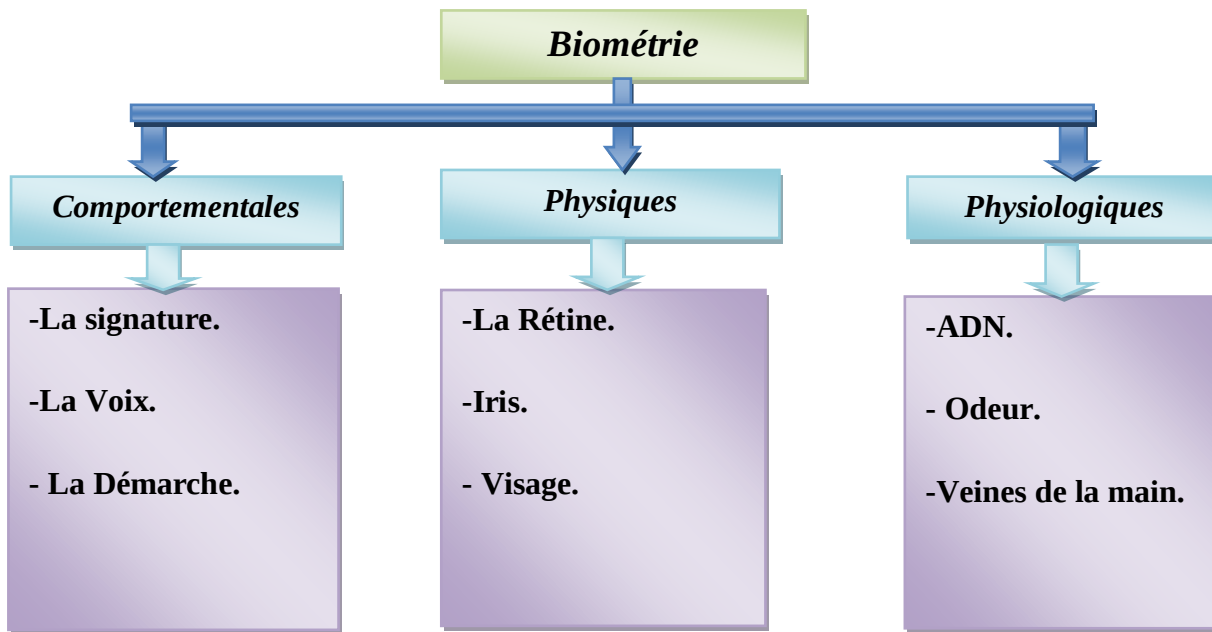


Figure 1.1 : Classification d'un certain nombre de modalités biométrie.

1.2.1 La signature :

La vérification de la signature analyse la façon dont un utilisateur signe son nom. Les caractéristiques dynamiques de la signature comme la vitesse et la pression sont aussi importantes que la forme géométrique de la signature. [3]

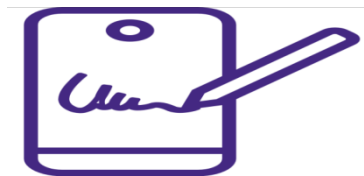


Figure 1.2: Photo de signature.

1.2.2 La voix :

Les données utilisées par la reconnaissance vocale proviennent à la fois de facteurs physiologiques et comportementaux. L'identification par la voix basée sur la forme et la taille des appendices (bouche, cavités nasales et les lèvres) utilisées dans la synthèse du son.[4]



Figure 1.3: Spectre d'un signal voix.

1.2.3 La démarche :

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps...), en analysant des séquences d'images.[4]



Figure 1.4: Photo de marche

1.2.4 La rétine :

La rétine C'est la couche sensorielle de l'œil qui permet la vision. La détermination des caractéristiques de la rétine consiste à extraire la distribution géographique des vaisseaux sanguins Cette technologie est adaptée aux applications de haute sécurité (salles de coffres forts, sites militaires.....).[5]

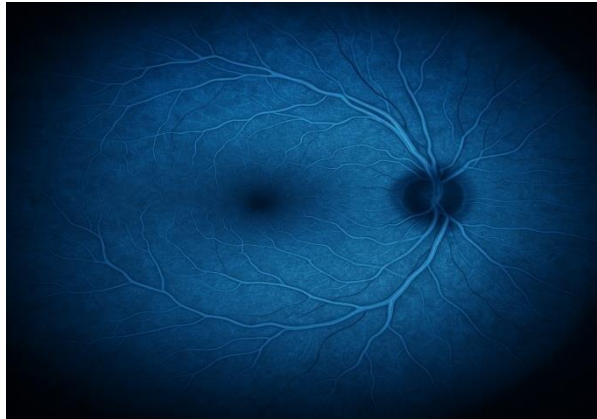


Figure 1.5:Photo de rétine.

1.2.5 L'iris :

L'iris est la région, sous forme d'anneau, située entre la pupille et le blanc de l'œil, il a une structure extraordinaire et offre de nombreuses caractéristiques de texture qui sont uniques pour chaque individu.[6]



Figure 1.6 : Photo d'iris.

1.2.6 La Visage :

On peut identifier un individu en fonction de ses caractéristiques faciales en effectuant des mesures : écartement des yeux, arêtes du nez, commissures des lèvres, oreilles, menton ces différentes caractéristiques sont analysées par les systèmes de reconnaissance faciale et comparées à une base de données existante. Cette méthode permet d'identifier une personne ou de vérifier une identité. [6]



Figure 1.7: Photo de visage.

Chapitre 1 : la biométrie et la reconnaissance faciale

1.2.7 Analyse de l'ADN :

L'ADN présent dans les cellules du corps, il est spécifique pour chaque individu. C'est une analyse du patrimoine génétique qui permet une identification à partir des cheveux, fragment de peau, d'une trace de sang et d'une goutte de salive.[5]



Figure 1.8: Photo analyse de l'ADN.

1.2.8 L'empreinte digitale :

L'empreinte digitale est une signature que nous laissons derrière nous à chaque fois que nous touchons un objet. Cette signature unique et spécifique pour chaque individu permet l'identification de la personne grâce aux systèmes de reconnaissance biométrique. [2]



Figure 1.9: Photo de l'empreinte digitale.

1.3 Les avantages et les inconvénients de la reconnaissance de visage :

La reconnaissance faciale (Face Recognition, FR) est un système qui fournit des techniques d'intelligence artificielle et des descripteurs biométriques pour comparer et analyser le visage d'une personne afin de l'identifier. La reconnaissance faciale a facilité la création et le développement avancé les grandes données, des réseaux de neurones et des GPU.[7]

Chapitre 1 : la biométrie et la reconnaissance faciale

Les avantages	Les inconvénients
- Facile à mettre en œuvre et à tester car il ne nécessite pas d'équipement spécial, mais tout ce dont vous avez besoin est d'une caméra haute résolution.	- Psychologiquement, certaines personnes rejettent leur image photographique (refus de son image, ajout d'accessoires, rôle, religion, critique de la qualité de la caméra, etc.), l'image est considérée comme trop personnelle Peut être utilisée.
-Aucune action de l'utilisateur (n'implique pas de coopération de l'utilisateur).	- Présence ou absence des composants structurels : La présence des composants structurels telle que la barbe, la moustache ou bien les lunettes.[8]
- Bien accepté par le public.	- Difficultés de différencier de vrais jumeaux qui ont le même indicatif d'ADN.
- Pas de contact physique...[7]	-Technologie sensible à l'environnement (éclairage, position, expression du visage...).[9]

Tableau 1.1 : Les avantages et les inconvénients de la reconnaissance de visage.



Figure1.10 : variation de pose, changement d'illumination.

1.4 Processus de la reconnaissance faciale :

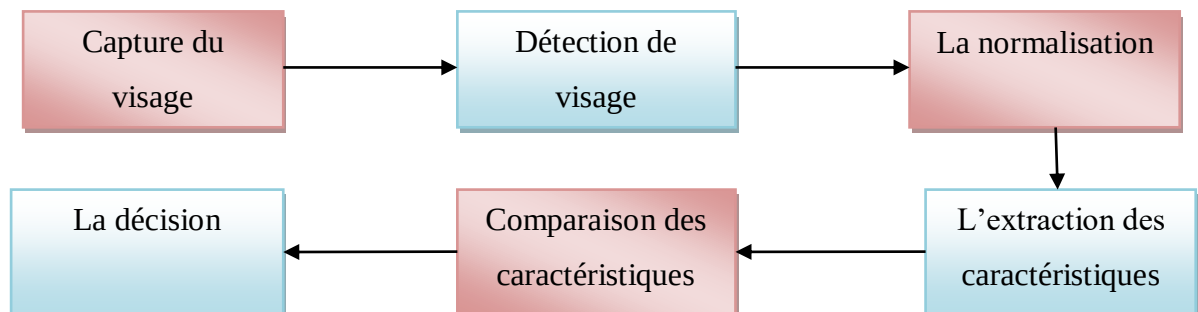


Figure1.11 : Système de reconnaissance de visage.

Chapitre 1 : la biométrie et la reconnaissance faciale

1.4.1 Capture du visage : La capture est la première étape dans le processus. Il faut réussir à capter l'information pertinente sans bruit. Dans la reconnaissance de visage on peut utiliser les capteurs 3D par exemple pour s'affranchir des problèmes de pose. Mais leur prix excessif ne permet pas une utilisation à grande échelle. Les capteurs en proche infrarouge sont utilisés pour éliminer les problèmes de l'illumination. Le codage consiste en l'acquisition d'image et sa digitalisation, ce qui donne lieu à une représentation bidimensionnelle au visage. L'image dans cette étape est dans un état brut ce qui engendre un risque de bruit qui peut dégrader les performances du système et donne lieu à une représentation 2D (la matrice des niveaux de gris) pour un objet 3D (le visage).[10]

1.4.2 Détection : La détection de visage peut se faire par détection de la couleur de la peau, la forme de la tête ou par des méthodes détectant les différentes caractéristiques du Visage. Cette étape est autant plus délicate quand l'image acquise contient plusieurs objets de visage ou un fond non uniforme qui crée une texture perturbant la bonne segmentation du visage. Cette étape est dépendante de la qualité des images acquises.[10]

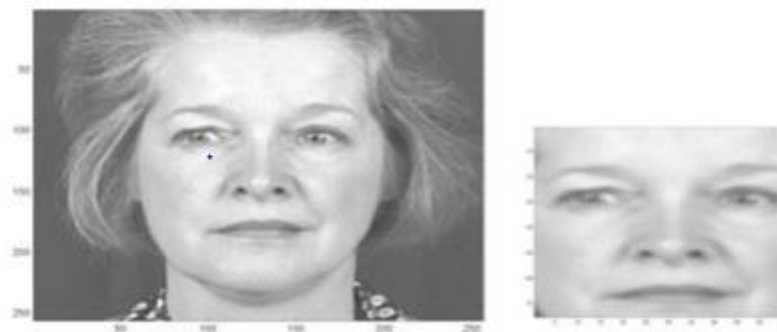


Figure1.12 : Détection de visage.

1.4.3 La normalisation : Est constituée de deux processus : géométrique et photométrique. La normalisation géométrique est nécessaire parce que la taille du visage à l'intérieur de l'image acquise peut varier en fonction de la distance entre le module d'acquisition et la personne. L'étape de normalisation photométrique tente d'éliminer ou de réduire les effets de l'illumination de l'image.[11]

Chapitre 1 : la biométrie et la reconnaissance faciale

1.4.4 L'extraction des caractéristiques : Le but est 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.[12]

1.4.5 Comparaison des caractéristiques : Selon les caractéristiques extraites précédemment, les algorithmes de comparaison diffèrent. On trouve dans la littérature plusieurs approches : calcul de distance, calcul de similarité...etc. Cette comparaison produit un score, représentant la similarité ou la distance de l'image test par rapport à l'image ou au modèle référence.[13]

1.4.6 La décision : C'est l'étape qui fait la différence entre un système d'identification d'individus et un système de vérification. Dans cette étape, un système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée à partir de ceux stockés dans la base de données, il est caractérisé par son taux de reconnaissance. En revanche, dans un système de vérification il s'agit de décider si le visage en entrée est bien celui de l'individu (modèle) proclamé ou il s'agit d'un imposteur. Pour estimer la différence entre deux images, il faut introduire une mesure de similarité.[10]

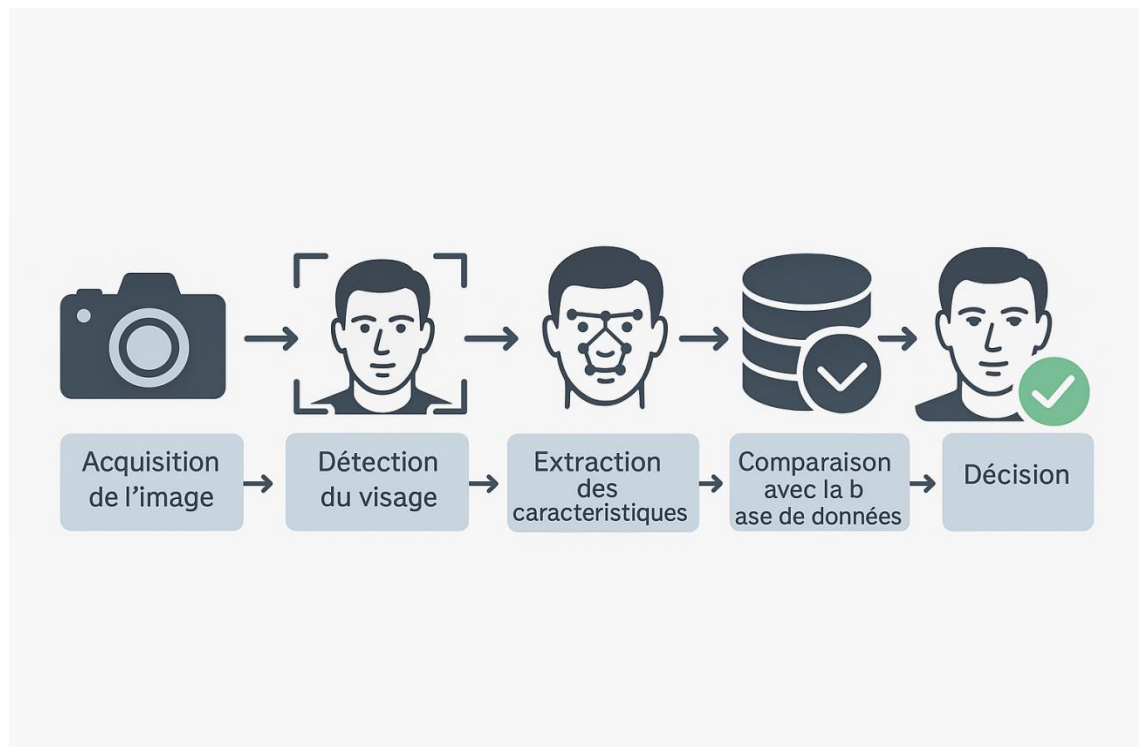


Figure1.13 : Processus de reconnaissance faciale par l'intelligence artificielle.

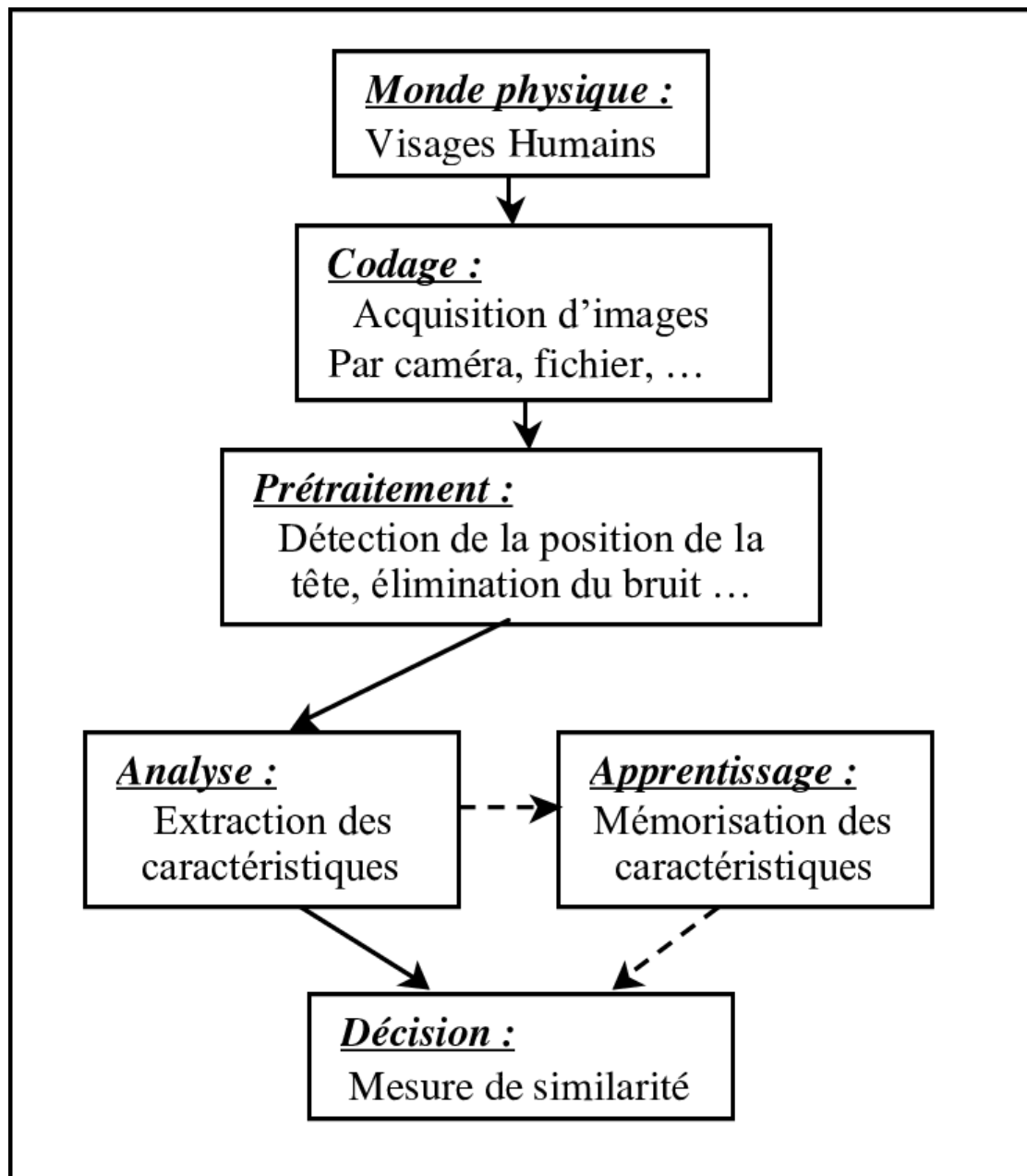


Figure1.14 : Schéma général d'un système de reconnaissance des visages.

Chapitre 1 : la biométrie et la reconnaissance faciale

1.5 Les défis de la reconnaissance faciale :

La reconnaissance faciale est une technologie puissante utilisée dans de nombreux domaines, mais elle rencontre également plusieurs défis. Voici quelques défis principaux à inclure :

1.5.1 Précision et Taux d'Erreur : Les systèmes de reconnaissance faciale peuvent parfois produire des erreurs, surtout dans des conditions de faible luminosité, avec des angles de vue atypiques ou des visages partiellement masqués. Les faux positifs (identifier une personne comme étant quelqu'un d'autre) et les faux négatifs (ne pas reconnaître une personne) sont des problèmes courants. [14]

1.5.2 Diversité des Visages : Les systèmes peuvent être biaisés et moins précis pour certains groupes démographiques, notamment les personnes de couleur ou les femmes, en raison de données d'entraînement non diversifiées. Cela peut entraîner des discriminations et des inégalités dans l'application de la technologie. [15]

1.5.3 Vie Privée et Sécurité : La collecte de données faciales soulève des préoccupations sur la protection de la vie privée. Le stockage des données faciales peut être vulnérable aux piratages, ce qui expose les individus à des risques de vol d'identité.[16]

1.5.4 Conditions environnementales : La qualité de la reconnaissance faciale peut être affectée par des conditions environnementales telles que l'éclairage, les masques faciaux, ou même la présence de lunettes ou de maquillage.[17]

1.5.5 Éthique et Consentement : L'utilisation de la reconnaissance faciale sans le consentement explicite des individus soulève des questions éthiques. Il existe un débat sur l'utilisation de ces technologies dans des espaces publics, comme les aéroports ou les rues.[18]

1.5.6 Normes Juridiques et Régulations : Le cadre juridique autour de la reconnaissance faciale varie d'un pays à l'autre, et les lois évoluent régulièrement. Certaines juridictions imposent des restrictions strictes à son utilisation, tandis que d'autres sont plus permissives.[19]

Chapitre 1 : la biométrie et la reconnaissance faciale

1.5.7 Manipulation de l'image : Les technologies permettant de manipuler des visages compliquent la tâche des systèmes de reconnaissance faciale, car elles peuvent tromper ces systèmes avec des images falsifiées.[20]



Figure1.15 : Variations faciales et défis de la reconnaissance biométrique.

1.6 Mesure de la performance des systèmes de reconnaissance de visages :

L'efficacité d'un système biométrique est représentée par deux types de taux d'erreur :

Une erreur de faux rejet FR : Si un utilisateur enregistré est rejeté. Ici le système évalue que ses données biométriques ne correspondent pas aux données de l'utilisateur dans la base de données.

- Le véritable sujet est accepté.
- Le véritable sujet est rejeté (FRE ou FR).
- L'imposteur est accepté (FAE ou FA).
- L'imposteur est rejeté.

Tout d'abord, afin de comprendre comment déterminer la performance d'un système biométrique, il nous faut définir clairement trois critères principaux :

Chapitre 1 : la biométrie et la reconnaissance faciale

1. Le premier critère s'appelle le taux de faux rejet (TFR). Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.
2. Le deuxième critère est le taux de fausse acceptation (TFA). Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.
3. Le troisième critère est connu sous le nom de taux d'égale erreur (TEE). Ce taux est calculé à partir des deux premiers critères et constitue un point de mesure de performance courant. Ce point correspond à l'endroit où $TFR = TFA$, c'est-à-dire le meilleur compromis entre les faux rejets et les fausses acceptations.[21]

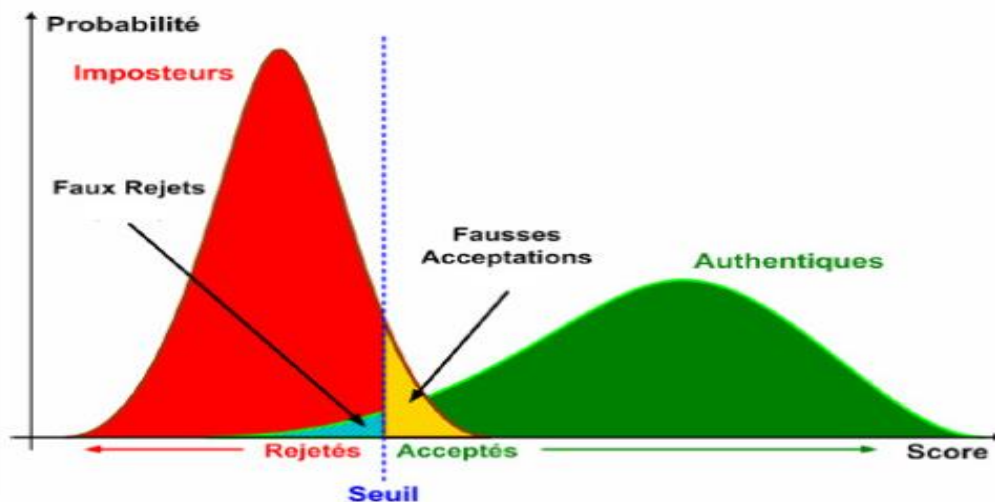


Figure1.16 : Illustration du TFR et du TFA.

La figure 1.15 illustre le TFR et le TFA à partir de distributions des scores authentiques et imposteurs tandis que l'EER est représenté sur la figure 1.16. Selon la nature (authentification ou identification) du système biométrique, il existe deux façons de mesurer la performance en termes de Taux d'acceptation Faux TFA le taux de faux rejet TFR, défini comme suit :

$$TFR = \frac{\text{Nombre des clients rejetés (FR)}}{\text{Nombre total d'accès clients}}$$

$$TFA = \frac{\text{Nombre des imposteurs acceptés (FA)}}{\text{Nombre total d'accès imposteurs}}$$

Chapitre 1 : la biométrie et la reconnaissance faciale

Une vérification parfaite d'identité ($FA=0$ et $FR=0$) est non réalisable dans la pratique. Cependant, comme montré par l'étude l'hypothèse de test binaire, n'importe lequel de ces deux taux (TFA, TFR) peut être réduit à une petite valeur arbitraire en changeant le seuil de décision, avec l'inconvénient d'augmenter l'autre. Une seule mesure peut être obtenue en combinant ces deux taux d'erreurs dans le taux erreur totale (TET) ou son complément, le taux de réussite total (TR) :

$$TET = \frac{\text{Nombre de fausses acceptations}(FA) + \text{Nombre de faux rejets}(FR)}{\text{Nombre totale d' accès}}$$

$$TR = 1 - TET$$

Cependant, un soin devrait être pris en utilisant une seule mesure. En effet, cette seule mesure (TET ou TR) pourrait être fortement pondérée par l'un ou l'autre type d'erreurs (TFA ou TFR), dépendant seulement du nombre d'accès qui ont été utilisés en obtenant ce type d'erreur. Le TET sera toujours plus près de l'erreur (TFA ou TFR) qui a été obtenue en utilisant le plus grand nombre d'accès dans son type. Lorsque le système opère en mode authentification, on utilise ce que l'on appelle une courbe ROC. La courbe ROC (Figure 1.16) trace le taux de faux rejet en fonction du taux de fausse acceptation. 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 performance globale d'un système de vérification d'identité est mieux caractérisée par sa courbe caractéristique de fonctionnement, qui représente le TFA en fonction du TFR. [21]

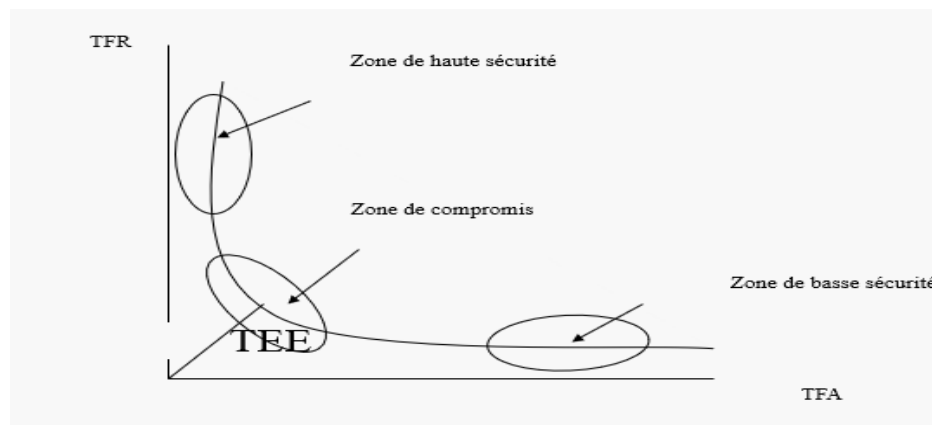


Figure 1.17: Courbe ROC

Chapitre 1 : la biométrie et la reconnaissance faciale

Le taux d'égale erreur TEE correspond au point $TFA = TFR$, c'est-à-dire graphiquement à l'intersection de la courbe ROC avec la première bissectrice. Il est fréquemment utilisé pour donner un aperçu de la performance d'un système. Seuls des systèmes qui produisent des taux TEE (taux d'erreur égale) faibles sont capables d'être déployés en mode identification. Ainsi, les protocoles d'évaluation diffèrent dans le mode identification et le mode vérification. Il faut savoir qu'en mode identification, deux scénarios sont possibles qui induisent deux protocoles différents.

Si l'identification se fait dans ce qui est appelé un mode fermé, c'est-à-dire que chaque personne est représentée dans la base de données par au moins une référence, alors le système n'est pas obligé de faire du rejet. Il peut assigner l'identité de la personne qui a le score le plus élevé (dans le cas de mesure de score de similitude). L'évaluation doit se faire sur toutes les comparaisons possibles entre les éléments de la base des références et les autres éléments de la base afin de simuler au mieux le cas d'un processus d'identification. Un deuxième scénario est possible en mode identification, c'est le mode ouvert. Dans ce cas, toutes les personnes de la base de test ne sont pas représentées dans la base de référence. En mode évaluation, il est primordial de regrouper les personnes de la base de données considérée en deux groupes, celles disposant de références et celles qui n'en ont pas. Ensuite, le système doit pouvoir prendre deux décisions distinctes : soit rejeter un échantillon test ou lui assigner une identité représentée dans la base des référents. Pour mettre en place une stratégie de rejet, il est impératif de fixer un seuil de décision analogue à celui fixé en mode vérification. La performance des systèmes biométriques est mesurée par leur exactitude dans l'identification, qui est calculée en utilisant les TFR et TFA. Le taux où on a la valeur du TFR est égal à la valeur du TFA s'appelle le taux d'erreur égal "TEE " et il est utilisé pour comparer les systèmes. Souvent, le taux véritable d'acceptation TFA est également employé comme seule mesure de performance. Dans tout système, on ne peut pas simultanément diminuer à la fois TFA et TFR, c'est pour cela que lors de la conception du système, on essaie de dégager un seuil de décision. Et puisque la sécurité est habituellement l'objectif principal, un bas TFA est habituellement choisi aux dépens d'un haut TFR.[22]

1.7 Conclusion :

Dans ce chapitre, nous avons présenté les technologies utilisées dans les systèmes biométriques pour l'identification des personnes. Cette étude nous a permis de constater que la reconnaissance de visage suscite de plus en plus l'intérêt de la communauté scientifique, car elle présente plusieurs défis et verrous technologiques. Enfin, nous avons mis en évidence le processus de la reconnaissance automatique de visage, ainsi les différentes difficultés liées à cette tâche. La technique utilisée aux différentes étapes de la reconnaissance faciale sera détaillée dans le chapitre suivant.

Chapitre 2 :
Analyse des paramètres de Haralick pour
la reconnaissance de visage.

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

2.1 Introduction :

Considérée comme l'une des applications les plus réussies de l'analyse et de la compréhension d'images, la reconnaissance faciale a récemment suscité un grand intérêt. Étant donné que les paramètres de Haralick sont des caractéristiques statistiques extraites de la matrice de co-occurrence des niveaux de gris (GLCM - Gray Level Co-occurrence Matrix), ces caractéristiques sont largement utilisées dans l'analyse de texture et peuvent être appliquées à la reconnaissance faciale pour extraire des informations distinctives sur la texture de l'image du visage.

Dans ce chapitre, nous allons présenter une méthode de reconnaissance faciale qui repose principalement sur les paramètres de Haralick.

2.2 Les méthodes de reconnaissance de visage :

De nombreux algorithmes ont été proposés dans la littérature pour la reconnaissance faciale, elles peuvent être classées en trois catégories :

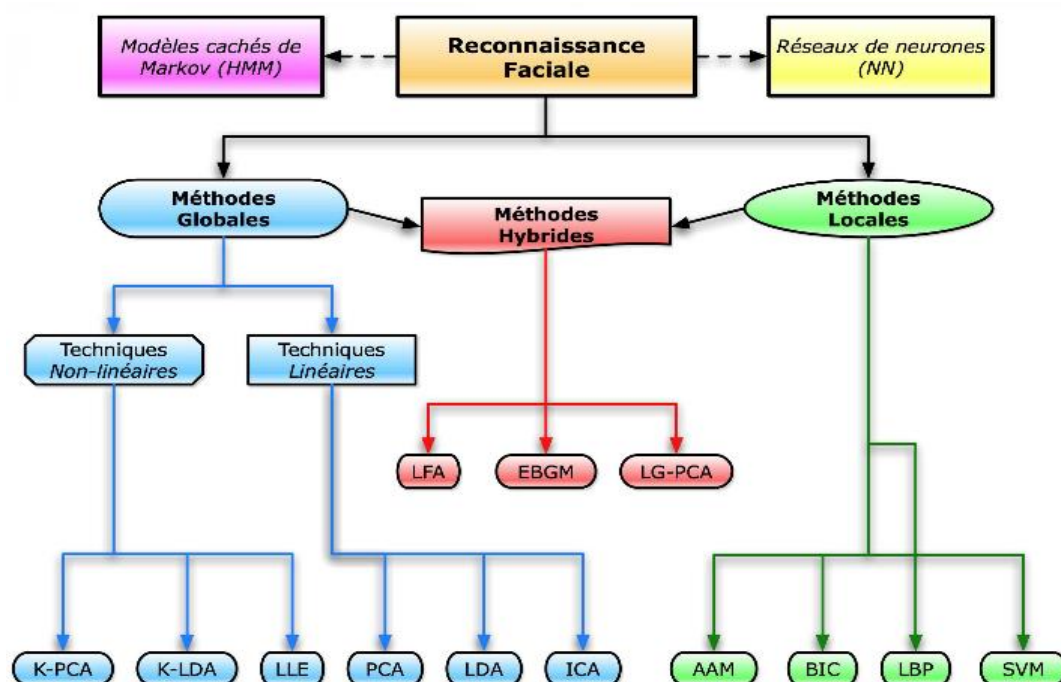


Figure 2.1: Classification des méthodes principales utilisées en reconnaissance faciale.

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

2.2.1 Les méthodes globales :

Le principe de cette approche est de représenter l'image de visage de dimension (m, n) par un seul vecteur de dimension $(m \times n)$ obtenu par la concaténation des valeurs du niveau de gris des pixels de l'image faciale, puis on projette l'image d'entrée dans un espace de plus faible dimension, en sélectionnant les caractéristiques nécessaires et discriminantes. L'avantage des méthodes globales est qu'elles conservent implicitement les informations de texture et de forme utiles pour la reconnaissance de visage, ainsi qu'elles permettent une meilleure capture de l'aspect global du visage que les présentations locales, de plus elles sont rapides à mettre en œuvre. Cependant leurs inconvénients résident dans leurs sensibilités aux conditions de la luminosité, de pose et d'expression faciale, de même, la taille des données à traiter est importante.[23]

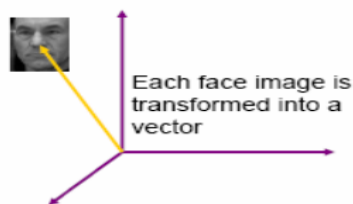


Figure 2.2: Le principe des méthodes globales.

Les méthodes globales peuvent se décomposer en deux types de techniques à savoir : les techniques linéaires et les techniques non linéaires.

a) Les Techniques Linéaires : Ce sont des techniques qui projettent linéairement les données des visages d'espace de grande dimension sur un espace de plus faible dimension. Cependant elles sont sensibles aux luminosités et surtout aux variations non convexes, et même l'utilisation des distances classiques dans l'espace projeté comme la distance Euclidienne et plus généralement les distances de Mahalanobis ne permettent pas de réaliser une bonne classification entre les classes visages et non-visages et entre les individus eux-mêmes. Les techniques linéaires les plus connues sont :

Eigenfaces, (**PCA** pour "Principal Component Analysis"). Son principe consiste à chercher les directions de l'espace qui représentent le mieux les corrélations entre les variables aléatoires. Il s'agit d'une transformation orthogonale linéaire des données

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

dans un nouvel espace représenté par des vecteurs propres associés aux plus grandes valeurs propres, les images des visages seront ensuite projetées sur cet espace. Cette technique est à la base de nombreuses méthodes globales qui apportent des améliorations ou des variations. Par exemple pour les travaux réalisés sur le choix des vecteurs propres nous pouvons citer :

- Les travaux de Kirby et al, qui proposent de retenir les vecteurs propres associés aux plus grandes valeurs propres jusqu'à ce que la somme de ces dernières dépasse 90% de leur énergie totale.
- Martinez et al, dans obtiennent un meilleur taux de reconnaissance en ignorant les premiers vecteurs propres (encodant souvent les variations d'illumination).

La technique Belhumeur et al, (**LDA** pour "Linéar Discriminant Analysis"), appelée Fisher faces qui divise les visages en classes selon le critère de Fisher. Cette technique est une variante de PCA, elle vise à trouver les directions de projection les plus discriminantes dans l'espace propre en maximisant le ratio entre la variance inter-classe et la variance intra-classe. Une des méthodes la plus utilisée pour le contourner consiste à utiliser d'abord le PCA pour diminuer la dimension des échantillons et ensuite nous réalisons le LDA.

Donc chaque visage se compose d'un grand nombre de pixels sera réduit à un plus petit ensemble de combinaisons linéaires avant la classification. Les combinaisons linéaires obtenues en utilisant PCA construisent un sous-espace pour représenter de manière optimale seulement l'objet visage tandis que LDA cherche à réaliser un sous-espace discriminant pour distinguer de façon optimale, les visages de différentes personnes. Cependant quand il n'y a pas beaucoup d'images par personne cette méthode marche moins bien que celle basée sur PCA.

D'autres techniques linéaires ont également été proposées nous citons par exemple :

- L'analyse en composantes indépendantes (ICA).
- La factorisation de matrices non négatives (NMF).
- L'analyse discriminante bilinéaire (BDA).
- La technique de Vecteurs communs discriminants (DCV).

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

Bien que les méthodes globales linéaires soient efficaces, et aient eu beaucoup de succès, elles ne sont pas assez précises. Ceci est dû à des transformations non-linéaires, une simple modification de la luminosité déforme les images de visages de façon non linéaire.[24]

b) Les Techniques Non-Linéaires : Afin de pouvoir traiter le problème de la non-linéarité, des techniques globales nonlinéaires ont été développées. Parmi ces méthodes on trouve :

Kernel-PCA (l'Analyse en Composantes Principales à Noyaux), et Kernel-LDA (L'Analyse Discriminante Linéaire à Noyaux), qui se basent sur la notion mathématique "noyau" en étendant les techniques PCA et LDA.

La technique de MDS (Multi Dimensional Scaling) vise à préserver autant que possible les propriétés globales des données d'apprentissage dans le nouvel espace de faible dimension en réalisant un mapping. La qualité de ce dernier est exprimée à travers une fonction de stress (ex. la fonction de stress brut, la fonction de coût de Sammon), qui est une mesure de l'erreur des distances entre les paires des échantillons dans les espaces de faible et de grande dimension.

Il existe d'autres techniques comme l'isomap, les diffusions maps, les approches neuronales etc. Bien que les méthodes non-linéaires peuvent atteindre une amélioration de taux de reconnaissance sur les données d'entraînement en effectuant une projection nonlinéaire de l'espace des images sur l'espace de caractéristiques (featurespace) permettant une réduction de dimension de meilleure façon, elles ne peuvent pas être robustes pour de nouvelles données en raison de leur grande flexibilité contrairement aux méthodes linéaires.[11]

2.2.2 Les méthodes locales :

Les méthodes locales, basées sur des modèles, utilisent des connaissances a priori que l'on possède sur la morphologie du visage et s'appuient en général sur des points caractéristiques de celui-ci. Kanade présenta un des premiers algorithmes de ce type [en détectant certains points ou traits caractéristiques d'un visage puis en les comparant avec des paramètres extraits d'autres visages. Ces méthodes constituent une autre approche pour prendre en compte la non-linéarité en construisant un espace

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

de caractéristiques local et en utilisant des filtres d'images appropriés, de manière que les distributions des visages soient moins affectées par divers changements. Toutes ces méthodes ont l'avantage de pouvoir modéliser plus facilement les variations de pose, d'éclairage et d'expression par rapport aux méthodes globales. Toutefois, elles sont plus lourdes à utiliser puisqu'il faut souvent placer manuellement un assez grand nombre de points sur le visage alors que les méthodes globales ne nécessitent de connaître que la position des yeux afin de normaliser les images, ce qui peut être fait automatiquement et de manière assez fiable par un algorithme de détection. Dans cette catégorie, on trouve plusieurs méthodes comme : filtres de gabor, Dynamic link architecture, HMM... [23]

2.2.3 Les méthodes hybrides :

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurales) avec l'extraction de caractéristiques d'apparence locales. Elles permettent d'augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d'éclairement et d'expressions faciales. [23]

Le tableau 2.1 résume la différence entre les méthodes locales et méthodes globales.

Facteur de variation	Caractéristiques locales	Caractéristiques globale
Eclairage (Illumination)	Très sensible	Sensible
Expression	Pas sensible	Sensible
Pose	Sensible	Très sensible
Bruit	Très sensible	Sensible

Tableau 2.1 : Comparaison des méthodes basées sur les caractéristiques locales et les caractéristiques globales en fonction des critères de variation.[21]

Actuellement, après ce bref aperçu des différentes méthodes utilisées dans le domaine de l'authentification par reconnaissance faciale, nous allons passer à l'explication de la technique basée sur les paramètres de Haralick pour l'identification du visage à travers l'analyse de la texture de l'image.

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

2.3 La Technique utilisée :

- **Les Matrices de Cooccurrence :**

L'approche statistique du second ordre la plus connue pour l'analyse de la texture des images est la matrice de cooccurrence GLCM (Gray Level Cooccurrence Matrix). C'était le résultat de la première approche consistant à décrire, puis à classer, la texture de l'image. Il reste populaire aujourd'hui en raison de ses bonnes performances. Parmi les propriétés de la texture on trouve la distribution et la cooccurrence spatiale de deux ou plusieurs niveaux de gris dans une région locale. Cette cooccurrence peut être résumée dans une matrice dont chaque élément est la probabilité (nombre d'apparition dans l'image) d'un couple de niveau de gris séparés par une relation spatiale R . R est en général définie par un vecteur de déplacement r (d, θ) où d est la distance entre les deux pixels et θ la direction. Les matrices de cooccurrence étant symétriques, on les calculera en général dans les directions 0, 45, 90 et 135° mais peuvent prendre également, d'autres valeurs compris entre 0 et 135°. Pour construire ces matrices M , $n \times n$ (avec n nombre de niveaux de gris de l'image), on va ainsi compter en $M(i, j)$, le nombre de fois où le niveau de gris j a succédé au niveau i pour un vecteur de déplacement $r(d, \theta)$. Haralick a proposé l'utilisation des matrices de cooccurrence pour extraire les caractéristiques de la texture de l'image. Pour une image codée en 256 niveaux de gris, sa matrice de cooccurrence est la matrice carrée de 256×256 tel que l'élément à la ligne i et la colonne j représente la probabilité (ou le nombre d'occurrence) qu'un pixel d'intensité i apparaît dans l'image à une distance D et une direction θ d'un pixel d'intensité j . [25]

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

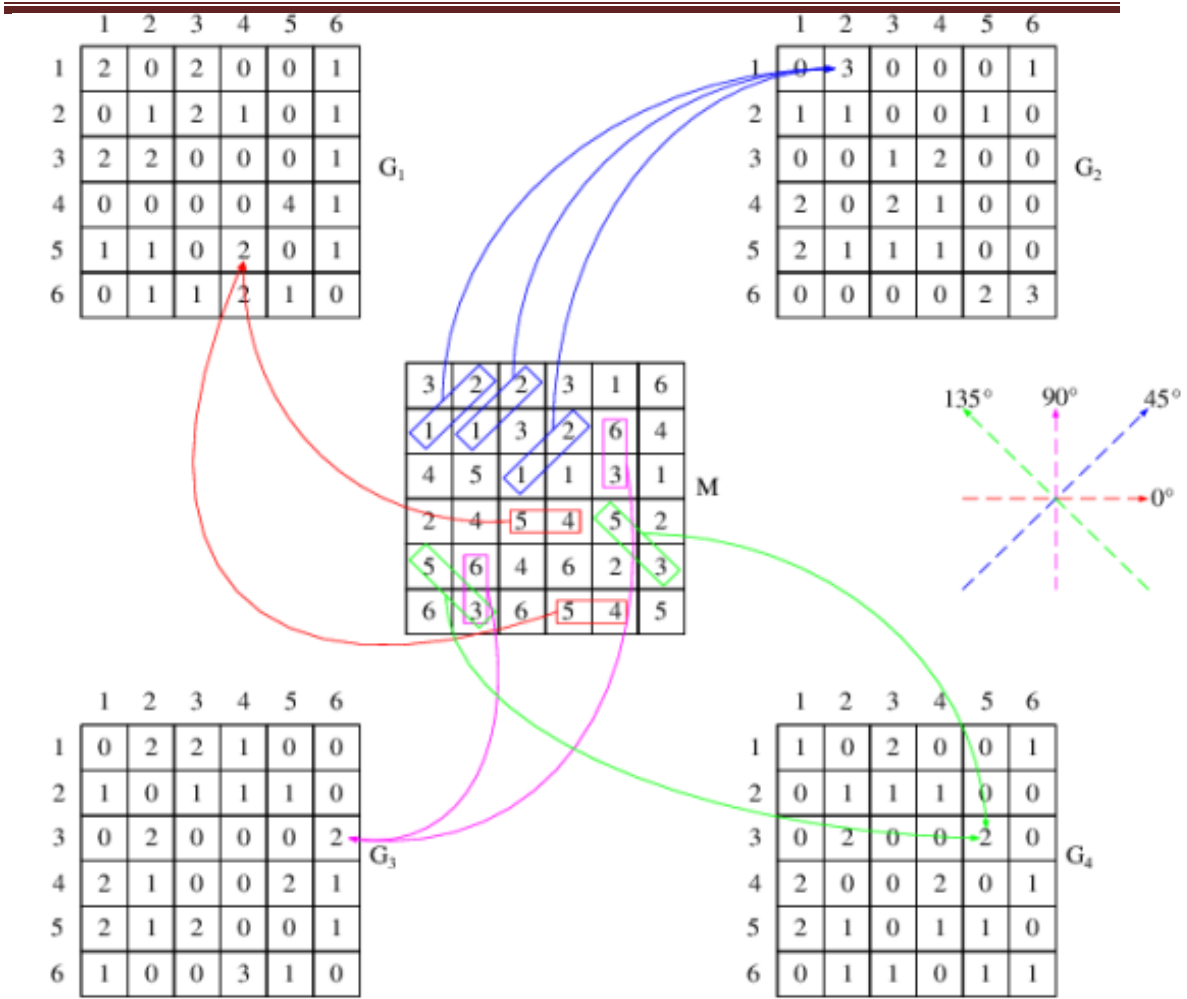


Figure 2.3: Formation de la matrice de cooccurrence GLCM.

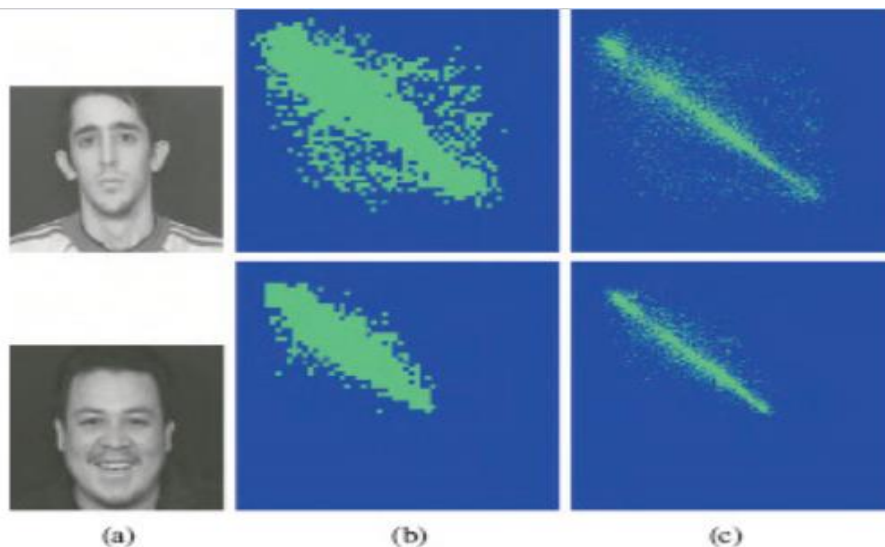


Figure 2.4 : Exemple sur deux images de visages (b) matrice de cooccurrence avec 64 niveaux de gris (c) avec 256 niveaux de gris.

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

La taille de la matrice de cooccurrence peut prendre de très grandes valeurs en dépendance avec le nombre de niveaux de gris de l'image, la matrice d'une image codée sur 8 bit (256 niveaux de gris) aura 256×256 éléments, ce qu'est pénalisant en termes de temps de calcul dès les résolutions plus élevées. Pour cette raison qu'on procède souvent à la quantification de l'image avant le calcul du GLCM.

Dans la plupart des applications, une seule matrice calculée qui est la somme des matrices obtenues pour $q = 0^\circ, 45^\circ, 90^\circ$ et 135° ; cette matrice dépend alors, plutôt du paramètre D . De plus, souvent, pour une direction donnée, on ne se préoccupe pas du sens de parcours, ce qui revient à rendre la matrice symétrique.

La matrice de cooccurrence contient un très grand nombre d'information, Ce qui les rend difficile à être exploiter directement, C'est pourquoi Haralick a proposé d'en extraire 14 attributs qui décrivent les caractéristiques physiques de la texture. Ces 14 attributs sont :

Caractéristique de la texture	Description	Formule
1. L'énergie(ou moment angulaire second).	L'énergie mesure l'homogénéité de l'image. Plus cette valeur est faible, moins l'image est uniforme et l'image contient beaucoup de variation de couleur. (i, j) : coordonnées dans la matrice. $P(i, j)$: valeurs normalisées de la matrice. Valeur dans l'intervalle $[0,1]$.	$f_1 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p(i, j)^2$
2. Le contraste (ou inertie).	L'inertie mesure les variations locales des couleurs. Si ces variations sont importantes, alors le contraste sera élevé. Ce paramètre est fortement non corrélé à l'énergie. Valeur dans l'intervalle $[0, (Ng-1)]$.	$f_2 = \sum_{n=0}^{Ng-1} n^2 \left\{ \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} P i-j = n^{(i,j)} \right\}$
3. Corrélation.	Où μ_x, μ_y, σ_x et σ_y sont respectivement les moyennes et les écarts type de p_x et p_y . Ce paramètre permet de déterminer si certaines colonnes de la matrice sont	$f_3 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} \frac{(i - \mu_x)(j - \mu_y)p(i, j)}{\sigma_x \sigma_y}$

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

	égales, c'est-à-dire s'il existe des dépendances linéaires dans l'image. En effet, plus les valeurs sont uniformément distribuées dans la matrice de cooccurrences et plus la corrélation est importante. Valeur dans l'intervalle [-1,1]. La corrélation n'est corrélée ni à l'énergie, ni à l'entropie.	
4. La variance.	La variance mesure la dispersion des valeurs autour de la moyenne. Plus ce paramètre est élevé et plus importants sont les écarts entre les valeurs et la moyenne. Elle représente l'hétérogénéité de la texture.	$f_4 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} (i - \mu)^2 p(i, j)$
5. Moment différentiel inverse (Homogénéité).	Ce paramètre mesure l'homogénéité de l'image, plus l'image contient de régions homogènes, plus il est élevé. Valeur dans l'intervalle [0,1].	$f_5 = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} \frac{p(i, j)}{1 + (i - j)^2}$
6. Moyenne des sommes.	Cela fait référence à la moyenne statistique des sommes des lignes ou des colonnes dans la matrice de co-occurrence des niveaux de gris (GLCM) C'est une mesure du niveau de répétitivité ou de régularité des motifs de niveaux de gris présents dans l'image. Elle donne une idée du degré global de répétition des intensités ; plus cette valeur est élevée, plus la distribution des niveaux de gris est régulière.	$f_6 = \sum_{k=2}^{2Ng} k p_{x+y}(k)$
7. Variance des sommes.	Il représente la dispersion des sommes autour de leur moyenne, et mesure le degré de variation ou de diversité dans la répétition des niveaux de	$f_7 = \sum_{k=2}^{2Ng} (k - f_6)^2 p_{x+y}(k)$

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

	gris dans l'image. Si la valeur est élevée, cela indique une grande variance de texture, c'est-à-dire des changements marqués dans le motif de l'image. En revanche, si la valeur est faible, cela reflète une texture régulière et homogène.	
8. Entropie des sommes.	Elle mesure le degré d'aléa ou de désordre dans les sommes des valeurs de la GLCM. Plus l'entropie est élevée, plus la distribution des niveaux de gris est aléatoire, ce qui reflète une texture irrégulière et complexe. En revanche, une entropie faible indique une texture plus organisée et répétitive.	$f_8 = - \sum_{k=2}^{2Ng} p_{x+y}(k) \log\{p_{x+y}(k)\}$
9. Entropie.	Ce paramètre mesure le désordre dans l'image. sa valeur sera élevée en cas de texture complètement aléatoire (sans structure apparente). Lorsque les valeurs de la matrice de cooccurrences sont presque toutes égales, l'entropie est élevée.	$f_9 = - \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p(i, j) \log\{p(i, j)\}$
10. Variance des différences.	Mesure la dispersion ou la diversité des différences de niveaux de gris entre les pixels adjacents dans l'image. Valeur élevée → texture irrégulière avec des variations marquées. Valeur faible → texture homogène avec de faibles variations. Ce paramètre est utilisé pour l'analyse de texture d'image et la distinction des motifs.	$f_{10} = \sum_{k=0}^{Ng-1} \left[k - \sum_{l=0}^{Ng-1} l p_{x-y}(l) \right]^2 p_{x-y}(k)$

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

11. Entropie des différences.	Valeur dans l'intervalle [0,2. Log (Ng-1)]	$f_{11} = - \sum_{k=0}^{Ng-1} p_{x-y}(k) \log\{p_{x-y}(k)\}$
12. Information sur la corrélation 1.	Soient : P_x, P_y les probabilités selon x et y, et H_X, H_Y leurs entropie respective.	$f_{12} = \frac{f_9 - H_{XY1}}{\max(H_X, H_Y)}$
13. Information sur la corrélation 2.	$H_X = - \sum_{i=1}^{Ng} p_x(i) \log\{p_x(i)\}$ $H_Y = - \sum_{j=1}^{Ng} p_y(j) \log\{p_y(j)\}$ $H_{XY1} = - \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p(i,j) \log\{p_x(i)p_y(j)\}$ $H_{XY2} = - \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p_x(i)p_y(j) \log\{p_x(i)p_y(j)\}$	$f_{13} = (1 - \exp[-2(H_{XY2} - f_9)])^{1/2}$
14. Coefficient de corrélation maximal.	Soient la matrice : $Q(i,j) = \sum_{k=1}^{Ng} \frac{p(i,k) p(j,k)}{p_x(i) p_y(j)}$ $V = 2^{eme}$ Plus grande valeur propre de Q	$f_{14} = \sqrt{V}$

Tableau 2.2: Les 14 paramètres de Haralick.

$p_x(i)$ et $p_y(j)$ sont les probabilités marginales.

$$p_x(i) = \sum_{j=1}^{Ng} p(i,j)$$

$$p_y(j) = \sum_{i=1}^{Ng} p(i,j)$$

μ_x et μ_y sont les moyennes de $p_x(i)$ et $p_y(j)$ définies par :

$$\mu_x = \sum_{i=1}^{Ng} i p_x(i)$$

$$\mu_y = \sum_{j=1}^{Ng} j p_y(j)$$

Chapitre 2 : Analyse des paramètres de Haralick pour la reconnaissance de visage

σ_x et σ_y sont les écarts types de $p_x(i)$ et $p_y(j)$:

$$\sigma_x = \left(\sum_{i=1}^{Ng} p_x(i) (i - \mu_x)^2 \right)^{1/2}$$

$$\sigma_y = \left(\sum_{j=1}^{Ng} p_y(j) (j - \mu_y)^2 \right)^{1/2}$$

$$p_{x+y}(k) = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p_{i+j=k}(i, j); k = 2, 3, \dots, 2N$$

$$p_{x-y}(k) = \sum_{i=1}^{Ng} \sum_{j=1}^{Ng} p_{i-j=k}(i, j); k = 0, 1, \dots, N - 1$$

Les attributs f6, f7, f8, f10, f11, f12, f13 et f14 apportent des informations supplémentaires sur les degrés d'homogénéité et de complexité de l'image, ainsi que sur la corrélation. La méthode d'extraction de ces paramètres basée sur le calcul des matrices de cooccurrences est une des méthodes les plus proches de la notion de texture. Elles mettent effectivement en avant les relations qui existent entre les pixels de l'image en faisant intervenir l'aspect local (les niveaux de gris) et l'aspect spatial (δ, θ). Cependant, ces matrices sont calculées de façon globale pour toute l'image, ce qui n'est pas sans poser de problème quand nous savons qu'il est possible d'avoir plusieurs textures différentes dans une même image. Suggère de calculer des matrices de cooccurrence avec différentes directions et d'en faire la moyenne afin d'obtenir une seule matrice représentant les caractéristiques de la texture dans toutes les directions. [26]

2.4 Conclusion :

Dans ce chapitre, nous avons mis en lumière les différents types de reconnaissance faciale, et nous avons expliqué en détail la technique utilisée pour la reconnaissance du visage.

Chapitre 3 :
Environnement de Travail

3.1 Introduction :

Le but pratique de la reconnaissance Biométrique est d'avoir un système performant et applicable dans la réalité ; malgré tous les problèmes existant dans la réalité et qui perturbe la qualité de ces systèmes. On cite comme exemple les problèmes de bruit des systèmes électronique utilisé pendant le processus d'acquisition et de stockage des données. Les protocoles de test doivent être conçus soigneusement pour éviter les défauts méthodologiques, qui se produisent si l'algorithme de vérification est examiné en utilisant les mêmes données qui ont été employées pour la conception. Et comme notre objectif repose sur une modalité spécifique qui est la reconnaissance de visage, plusieurs banques d'images ont été créées afin de comparer les différentes méthodes entre elles selon diverses conditions (éclairage, pose, occultations, etc.). Parmi celles-ci, il y a notamment la FERET, AR-face, AT&T (appelée auparavant Olivetti), XM2VTS, Yale, MIT, Achermann ainsi que plusieurs autres. Chacune d'entre elles possède évidemment ses particularités spécifiques ainsi que ses qualités et Défauts. Nous allons présenter dans ce chapitre, la base de données des visages qui a été choisie pour nos expériences. Ainsi le protocole expérimental qui a été soigneusement conçu pour cette base de données. La base de données que nous avons travaillée sur laquelle est une base multimodale développée au sein du projet européen ACTS, elle contient des images fixes, des séquences vidéo et des images faciales de 295 personnes. Elle est utilisée pour la vérification d'identité. La base de données XM2VTS a été réalisée sur une longue période ce qui a permis d'obtenir plusieurs images d'une même personne et donc une grande variabilité d'apparence (changement de coiffure, présence et/ou absence de lunettes, ...etc.). Par contre, seules les expressions neutres ont été considérées. La motivation pour le choix de cette base de données est principalement sa taille tout à fait grande, et sa popularité. On a choisi la base de données prolongée XM2VTS puisqu'elle est devenue une norme dans la communauté biométrique audio et visuelle de vérification d'identité. [27]

3.2 Présentation de la base de données XM2VTS :

XM2VTS est une base de données multimodale publiquement disponible, elle est enregistrée spécifiquement pour évaluer l'exécution des approches biométriques à la vérification d'identité. Elle contient les enregistrements synchronisés des visages et des paroles de 295 personnes. Les sujets ont été enregistrés en quatre sessions séparées uniformément distribuées pendant 5 mois. En effet, C'est le centre CVSSP

(Centre for Vision, Speech and Signal Processing), de l'université de Surrey, en grande Bretagne, qui a conçu la base de données XM2VTS, pour permettre la comparaison de différentes méthodes de vérification d'identité. Elle succède à la base de données M2VTS (Multi Modal Vérification for Téléservices and Security applications). Sa construction s'inscrit dans le cadre du projet européen ACTS qui a pour but d'étudier le contrôle d'accès par une vérification multimodale d'identité. La session se compose de deux enregistrements. Un enregistrement pour les séquences de la parole et un enregistrement pour les séquences vidéo de la tête. Pour chaque personne huit prises ont été effectuées en quatre sessions distribuées pendant cinq mois afin de prendre en compte les changements d'apparence des personnes selon plusieurs facteurs (lunettes, barbe, coupe de cheveux, pose...). Les vidéos et photos sont en couleur de haute résolution (format ppm), la taille est de 256 x 256 pixels pour les images et de très bonne qualité codé sur 24 bits dans l'espace RGB. Cela permet de travailler en niveaux de gris ou en couleur. Le choix principal de XM2VTS est sa taille grande, avec 295 personnes et 2360 images en total et sa popularité puisqu'elle est devenue une norme dans la communauté biométrique audio et visuelle de vérification multimodale d'identité.

Nous ne nous intéresserons évidemment, dans le cadre de ce projet, qu'aux photographies prises de face pour le processus de l'authentification de visage. L'éclairage des faces de ces deux ensembles est contrôlé. La figure 3.1 présente des images de face typiques de la base de données XM2VTS.[27]



Figure 3.1 : Images typiques de la base de données XM2VTS.

3.3 Le protocole de Lausanne :

Si on parle d'une base de données pour la vérification d'identité cela veut dire la nécessiter d'un protocole performant qui permet la comparaison entre les algorithmes de vérification. Pour la base de données XM2VTS le protocole associé s'appelle le protocole de lausanne. Son principe est de partager la base de données en deux classes, 200 personnes pour les clients, et 95 pour les imposteurs.

La base de données est divisée en trois ensembles : apprentissage, évaluation et test. L'ensemble apprentissage permet de construire les modèles de clients. L'ensemble test est utilisé pour calculer les scores des clients et des imposteurs. En fonction de ces scores, un seuil est choisi afin de déterminer si une personne est acceptée ou non.

- 1. L'ensemble d'apprentissage** : il contient l'information concernant les personnes connues du système (seulement les clients).
- 2. L'ensemble d'évaluation** : permet d'établir les paramètres du système de reconnaissance de visage.
- 3. L'ensemble de test** : permet de tester le système en lui présentant des images de personnes lui étant totalement inconnues.

Il existe Deux configurations différentes, la configuration I et la configuration II.

Chapitre 3 : Environnement de Travail

Nous utiliserons la configuration I dans le cadre de cette thèse puisqu'elle est la plus dure. Dans la configuration I, pour la formation de l'ensemble d'apprentissage trois images par client sont employées afin de créer les caractéristiques ou modèles clients. L'ensemble d'évaluation est constitué de trois autres images par client, ils sont utilisés essentiellement pour fixer les paramètres de l'algorithme de reconnaissance ou de vérification des visages. L'ensemble de test est formé par les deux autres images restantes.

Pour la classe des imposteurs, les 95 imposteurs sont réparties dans deux ensembles : 20 pour L'ensemble d'évaluation et 75 pour l'ensemble de test.[28]

La répartition des images selon la configuration I est représentée par la figure 3.2.

Session	Pause	Clients	Imposteurs	
1	1	Apprentissage	Evaluation	Test
	2	Evaluation		
2	1	Apprentissage		
	2	Evaluation		
3	1	Apprentissage		
	2	Evaluation		
4	1	Test		
	2			

Figure 3.2 : Répartition des images de la base de données selon la configuration I.

Dans la configuration II, pour la catégorie clients, quatre images par clients des deux premières sessions sont employées pour former l'ensemble d'apprentissage et les deux images de la troisième session constituent l'ensemble d'évaluation, alors que les deux images restantes de la quatrième session constituent l'ensemble de test. Pour la catégorie imposteurs la répartition est identique à la répartition de la configuration I. La répartition dès l'images selon la configuration II est représentée par la figure 3.3.

Session	Pause	Clients	Imposteurs	
1	1 2	Apprentissage	Evaluation	Test
2	1 2			
3	1 2	Evaluation		
4	1 2	Test		

Figure 3.3 : Répartition des images de la base de données selon la configuration II.

Les tailles des différents ensembles de la base de données selon les deux configurations citées précédemment sont reprises dans le tableau 3.1.

Ensemble	Clients	Imposteurs
Apprentissage	600 images (3 par personne)	0 images
Evaluation	600 images (3 par personne)	200 images (8 par personne)
Test	200 images (2 par personne)	560 images (8 par personne)

Tableau 3.1 : Répartition des photos dans les différents ensembles.

3.4 Conclusion :

Dans ce chapitre, nous avons présenté la base de données d'images de visages XM2VTS, choisie en raison de sa popularité et de son adoption comme référence dans la communauté biométrique audiovisuelle pour la vérification d'identité. Cette base permet de comparer efficacement les résultats obtenus à l'aide la technique explorée dans cette thèse avec ceux proposés par d'autres chercheurs. Notre choix s'est également porté sur cette base car elle contient des images facilement convertibles en niveaux de gris, ce qui est particulièrement pertinent dans le cadre de notre travail. En effet, nous nous intéressons ici à l'analyse des visages à partir d'images en nuances de gris afin d'évaluer dans quelle mesure les informations d'intensité lumineuse, indépendamment de la couleur, peuvent contribuer à l'authentification faciale. Le chapitre suivant décrit les différents traitements appliqués sur ces images en niveaux de gris.

Chapitre 4 :
Mise en œuvre et Résultats

4.1 Introduction :

Après avoir présenté la technique de reconnaissance faciale dans le chapitre précédent, il est maintenant temps d'appliquer cette technique de manière pratique pour analyser ses avantages et ses inconvénients, notamment en termes de taux de succès et de temps de calcul pour le processus d'authentification faciale. En effet, l'efficacité de cet algorithme dépend largement de la qualité des résultats de détection et de normalisation des visages.

Les expériences ont été réalisées sur les visages de la base de données **XM2VTS**, qui contient des images prises dans des conditions idéales (vue frontale pour toutes les images, éclairage constant sur les visages et une distance fixe entre le visage et la caméra). Le choix principal de cette base de données est sa grande taille, comprenant 295 personnes et un total de 2360 images. De plus, elle est populaire, étant devenue une norme dans la communauté biométrique audio et visuelle pour la vérification multimodale de l'identité. Pour chaque personne, huit prises ont été réalisées lors de quatre sessions réparties sur cinq mois. Le protocole associé à **XM2VTS** divise la base en deux catégories : 200 clients et 95 imposteurs, avec des personnes des deux sexes et de différents âges. Les images sont en couleur et de haute qualité, avec une taille de (256x256).[13]

La figure 4.1 représente quelques exemples d'images de visages de la base de données XM2VTS.



Figure 4.1 : quelques exemples d'images de visages de la base de données XM2VTS. Le système de reconnaissance de visage peut être composé de trois étapes à savoir : la détection et prétraitement de visage, extraction de caractéristiques et reconnaissance de visages.

4.2 Prétraitement :

Le prétraitement est une phase importante dans le processus d'authentification ; c'est une méthode simple qui augmente en général les performances du système. Elle permet souvent une première réduction des données et elle atténue les effets de

différentes conditions lors des prises de vues. En regardant les images on aperçoit directement qu'apparaissent au niveau du cou des particularités non souhaitées comme les cols de chemise,... etc. par ailleurs les cheveux sont également une caractéristique changeante au cours temps. C'est pourquoi nous avons décidé de couper les images dont l'opération est d'extraire seulement les paramètres essentiels pour l'identificateur et qui changent très peu avec le temps. On utilise filtrage uniforme passe-bas pour la décimation. Quand les images sont filtrées par un filtre passe-bas, on peut réduire bien étendu la résolution des images. Ainsi les images de dimension (N x M) après découpage se transforment en une dimension (N/2 x M/2) après décimation (voir figure 4.2 puis nous faisons la photo normalisation aux images. La photonormalisation a un double effet : d'une part elle supprime pour tout vecteur un éventuel décalage par rapport à l'origine et ensuite elle supprime tout effet d'amplification (multiplication par un scalaire). Pour chaque image on effectue l'opération suivante :

$$\textit{photonormalisation}(x) = \frac{x - \textit{mean}(x)}{\textit{std}(x)}$$

Finalement on applique la normalisation qui s'agit sur un groupe d'image (pour chaque composante, on retire la moyenne de cette composante pour toutes les images et on divise par la déviation standard)

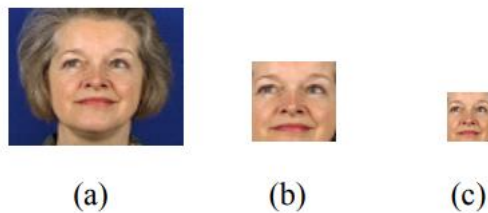


Figure 4.2 : a) image d'entrée, b) image après découpage et c) image après décimation.

4.3 Extraction des caractéristiques

L'extraction des caractéristiques se fait par la méthode expliquée déjà dans le chapitre 02.

4.4 Classification

Dans le problème de vérification d'identités, nous cherchons à définir, pour chaque

personne, ou de manière globale, un seuil. Ce dernier va déterminer le minimum de ressemblance entre deux images pour admettre qu'il s'agit de la même personne. Ce minimum de ressemblance va s'exprimer comme une distance maximale entre les caractéristiques des deux images. Le problème qui nous occupe il contient deux classes, à savoir d'une part les clients et d'autres part les imposteurs. Un système d'authentification impitoyable et extrêmement strict indique un TFA (Taux de Fausse Acceptation) faible et un TFR (Taux de Faux Rejet) élevé. Par contre un système laxiste sera caractérisé par un TFA élevé et un TFR plutôt bas. Le juste milieu situe quelque part entre les deux, et si les taux d'erreurs sont égaux, il se trouvera au taux d'égale erreur ou TEE.

Tous ces taux d'erreurs ont été calculés dans deux ensembles d'abord dans un ensemble d'évaluation, qui va permettre de fixer plus ou moins le TEE en faisant varier les paramètres d'acceptation et de rejet du système. Ensuite, dans un ensemble de test en utilisant les paramètres fixés précédemment. Ainsi, on peut vérifier la robustesse du système d'authentification de visage.

4.5 Mesure de similitude :

Une fois que les caractéristiques des images sont extraites, il reste à déterminer quelles sont les images semblables. Il y a beaucoup de mesures possibles de distance et de similitude, mais ici on a choisi la corrélation puisque nous donne les meilleurs résultats par rapport aux d'autre mesure de similitude et parce que la corrélation est mieux adaptée à des données de la grande dimension. Elle mesure le taux de changement entre les composantes de deux vecteurs A et B . Elle est donnée par la relation :

$$cor(A, B) = \sum_{i=1}^N \frac{(A_i - \mu_A)(B_i - \mu_B)}{\sigma_A \sigma_B}$$

Où : σ_A = l'écart type de A , μ_A = la moyenne de A_i .

σ_B = l'écart type de B , μ_B = le moyenne de B_i .

4.6 Présentation des résultats de la technique utilisée :

Nous extrayons la matrice de cooccurrence pour chaque image de visage après l'enchaînement ligne par ligne de la matrice de cooccurrence on obtient un vecteur caractéristique de taille $(Ng \times Ng)$ où Ng est le nombre des niveaux de gris contient sur

Chapitre 4 : Mise en œuvre et Résultats

l'image on a choisi $N_g=16$. Les paramètres choisis sont : la distance $d=1$, l'angle $\theta=0^\circ, 45^\circ, 90^\circ$, et 135° .

La taille de vecteur caractéristique des caractéristiques de Haralick de la matrice de concurrence est égale à 14. Cela veut dire une faible consommation du mémoire de stockage des données. Et cette taille de vecteur est indépendante de la taille de l'image. Les résultats de l'authentification de visage par ces 14 paramètres de Haralick de chaque image sont montrés dans le tableau ci-dessous. Avec un angle égal à 45° on trouve le maximum taux de succès de l'ordre de 66.09%

Niveaux de gris $N_g=16$ $d=1$	Ensemble d'évaluation			Ensemble de Test		
	TFR	TFA	TEE	TFR	TFA	TS (%)
Vecteur de Haralick_14 0°	0.1483	0.1484	0.148	0.2150	0.1479	63.71
Vecteur de Haralick_14 45°	0.1517	0.1525	0.152	0.1900	0.1491	66.09
Vecteur de Haralick_14 90°	0.1550	0.1557	0.155	0.1950	0.1536	65.14
Vecteur de Haralick_14 135°	0.1467	0.1472	0.147	0.1975	0.1439	65.86
Les 4 vecteurs de Haralick successive 52	0.1483	0.1492	0.148	0.2050	0.1509	64.41
La moyenne des vecteurs Harlick dans tous les angles 13	0.1467	0.1457	0.146	0.2050	0.1433	65.17

Tableau 4.1 : les résultats de 14 paramètres de Haralick avec 16 niveaux de gris et différents angles : $0^\circ, 45^\circ, 90^\circ, 135^\circ$.

4.7 Conclusion :

Dans ce chapitre, nous avons présenté et analysé les résultats des expériences du système de reconnaissance faciale basé sur les paramètres de Haralick extraits de la matrice de cooccurrence (GLCM). Les résultats ont montré que l'utilisation de ces paramètres permet une représentation efficace de la texture dans les images faciales, ce qui contribue à améliorer les performances du système de reconnaissance.

Les performances du système ont été évaluées selon plusieurs configurations, notamment le nombre de niveaux de gris (N_g), l'angle de calcul, ainsi que la taille du vecteur de caractéristiques obtenu. Les expériences ont démontré que les meilleures performances ont été atteintes avec $N_g = 16$ et un angle de 45° , où le taux de succès (TS) a atteint environ 66,09 % en utilisant uniquement les 14 paramètres de Haralick, ce qui reflète une grande efficacité dans la représentation des caractéristiques, tout en consommant peu de mémoire, en raison de la petite taille du vecteur, qui est indépendante de la taille de l'image.

CONCLUSION GENERALE :

Ce travail est destiné à l'authentification de visage à partir des images bidimensionnelles. Employé dans beaucoup d'application comme le contrôle d'accès, l'authentification des transactions, la répression et la personnalisation. On a choisi la reconnaissance faciale puisqu'elle offre plusieurs avantages : le système de capture (caméra) est facile à installer, il est accepté dans les lieux publics ce qui nous permet d'avoir des bases de données de plus en plus grandes et ainsi améliorer les performances de la reconnaissance.

Ces dernières années, la technique d'analyse de texture basée sur la matrice de cooccurrence des niveaux de gris (GLCM) a suscité un intérêt croissant dans le domaine de la reconnaissance faciale, en raison de sa capacité à extraire des informations précises sur la structure texturale de l'image. L'objectif de ce travail est de mettre en évidence l'efficacité de cette technique pour améliorer la précision des systèmes de vérification d'identité, en la combinant avec des algorithmes d'extraction de caractéristiques. Nous avons extrait des descripteurs de Haralick à partir de la matrice GLCM selon différents angles et directions, ce qui a permis une représentation plus complète du contenu textural des images faciales.

À la fin de ce travail, nous affirmons que l'utilisation des paramètres de Haralick extraits de la matrice de cooccurrence des niveaux de gris (GLCM) constitue un choix remarquable dans le domaine de la reconnaissance faciale, en raison de leur capacité à décrire avec précision les caractéristiques texturales des images. À travers des expérimentations menées sur la base de données bien connue XM2VTS, et en suivant le protocole de Lausanne, des résultats prometteurs ont été obtenus, confirmant l'efficacité de cette approche.

Les expériences ont montré que la meilleure performance du système a été atteinte avec un angle de 45° et 16 niveaux de gris, réalisant un taux de réussite de 66,09 %. Ce résultat est d'autant plus significatif qu'il a été obtenu avec des vecteurs simples composés de seulement 14 paramètres, assurant ainsi un bon compromis entre performance et précision de classification d'une part, et efficacité en termes de mémoire et de rapidité d'exécution d'autre part.

Ces résultats confirment que la combinaison des techniques d'analyse statistique de texture avec les systèmes de reconnaissance faciale peut offrir des solutions pratiques et efficaces pour les applications de vérification biométrique, ouvrant la voie à de futures améliorations reposant sur une exploitation plus approfondie des informations chromatiques et texturales.

REFERENCES :

- [1] allam, N. (2018). Application de l'analyse discriminante linéaire (LDA) dans la reconnaissance du visage. mémoire de master en informatique, Université Kasdi Merbah, Ouargla.
- [2] Djili, I. (Octobre2020). Système de reconnaissance d'iris par réseaux de neurones convolutionnels. mémoire de master , Kasdi Merbah , Ouargla.
- [3] Rayene, A., & CHOUFFA, N. (2021, 2022). Développement d'un système biométrique à partir des veines du doigt. U Université Badji Mokhtar, Annaba.
- [4] Aziza, B. (Juillet 2019). Identification des personnes par leurs empreintes palmaire. Mémoire de fin d'étude pour l'obtention du diplôme de Master Académique, Université 8Mai 1945, Guelma .
- [5] Sara, L., & Trabelsi, M. (2020). Reconnaissance de forme et classification automatique : Application à la prédiction du genre et l'estimation de l'âge. Mémoire de Master 2 en Administration et Sécurité des Réseaux, Kasdi Merbah, Ourgla.
- [6] Fayza, B., & FADLI, N. (2022). Conception d'un système d'authentification et d'identification basé sur la biométrie d'iris. Mémoire de master.
- [7] Farid AYECHÉ, ., E. (2018). Traitement automatique d'images de visages algorithmes et architecture. Mémoire de Doctorat en Sciences en Informatique, Université Farhat Abbas, Sétif.
- [8] Aziz, Z. A., & BOUDIB, M. T. (2017). Etude et réalisation d'un système de reconnaissance de faces humaines par la méthode des faces propre. Mémoire de Master, Blida 1.
- [9] RAZIKA, M. (2012). RECONAISSANCE BIOMETRIQUE DU VISAGE PAR L'ANALYSE EN COMPOSANTES PRINCIPALES . Mémoire De Master en Génie Électrique et Informatique, UNIVERSITE KASDI-MERBAH, OUARGLA.
- [10] Bentauza, M. C. (2013). Reconnaissance faciale avec caméra pour le controle. Mémoire de master, Mouhamed Khider, biskra.

- [11] BéchairiaNadjoua. (Juin 2019). Reconnaissance Du Visage Dans Des Conditions D'Eclairage Variant. Mémoire de Master Académique, Université 8 Mai 1945 , Guelma.
- [12] NADJETTE, A. (Juin 2020). Mise au point d'une application de reconnaissance faciale. Mémoire de master académique en Informatique, Université Mohamed Khider , BISKRA.
- [13]Meriem, F. (2013). Combinaisons de données d'espaces couleurs et de méthodes de vérification d'identité pour l'authentification de visages. Thèse présentée en vue de l'obtention du diplôme de Doctorat en sciences en automatique, Université Mohamed Khider, Biskra.
- [14] Klontz, A. (2013.J.). Face recognition vendor test 2013: Performance of face recognition algorithms. National Institute of Standards and Technology (NIST).
- [15] Buolamwini, & Gebru, T. (2018). Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classificatio. Proceedings of the 1st Conference on Fairness, Accountability, and Transparency (FAT).
- [16] Kotz, P. S. (2020). Privacy Implications of Face Recognition Systems. Journal of Privacy and Confidentiality.
- [17] Ding, R. G., & Cohn, J. F. (2000). Facial recognition under varying illumination. IEEE Transactions on Image Processing.
- [18] Sullivan, R. J. (2020). The Ethics of Facial Recognition. Journal of Ethics and Information Technology.
- [19] Commission, E. (2021). Proposal for a Regulation of the European Parliament and of the Council on Artificial Intelligence (AI Act). European Commission.
- [20] Korshunov, A., & . Marcel, S. (2020). Deepfakes: A Survey. Proceedings of the International Conference on Biometrics.
- [21] Saleh, M. M. (2021). Reconnaissance de visage basée sur une approche triangulaire.Mémoire de master, BADJI MOKHTAR , ANNABA.

- [22] Beveridge, R., & Kirby, M. (2005). Biometrics and Face Recognition. P 25. IS&T Colloquium.
- [23] Fathi, B. A. (2013-2014). Extraction des caractéristiques pour l'analyse biométrique d'un visage. Mémoire MASTER ACADEMIQUE, UNIVERSITE KASDI MERBAH , OUARGLA.
- [24] Bouchra, K. (2012). Mise au point d'une application de reconnaissance faciale.Mémoire Maste, Université Abou Bakr Belkaid, Tlemcen.
- [25] Abdelfeteh, B. (2020). Analyse des paramètres de Haralick pour la classification des anomalies mammaires. université 8 Mai 1945, Guelma.
- [26] R. M. Haralick, «. ». (1979). Statistical and structural approaches to texture. vol. 67(no. 5), p786–804.
- [27] Messer, K., Matas, J., Kittler, J., & Jonsson, K. (Mars 1999). Xm2vtsdb : The extended m2vts databas., (pp. pages 72–77).
- [28] Luetin, J., & Maitre, G. (1979). Evaluation protocol for the extended M2VTS database.(IDIAP,available)Récupérésur<http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/faceavbpa2001/protocol.ps>.