République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur et de la recherche scientifique
Université 8Mai 1945 – Guelma
Faculté des sciences et de la Technologie
Département d'Electronique et Télécommunications

Mémoire de fin d'étude
pour l'obtention du diplôme de Master Académique

Domaine : **Sciences et Technologie**
Filière : **Electronique**
Spécialité : **Instrumentation**
Thème :

Reconnaissance du visage sous l'éclairage invariant par la méthode TanTriggs

Présenté par :

Boualleg Sihem
Saad Khorchef Fatma

Sous la direction de :

Dr. BOUALLEG ABDELHALIM

Juillet 2021

REMERCIEMENT

Tout d'abord, nous remercions Dieu Tout-Puissant de nous éclairer sur le droit chemin

Nous adressons nos plus vifs remerciements à :

Nos chers parents pour leur soutien et leurs encouragements tout au long de nos années scolaires sans lesquelles nous n'aurions jamais réussi.

Le maître A.H Boualleg pour avoir accepté de nous encadrer en fin de thèse, pour son aide et sa disponibilité tout au long de cette période.

Nous remercions également les membres du jury pour le temps précieux qu'ils ont consacré à l'étude de notre mémoire.

Nos remerciements et notre gratitude vont aux professeurs et enseignants du département d'électronique ainsi qu'aux étudiants et au personnel qui ont travaillé avec nous tout au long de notre université.

Nos proches, amis et toutes les personnes qui nous ont aidé de près ou de loin à réaliser cet humble travail.

Dédicace Sihem

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mon cher frère et soeur pour leurs encouragements constants et leur soutien moral,

À ma petite famille, mon cher mari et ma chère fille Anfal, pour leur amour, leurs encouragements et leur soutien constant.

A mes proches et à tous les membres de ma famille, en particulier mon cher oncle, pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Merci d'être toujours là pour moi.

Dédicace Fatima

A mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs et frères pour leurs encouragements permanents, et leur soutien moral,

A mes proches et toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Merci d'être toujours là pour moi.

الملخـــص

نظام التعرف على الوجه، الذي أصبح اليوم من أكثر الأنظمة استخدامًا في عمليات الأمن والمراقبة، وعلى الرغم من التطور التكنولوجي الكبير الذي عرفه، إلا أنه لا يزال حساسًا ويتدهور أداؤه عند تغيير في ظروف التصوير سواء من حيث الإضاءة أو التغييرات التي تطرأ على الوجه نتيجة التقدم في العمر أو تعابير الوجه .... إلخ. العمل المنجز في إطار هذه الأطروحة هو محاولة تحسين أداء نظام التعرف على الوجه عندما تكون ظروف الإضاءة سيئة وغير متوازنة. بعد دراسة مشكلة الإضاءة في صور الوجوه المراد التعرف عليها، وعرض الطرق والحلول المختلفة التي ساهمت في تحسين أداء هذه الأنظمة، تركزت على نظريات تعديل الضوء والأساليب المحلية أو الشاملة، تم اقتراح حلول لكل خطوة من خطوات التعرف على الوجه.

أدت الحلول المقترحة في كل مستوى من هذه السلسلة إلى تحسين أداء كبير مقارنة بالطرق التقليدية. بالنسبة لخوارزميات التعرف حيث تم اقتراح معالجة الصورة بتقنية TT لموازنة الإضاءة والتي تهتم بفصل الضوء عن الصورة ومن ثمة استعمال الواصف المحلي LPQ لمطابقة الصور المراد التعرف عليها، في هذا العمل لإجراء التجارب التطبيقية على قاعدة البيانات Yale B و Yale B étendu وهذا للتمكن من مقارنة النتائج لمعرفة مدى تحسنها كون هذه القاعدة من أكثر القواعد استغلال في الدراسات الأكاديمية .

الكلمات الدلالية: معرفة الوجه، الوصف المحلي LPQ..TT

Résumé

Le système de reconnaissance faciale, qui est devenu aujourd'hui l'un des systèmes les plus utilisés dans la sécurité et les opérations de surveillance, et malgré le grand développement technologique qu'il et connue, ils sont toujours sensibles et leurs performances se détériorent, lorsqu'il y a un changement dans les conditions de prise de vue, que ce soit en termes d'éclairage ou de changement de l'accueil du visage avilissement ou d'expressions de visage, ... etc. Le travail effectué dans le cadre de cette mémoire est d'essayer d'améliorer les performances du système de reconnaissance faciale lorsque les conditions d'éclairage sont mauvaises et déséquilibrées. Après avoir l'étudié la problématique de l'éclairage dans les images de visages à reconnaître, et présenté les différentes méthodes et solutions qui ont contribué à améliorer les performances de ces systèmes, centrés sur les théories de la modification de la lumière et les méthodes de description locales ou globales, des solutions ont été proposées pour chaque étape de la reconnaissance faciale.

Les solutions proposées à chaque niveau de cette chaîne ont apporté une amélioration significative des performances par rapport aux approches classiques. Pour les algorithmes de reconnaissance, nous avons proposé l'utilisation la méthode TT (Tan et Triggs) pour la normalisation d'éclairage, qui concerne la séparation de la lumière de l'image, et l'utilisation du descripteur local LPQ (Local Phase Quantization) pour faire comparer les images à reconnaître, dans ce travail an à mener des expériences pratiques sur la base de données YaleB et YaleB étendues, afin d' avoir comparé les résultat et connaître l'amélioration ou la dégradation, puisque les deux cette base de donnée est la plus utilisée dans les études académiques.

Mots clés: Reconnaissance facial, TT, description locale LPQ.

Abstrat

The facial recognition system, which today has become one of the most widely used systems in security and surveillance operations, and despite the great technological development that it has known, they are still sensitive and and their performance is improving. deteriorate, when there is a change in the shooting conditions, whether in terms of lighting or change in the reception of the face debasement or facial expressions, ... etc. The work done within the framework of this thesis is to try to improve the performance of the facial recognition system when the lighting conditions are bad and unbalanced. After having studied the problem of lighting in the images of faces to be recognized, and presented the different methods and solutions that have contributed to improving the performance of these systems, centered on the theories of the modification of light and the methods of local or global description, solutions have been proposed for each step of facial recognition.

The solutions proposed at each level of this chain have brought an improvement significant performance compared to conventional approaches. For algorithms of recognition, we proposed the use of the TT method (Tan and Triggs) for lighting normalization, which concerns the separation of light from the image, and the use of the local descriptor LPQ (Local Phase Quantization) to make compare the images to be recognized, in this work year to conduct practical experiments on the extended YaleB and YaleB database, in order to have compared the results and know the improvement or degradation, since both this database is the more used in academic studies.

Keywords : Face recognition, TT, local description LPQ.

Sommaire

Chapitre II : La reconnaissance de visage

Chapitre III : Normalisation d'illumination et méthode de texture locale

Chapitre IV : Méthodologie et conception

Liste Des Figure

Liste Des tableaux

Introduction générale

Depuis quelques années, on observe l'émergence d'une tendance générale visant à rendre plus naturels les rapports hommes-machines. Il revient désormais à la machine de se comporter comme l'humain ou le dépasser pour certains.

Cet énorme développement technologique, permis de réaliser des systèmes peut communiquait avec l'être humain, et même capable de manipuler des compétences qui été réserver à l'être humain tell que, faire la déférence entre les vois, la déférence entre les individus, lire les humanisons sur les visages, …etc.

Les scientifiques dans l'heur recherche an améliorent la communication homme-machine en remarquées que le visage est un stimulus dont l'importance et la particularité dans la littérature scientifique. Etant la partie la plus expressive et communicative d'un être humain.

Le visage est le miroir de l'âme, il reflète la peur, la colère, la joie, la tristesse, le dégoût, la surprise ou le mépris, car il se concentre sur l'évaluation de la douleur du patient et de l'enfant, l'évaluation du nerf facial, le marketing ou même la conduite moins anticipée.

L'analyse simple est devenue un outil important pour vérifier ou identifier les individus, Principalement dans le domaine de la sécurité, il est utilisé comme moyen d'entrée dans les bâtiments hautement sécurisés, utile pour l'identification à la frontière, et comme moyen de paiement électronique depuis quelques années.

Les systèmes de reconnaissance faciale ou d'analyse faciale peuvent atteindre des taux de reconnaissance élevés lors de l'acquisition d'images dans de bonnes conditions , cependant, leurs performances seront fortement réduites lorsque les images proviennent d'acquisitions non contrôlées (faible luminosité, ombrage du visage, images d'interphone, etc.). Compte tenu de ce point, nous proposons d'améliorer la robustesse du taux de reconnaissance inférieur dans des conditions d'éclairage non contrôlées en fusionnant

d'abord les méthodes classiques, puis nous proposons une nouvelle forme d'utilisation des descripteurs.

Dans le premier chapitre est consacré à la présentation générale de la biométrie. Il décrit le principe de fonctionnement du système biométrique puis définit les outils utilisés pour évaluer ses performances.

Dans le deuxième chapitre, nous discuterons de la technologie la plus avancée de reconnaissance de visage. Nous utiliserons également des méthodes d'identification connues Mention des principes opérationnels et des enjeux liés à l'identification.

Dans le troisième chapitre est divisé en deux parties. Dans la première partie, nous allons présenter les dernières méthodes de normalisation d'illumination, et la méthode proposée est Tan et Triggs (TT). Dans la deuxième partie, nous présenterons les paramètres de région de texture binaire : LBP, LPQ et MB-LPQ,BISIF.

Dans le quatrième chapitre, nous limitons les résultats expérimentaux obtenus par chaque méthode en analysant leurs performances, puis discutons de l'interprétation des résultats. Enfin, la conclusion générale résumera les résultats obtenus par les différentes méthodes et apportera quelques points de vue sur les travaux futurs.

Chapitre I
La biométrie

I.1. Introduction

La biométrie constitue l'ensemble des technologies qui exploitent des caractéristique biométriques (physiques, comportementales ou biologiques) comme des moyens d'identification des individus.

Ces technologies exploitent les caractéristiques qui sont uniques chez les individus et ne peuvent être perdus ni volées ni reconstituées contrairement aux moyens classiques reposant sur des mots de passe ou des cartes magnétiques.

C'est pour cette raison que la biométrie apparaît comme l'une des meilleures technologies contre la fraude à l'identité. Le présent chapitre donne un aperçu sur les principales technologies biométriques qui sont disponibles ainsi que leurs comparatifs.

Il décrit également le principe de fonctionnement des systèmes biométriques et les outils utilisés pour mesurer leurs performances ainsi que leurs avantages et limites.

I.2. Définition

La biométrie s'impose de plus en plus comme alternative afin de remédier aux problèmes des méthodes précédentes. La biométrie est basée sur des caractéristiques propres à l'individu, qui ne peuvent n'être perdues. De plus, en pratique il n'est pas assez évident d'imiter une caractéristique biométrique. La biométrie permet de vérifier que l'usager est bien la personne qu'il prétend être. C'est une technologie qui utilise les caractéristiques physiques propres à chaque individu pour établir de façon aussi fiable que possible son identité.

Jouissant actuellement d'un certain engouement dû, sans doute, aux différents gadgets d'identification que l'on a pu voir dans certaines productions cinématographiques, la biométrie tend à envahir notre quotidien. Devant cette déferlante, il était nécessaire de faire le point sur ce qu'est exactement la biométrie, quelles techniques existent vraiment et leur degré de fiabilité.

La biométrie est une technique naissante qui nous permet de vérifier l'identité d'un individu en employant un ou plusieurs de ses caractéristiques personnelles. Donc, la reconnaissance biométrique est basée sur ce qui est un individu. Il existe plusieurs appondus biométriques, les plus connues étant:

• **Biologiques :** comme le sang, la salive, l'urine, l'odeur ou encore l'ADN…etc. Ces méthodes sont difficiles à mettre en œuvre pour une utilisation courante.

• **Comportementales :** comme la signature, les frappes clavier, la démarche (le mouvement des hanches, des bras et des épaules) …etc.

• **Morphologiques :** comme les empreintes digitales, le visage, l'iris, la rétine ou la forme de la main...etc.

• **Cachée :** comme la géométrie du cerveau, ECG et la biométrie de la main sans contact...etc. Ces techniques biométriques sont en cours de développement**.**

Pour assurer leurs fiabilités, les modalités biométriques doivent être déterminées par quelques caractéristiques. Parmi les propriétés d'une modalité biométrique, on trouve :

• **Universelles** : mesurables sur chaque individu.

• **Uniques** : différents entre-deux individus.

• **Permanentes** : invariables dans le temps.

• **Mesurables** : non coûteuse et non intrusives.

• **Précises** : peu de confusion entre individus.

• **Difficilement reproductibles**

Malheureusement, dans la pratique, on ne trouve pas toutes ces caractéristiques dans une même modalité. [1]

I.3. Un bref historique de la biométrie

La plus ancienne et célèbre méthode de reconnaissance est l'empreinte des mains (le pouce) qui est servi de signature lors des relations commerciales à Babylone (-3000 av. JC) et dans la Chine antique (7ème siècle). Selon le rapport de l'explorateur Joao de Barros.

Il a écrit que les marchands chinois relevaient les empreintes des mains et des pieds des enfants de jeune âge sur du papier en utilisant de l'encre afin de les distinguer les uns des autres**. [2]**

En 1684, l'Anglais Nehemiah Gro fut le premier scientifique à écrire des articles détaillés sur les empreintes digitales et les fameuses "nombreuses petites rides". Deux ans

plus tard, l'anatomiste italien Marcelo Malaga est le premier à utiliser un microscope pour examiner les empreintes digitales : il conclut : « Les rides des doigts peuvent être saisies, et les rides des jambes peuvent être tirées.

En 1823, le physicien tchèque Johannes Burkinje proposa de diviser les empreintes digitales en neuf types de motifs.

Puis, en 1860, le responsable britannique en Inde, William James Herschel, a souligné que "les rides sur les doigts représentant des empreintes digitales se sont formées avant la naissance des êtres humains et sont restées constantes tout au long de sa vie. À moins qu'il n'y ait une blessure profonde." Puis il imagina s'en servir pour signer des chèques. **[2]**

Le médecin écossais Henry Foulds travaille dans un hôpital japonais et a remarqué que les Japonais et les Chinois authentifient généralement les documents en utilisant leurs empreintes digitales. Sur cette base, il a affirmé dans une publication de 1880 que les empreintes digitales sont uniques à chaque personne et peuvent être utilisées pour identifier une personne.

En 1892, l'anthropologue anglais, Francis Galton, s'appuie sur toutes ces découvertes Pour décréter que les empreintes permettent l'identification d'un individu.

En 1775, le prêtre suisse Jean-Gaspar Lavatier publie un article sur la physionomie. Il est suggéré d'identifier une personne en observant le mouvement de son visage.

Quelques années plus tard, le médecin allemand François Joseph Gall s'opposa à Lavatier et avança une autre hypothèse, que ce n'était plus le visage qu'il fallait observer, mais le crâne qu'il fallait prendre en compte pour déterminer le caractère d'un individuel. En fait, ce crâne, selon lui, est disposé selon la forme du cerveau selon l'individualité.

Dans la même lignée, le docteur italien en médecine, Cesare Lombroso, propose en 1885 sa Théorie du criminel-né. Selon lui, le crime est le fait d'individus constitutionnellement procurés à cela, que l'on peut marquer par des traces physiques ou morphologiques dont il suffit de mettre l'inventaire. [3]

Cesare Lombroso, a donné un exemple, le poids du cerveau des honnêtes gens oscillerait de 1475 à 1550g, alors que chez les criminels, il serait de 1455g. Contre-exemple consternant pour les scientifiques : le cerveau de Léon Gambetta ne pèse que 1160g.

Alphonse Bertillon, responsable de l'identité judiciaire en France, bâtit "le Bertillonnage" qui s'appuie sur les modérations des osseuses et a consigné les signes particuliers d'un individu. Ces données étaient parachevées par des photographies et soigneusement classées. C'est en 1882 que le « système Bertillon » fut expérimenté pour la

première fois, Par la suite, l'utilisation des empreintes (dactyloscopie) fut améliorée par Edwards Henry, chef de la police Londonienne, et se généralisa dès le début du 20ème siècle. Ressemblant essentiellement aux mêmes méthodes employées par les Chinois durant des années.

Au 19ème siècle, la police criminelle fait énormément avancer la recherche du fait de la multiplication des Analyses d'Indices Biologiques (ADN)**. [2]**

Dans les trois dernières décennies, la biométrie a renforcé de l'utilisation d'une seule méthode (qui est l'empreinte) aux autres méthodes différentes l'une de l'autre (la rétine, l'iris, le visage, la voie,….etc.) ,et à cause des menaces les sociétés améliorent leurs méthodes de sécurité et continuent à chercher d'autres méthodes plus sécurisées tant que la technologie répond à leurs besoins et les prix du hardware nécessaire continuent à abaisser qui rendent des systèmes faisables pour de faibles et moyens budgets.

La technologie de biométrie s'impose Aujourd'hui comme un utile indispensable dans le domaine de sécurité public ou commerciale (e-commerce) Puisqu'elle utilise des critères permanents, uniques et infalsifiables **[3**]

I.4. Les systèmes biométriques

Un système biométrique est essentiellement un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Selon le contexte de l'application, un système biométrique peut fonctionner en mode d'enrôlement ou en mode de vérification ou bien en mode d'identification :

Le mode d'enrôlement est une phase d'apprentissage qui a pour but de recueillir des informations biométriques sur les personnes à identifier.

Plusieurs campagnes d'acquisitions de données peuvent être réalisées afin d'assurer une certaine robustesse au système de reconnaissance aux variations temporelles des données.

Pendant cette phase, les caractéristiques biométriques des individus sont saisies par un capteur biométrique, puis représentées sous forme numérique (signatures), et enfin stockées dans la base de données. Le traitement lié à l'enrôlement n'a pas de contrainte de temps, puisqu'il s'effectue « hors-ligne ».

Le mode de vérification ou authentification est une comparaison "un à un", dans lequel le système valide l'identité d'une personne en comparant les données biométriques saisie avec le modèle biométrique de cette personne stockée dans la base de données du système.

Dans un tel mode, le système doit alors répondre à la question suivante : « Suis-je réellement la personne que je suis en train de proclamer ?». Actuellement la vérification est réalisée via un numéro d'identification personnel, un nom d'utilisateur, ou bien une carte à puce. Le mode d'identification est une comparaison "un à N", dans lequel le système reconnaît un individu en l'appariant avec un des modèles de la base de données. La personne peut ne pas être dans la base de données. Ce mode consiste à associer une identité à une personne.

En d'autres termes, il répond à des questions du type: « Qui suis-je ? ».[4]

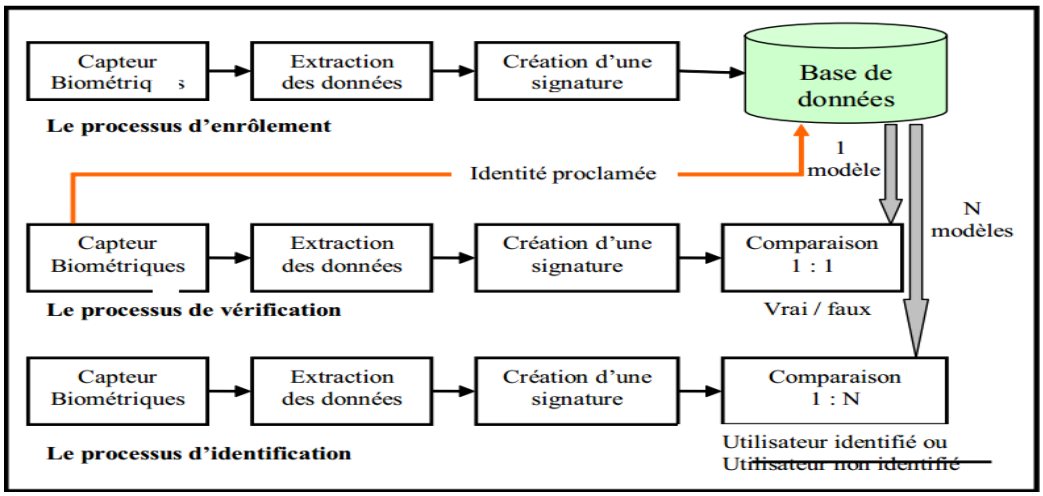


Figure 1.1 : Principaux modules d'un système biométrique ainsi que les différentes modes. [4]

Les différents modules qui composent un système biométrique sont représentés sur la figure 1.1 ; leur fonctionnement peut être résumé comme suit :

•**Module capteur biométrique :** correspond à la lecture de certaines caractéristiques physiologiques, comportementales ou biologiques d'une personne, au moyen d'un terminal de capture biométrique (ou capteur biométrique);

•**Module extraction des données :** extrait les informations pertinentes à partir des données biométriques brutes, par exemple des images de visage ou des régions caractéristiques de visage ;

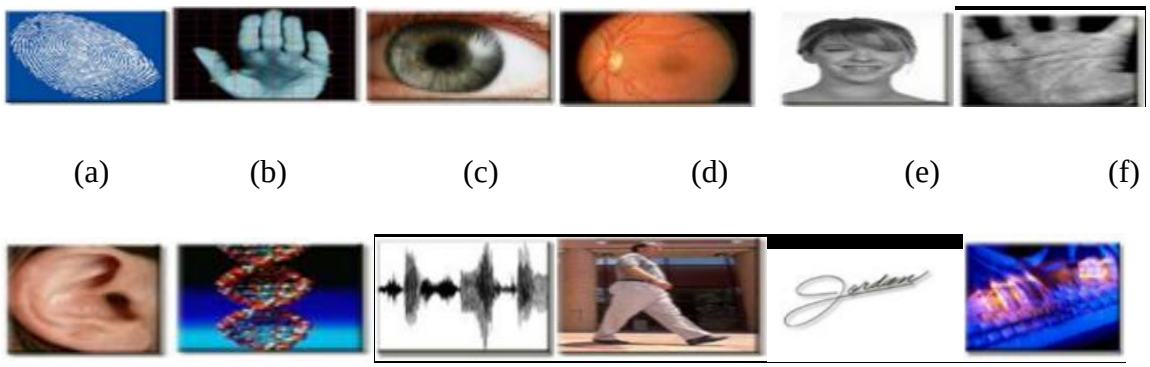
•**Module création d'une signature :** crée un modèle numérique afin de représenter la donnée biométrique acquise. Ce modèle, appelé aussi signature, sera conservé sur un support portable (puce ou autre) ou dans une base de données ;

•**Module comparaison :** compare les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) avec les « signatures » mémorisées. Ce module fonctionne soit en mode vérification (pour une identité proclamée) ou bien en mode identification (pour une identité recherchée).

•**Module base de données :** stocke les modèles biométriques des utilisateurs enrôlés. [4]

I.5. Les différentes modalités de la biométrie

De nombreuses méthodes ont été utilisées dans différents systèmes biométriques. Dans cette section, nous nous concentrerons sur les modalités comportementales et morphologiques. Nous allons également introduire quelques méthodes cachées qui sont étendues. Dans la figure suivante, certaines méthodes sont illustrées. [1]



(a) (b) (c) (d) (e) (f)

(g) (h) (i) (j) (k) (l)

Figure I.2 : Quelques modalités biométriques (a): digitale (b): la main (c): L'iris (d) : La rétine (e) : visage (f) : Empreinte palmaire (g): l'oreille (h): L'A.D.N (i): La voix (j):La démarche (k): La signature (l) : Dynamique de frappe. [1]

I.5.1. Modalités morphologiques

Une méthode morphologique peut être définie comme une mesure d'une des caractéristiques biologiques ou physiques d'un individu. Ci-dessous, nous présenterons certaines de ces méthodes ainsi que les façons de les utiliser. [1] :

I.5.1.1. L'empreinte digitale

Une empreinte digitale est le résultat de l'opposition sur un support d'un doigt préalablement encré, le dessin formé sur le support est constitué de l'empreinte, elle est constituée d'un ensemble de lignes Ponctuellement parallèles formant un motif unique pour chaque individu. On distingue les stries (ou crêtes, ce sont les lignes en contact avec une surface au toucher) et les sillons (ce sont les creux entre deux stries).

Les stries contiennent en leur centre un ensemble de pores régulièrement espacés. Chaque empreinte Les centres correspondent à l'endroit où les signes se rencontrent tandis que les deltas correspondent à l'endroit où ils divergent.

L'empreinte entière contient en moyenne une centaine de ces points caractéristiques, environ 40 points peuvent être extraits et donc les produits proposés sur le marché sont basés sur seulement 12 points ; Il est impossible de trouver deux personnes avec les mêmes 12 points. Les technologies utilisées pour mesurer les empreintes digitales sont variées : capteur de champ électrique, capteur optique, capteur thermique, capteur capacitif ou à ultrasons. [**5]**

Figure I.3 : Empreinte digitale [6]

- **Avantages et inconvénients de l'Empreinte digitale**

Le tableau I.1 ci-dessous présente certains avantages et inconvénients de la reconnaissance par l'empreinte digitale [6] :

Les avantages	Les inconvénients
▪ Le prix de la reconnaissance digital est faible. ▪ La taille du lecteur biométrique d'empreinte digital n'est pas volumineuse et le système reste très simple à mettre en place. ▪L'utilisation est facile, plus pratique et plus rapide, il suffit de poser son doigt dessus. ▪C'est aussi la technique la plus fiable : il n'y a qu'une chance sur 17 milliards de trouver deux empreintes avec plus de 17 points de similitude.	▪ Certaines personnes peuvent créer de "faux doigt" en utilisant l'empreinte digitale d'une autre personne, ou utiliser un doigt coupé (La détection du doigt vivant permet d'éviter ce type d'usurpation). ▪ Le manque d'hygiène, les traces de doigts se succèdent sur ce lecteur le rend très sale.

Tableau l.1 : Avantages et inconvénients de l'Empreinte digitale

I.5.1.2. L'iris

C'est une technologie fiable. Elle est plus précise que certaines méthodes biométriques. En effet, l'iris de l'œil a de nombreuses caractéristiques qui diffèrent d'un individu à l'autre. L'iris est constituée de vaisseaux sanguins et est disposé différemment d'une personne à l'autre. Chaque œil est unique. La probabilité de trouver une iris identique est inférieure à l'inverse du nombre d'humains ayant vécu sur Terre.

Une fois que l'image de la configuration des vaisseaux sanguins est obtenue par le système biométrique (figure I.4), le fonctionnement est quasi identique à celui du système analysant l'empreinte digitale. La grosseur des vaisseaux, leur positionnement et les bifurcations qui les caractérisent font partie des éléments, les minuties, qui seront étudiés par le système dans le but d'en dégager un algorithme particulier. La comparaison avec le fichier référence pourra s'ensuivre.

Le point faible de ce type de système utilisant l'œil à des fins d'identification ou de vérification est qu'il éprouve beaucoup de difficultés à lire l'image de l'œil d'une personne aveugle ou d'un individu ayant un problème de cataracte. [7]

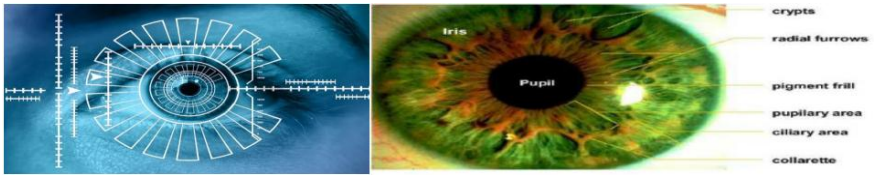


Figure I. 4 : Les caractéristiques de l'iris [8]

➢ **Avantages et inconvénients de L'iris**

Le tableau I.2 ci-dessous présente certains avantages et inconvénients de de la reconnaissance de l'iris [6] :

Les avantages	Les inconvénients
▪ La texture de l'iris est parfaitement stable au cours du temps. ▪ La vérification de l'identité est très rapide. ▪ Grande quantité d'information contenue dans l'iris. ▪ Vrais jumeaux non confondus. ,	▪ La prise de vue n'est pas très simple : la taille de l'iris est très variable suivant la lumière ambiante ou l'état de fatigue, et les utilisateurs ont tendance à bouger. ▪ La fiabilité diminue proportionnellement à la distance entre l'œil et la caméra. ▪ Dispositifs très couteux. ▪ Mal accepté par les utilisateurs (l'œil doit rester grand ouvert et il est éclairé par une source lumineuse)

Tableau I.2 : Avantages et inconvénients de L'iris

I.5.1.3. Le visage

Il s'agit de prendre une photo pour extraire un ensemble de facteurs qui se veulent spécifiques à chaque personne, ces facteurs sont choisis pour leur grande cohérence et concernent des zones du visage telles que : les yeux, la bouche, et la forme du visage (contour). La difficulté de reconnaître les visages est très variable selon que l'acquisition se déroule ou non dans un environnement contrôlé.

Dans un environnement contrôlé, des paramètres tels que l'arrière-plan, la direction et l'intensité des sources lumineuses, l'angle de prise de vue et la distance entre la caméra et le sujet sont des paramètres contrôlés par le système. Dans un environnement non supervisé, une série de prétraitements est souvent nécessaire avant que la reconnaissance réelle puisse être effectuée. Vous devez d'abord détecter la présence ou l'absence d'un visage sur la photo, puis le visage doit être segmenté.**[9]**

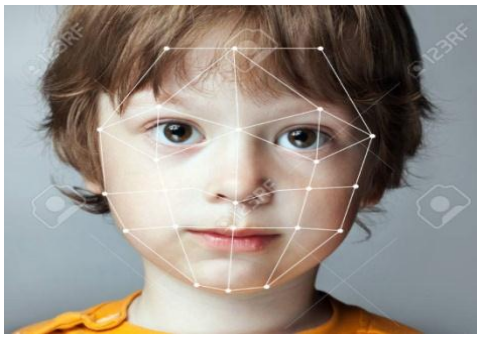


Figure I.5 : Le visage [10]

I.5.1.4. La rétine

La rétine est la « pellicule photo » de l'œil. Il se compose de 4 couches de cellules et est situé à l'arrière de l'œil. Les éléments qui distinguent deux réseaux sont les veines qui les bordent. L'arrangement de ces veines est stable et unique.

La biométrie rétinienne offre également un haut niveau de reconnaissance. Cette technologie est bien adaptée aux applications de haute sécurité (sites militaires et nucléaires, salles de sous-sol, etc). La disposition des veines rétiniennes assure une bonne fiabilité et une grande barrière contre la fraude.

L'utilisateur doit placer son œil à quelques centimètres du port de capture sur le lecteur de rétine. Il ne doit pas bouger et doit regarder un point vert vif en rotation. À ce stade, un faisceau de lumière traverse l'œil dans les vaisseaux sanguins capillaires de la rétine. Ainsi, le système localise et capture environ 400 points de référence. Après avoir pris une image de la rétine, le logiciel de l'appareil du lecteur découpe un anneau autour de la fovéa.

Détermine l'emplacement et la direction des veines. Puis il l'a noté dans un modèle. Les algorithmes de traitement restent relativement complexes. [11]

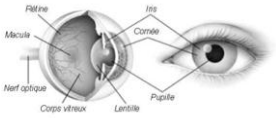



Figure I.6 : la reconnaissance de la rétine [11]

- **Avantages et inconvénients de la rétine**

Le tableau I.3 ci-dessous présente certains avantages et inconvénients de la reconnaissance de la rétine: [8]

Avantages	Inconvénients
▪ La fiabilité est une des plus élevée au monde. ▪ Les risques de fraude sont quasi nuls, puisque la partie du corps exploitée n'est pas apparente. ▪ La rétine est stable durant la vie d'un individu.	▪ Un système intrusif et peu agréable (rayon lumineux envoyé dans l'œil) et donc mauvaise acceptation du public. ▪ Une forte alcoolémie ou un diabète modifie le réseau veineux rétinien. ▪ La technique exclue d'emblée la clientèle aveugle de même que tous les sujets ayant une cataracte faible.

Tableau I.3 : Avantages et inconvénients de la rétine

I.5.1.5. La voix ou la parole

En 1962, Lawrence Kersta, ingénieur de Beautiful Labs, démontre que la voix de chacun est différente et qu'elle peut être représentée graphiquement. La voix est constituée de composantes physiologiques et comportementales [1].

Dans les années 1980, plusieurs entreprises ont développé des systèmes de reconnaissance vocale pour les forces de police et les agences d'espionnage. Le principe est le même que pour les systèmes précédents, une table de référence pour la voix d'une personne est préparée à l'avance. Pour ce faire, vous devez lire plusieurs fois une série de phrases ou de mots.

Extraire de nombreuses propriétés du son telles que la vitesse, la force, la dynamique et la forme des ondes produites. Une personne ne parle pas toujours de la même manière, ce qui nécessite d'appliquer une méthode pour éliminer certaines de ces différences. Ses propriétés qui composent une empreinte unique sont ensuite traitées par un algorithme et conservées pour comparaison ultérieure. **[1].**

Figure I. 7 : Enregistrement d'un signal vocal [6].

- **Avantages et inconvénients de La voix ou la parole**

Le tableau I.4 ci-dessous présente certains avantages et inconvénients de la reconnaissance de voix [6] :

Les avantages	Les inconvénient
• Système non intrusif • Faible coût • Très bien acceptées par les populations	• Sensible aux bruits ambiants • Fraude possible par enregistrement • Dépend de l'état de l'utilisateur (physique et émotionnel)

Tableau I.4 : Avantages et inconvénients de La voix ou la parole

I.5.1.6. La géométrie de la main

La reconnaissance de la main est l'un des prédécesseurs des technologies biométriques. À la fin des années 1960, Robert B. Miller a breveté un appareil pour mesurer les

caractéristiques de la main et les enregistrer pour une comparaison ultérieure. L'utilisateur pose sa main sur un gabarit.

Tout fonctionne Par la lumière infrarouge et l'image est capturée par un appareil photo numérique. Près d'une centaine de propriétés sont extraites de l'image et converties en données stockées en mémoire lors de la phase d'enregistrement ou comparées lors de la phase de sélection. Ces données concernent la longueur, la largeur et l'épaisseur de la main, ainsi que la forme des articulations et la longueur de l'articulation. [11]

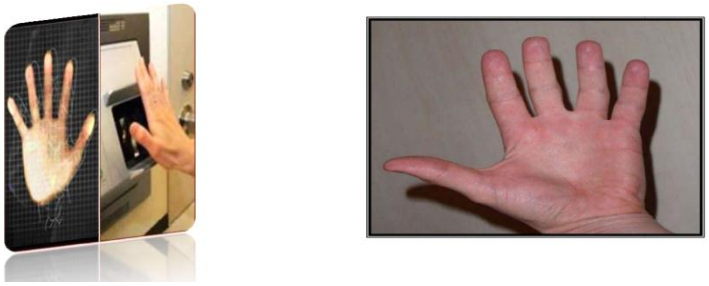


Figure I.8 : La reconnaissance de la main [11]

I.5.2. Modalités comportementales

S'agit d'un type de biométrie caractérisé par un trait d'attitude qui est appris et acquis au fil du temps plutôt qu'une caractéristique physiologique.

En conséquence, une modalité comportementale peut changer avec le temps. Voici quelques exemples de ce type de modalités biométrique :

I.5.2.1. Dynamique de la frappe au clavier

Selon la façon dont les gens tapent sur le clavier, les gens peuvent être authentifiés, et le système est basé sur cette frappe dynamique. L'avantage de cette méthode est qu'elle ne nécessite pas d'équipement spécial, puisque chaque ordinateur dispose d'un clavier et d'une application qui est adapté pour une utilisation dans ce domaine dont il existe plusieurs.

Dispositif logiciel (application) qui calcule le temps pendant lequel le doigt appuie sur une touche et le temps pendant lequel le doigt est en l'air (entre les frappes). Cette mesure est capturée environ 1 000 fois par seconde. La séquence de frappe est prédéfinie sous la forme d'un mot de passe. Dans un premier temps, l'utilisateur doit saisir plusieurs fois son mot de passe pour créer un formulaire de référencement **[9].**

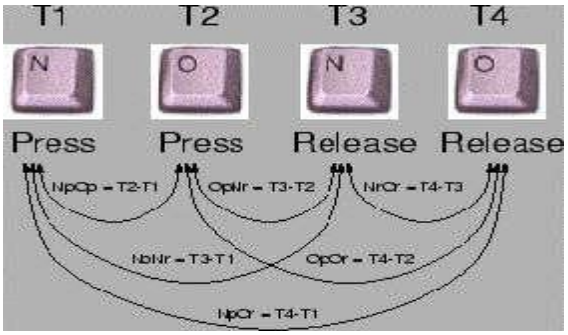


Figure I. 9 : Détail sur la dynamique de la frappe au clavier [1]

- **Avantages et inconvénients de la frappe au clavier**

Le tableau I.5 ci-dessous présente certains avantages et inconvénients de la frappe au clavier : [6]

Avantages	Inconvénients
• Facile à mettre en œuvre et pas coûteuse	• Très peu répandue • Dépend de l'état de l'utilisateur (physique et émotionnel)

Tableau I.5 : Avantages et inconvénients de la frappe au clavier

I.5.2.2. La démarche

Votre démarche est unique. Au point que c'est un facteur distinct dans les images vidéo, Watrix, une jeune société d'intelligence artificielle, a travaillé sur cette technologie et lance un programme qui permet d'identifier les individus dans un rayon de 50 mètres, même si la personne est de dos. Avec un visage masqué, cette nouvelle biotechnologie est basée sur des mesures de la démarche, de la forme du corps et de l'angle de mouvement des bras d'une personne dans la position de son corps, y compris sa façon de marcher. Toutes ces informations sont stockées dans une base de données que le programme consulte ensuite pour tenter d'identifier les personnes.

Cette technologie a aussi des inconvénients, et je constate qu'elle n'est pas encore capable d'identifier les personnes en temps réel. Elle n'est pas non plus aussi fiable que la reconnaissance faciale **[12]**.

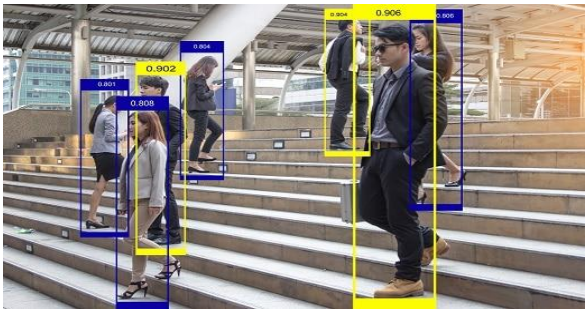


Figure I-10 : La reconnaissance des individus selon leurs comportements de démarche [13].

➢ **Avantages et inconvénients de La démarche**

Le tableau I.6 ci-dessous présente certains avantages et inconvénients de la reconnaissance de la démarche : [8]

Les avantages	Les inconvénients
• Système non intrusif • Très bien acceptées par les populations • Permet une reconnaissance à distance	• Très peu répandu et toujours en cours • Aucune preuve que la démarche est unique actuellement • Mise en œuvre difficile d'un tel système

Tableau I.6 : Avantages et inconvénients de La démarche

I.5.2.3. La signature

La signature est davantage utilisée pour authentifier des documents, des rapports, des contrats électroniques...etc.

Les systèmes de vérification de signature se répartissent en deux catégories selon le type d'acquisition de données : En ligne ou hors ligne.

Le système en ligne est généralement associé à une tablette graphique équipée d'un stylet, et cet appareil mesure de nombreuses caractéristiques lors de la signature, telles que la vitesse, l'ordre des frappes, la pression, l'accélération, le temps de contact du stylet, etc.

Les systèmes hors ligne traitent la signature à partir d'une image provenant d'un scanner. Ces systèmes sont très complexes en raison du manque de propriétés dynamiques stables. La difficulté réside aussi dans le fait qu'il est difficile de décrire l'apparence de la signature **[11].**

Figure I. 11: Signature biométrique [8]

- **Avantages et inconvénients de La signature**

Le tableau I.7 ci-dessous présente certains avantages et inconvénients de la reconnaissance de la dynamique de la signature : [6]

Les avantages	Les inconvénients
• Une forme acceptable juridiquement et administrativement pour l'identification des personnes • Signer est un geste naturel et facile pour les populations	• Difficile d'atteindre une très haute exactitude d'identification en raison des grandes variations de signature pour une même personne

Tableau I.7 : Avantages et inconvénients de La signature

I.5.3. Modalités biologiques

Cette catégorie est basée sur l'analyse des caractéristiques biologiques d'un individu Ce type d'analyse est basé sur les données biologiques de chaque individu. L'analyse biologique comprend : l'odeur, l'ADN, les signaux physiologiques...etc.

Cette méthode n'est pas largement utilisée pour le contrôle d'accès logique et physique.

I.5.3.1. L'odeur corporelle

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

Une collaboration entre l'entreprise d'ingénierie et de consulting Ilia Systems et le groupe de recherche GB2S (Group of Biometrics, Biosignals and Security) de l'université polytechnique de Madrid propose cette nouvelle technique de reconnaissance des odeurs corporelles, bien que des travaux ont été déjà fait par la société anglaise Mastiff-Electronics sur cette technique.

Au vu des bons premiers résultats obtenus, il apparait que cette forme de reconnaissance biométrique est une technologie prometteuse, de plus sa simplicité d'utilisation et son

emploi d'une manière non intrusive pourrait accélérer sa future adoption, à titre d'exemple un piéton pourrait passer à côté d'un détecteur d'odeur corporelle, il sera alors identifié sans aucune intervention de sa part. Parmi les principaux champs d'application les aéroports et les points de passage. [8]

- **Avantages et inconvénients de L'odeur corporelle**

Le tableau I.8 ci-dessous présente certains avantages et inconvénients de L'odeur corporelle : [8]

Avantages	Inconvénients
▪ Non intrusive. ▪ Simple à utiliser, sans coopération de la personne, qui la rend plus acceptable. ▪ L'odeur corporelle est identifiant unique pour chacun. ▪ Technique qui a montré son succès déjà avec les chiens	▪ L'odeur corporelle d'un individu peut varier en fonction de son humeur, de son régime alimentaire ou de son état de santé. ▪ Taux de faux rejet et fausse acceptation élevés. ▪ Le besoin de capteurs spéciales pour cette méthode.

Tableau I.8 : Avantages et inconvénients de L'odeur corporelle

I.5.3.2. L'ADN

Aussi appelée empreinte génétique, c'est une molécule qui contient des informations « génétiques », qui sont propres à chaque individu. L'analyse de ce fluide biologique utilise des techniques lourdes, coûteuses et à long terme. Biométrie ADN couramment utilisée en médecine légale pour identifier des personnes non identifiées ou pour déterminer la source d'échantillons biologiques restant sur les scènes de crime **[9].**

Figure I. 12 : A.D.N [8]

- **Avantages et inconvénients de L'ADN**

Le tableau I.9 ci-dessous présente certains avantages et inconvénients de l'A.D.N: [8]

Avantages	Inconvénients
▪ Elle est très précise. ▪ La fiabilité est une des plus élevée au monde : le taux d'erreur est de quasi nul	▪ L'identification d'un individu par analyse de son ADN s'avère complexe. ▪ Elle est coûteuse et lente à réaliser compte

▪ Les risques de fraude sont très bas. ▪ L'ADN est stable durant la vie d'un individu. ▪ L'ADN est différent chez les vrais jumeaux.	tenu des nombreuses manipulations biologiques. ▪ Elle n'est pas destinée au grand public. ▪ Cette technique très intrusive, elle nécessite un prélèvement d'échantillon (sang, salive, sperme, cheveux, urine, peau, dents, etc.).

Tableau I.9 : Avantages et inconvénients de L'ADN

I.5.3.3. Les signaux physiologiques

La thermographie se définit comme une technique permettant d'obtenir une image thermique d'une scène au moyen d'un appareillage approprié comme utiliser un appareil photo ou une caméra numérique dans le domaine de l'infrarouge.

La quantité de chaleur émise par les différentes parties du visage qui est capturées dans n'importe quelle condition d'éclairage et même dans le noir complet caractérise chaque individu de façon unique. Elle dépend de la localisation des veines mais aussi de l'épaisseur du squelette, la quantité de tissus, de muscles, de graisses, etc. [6]

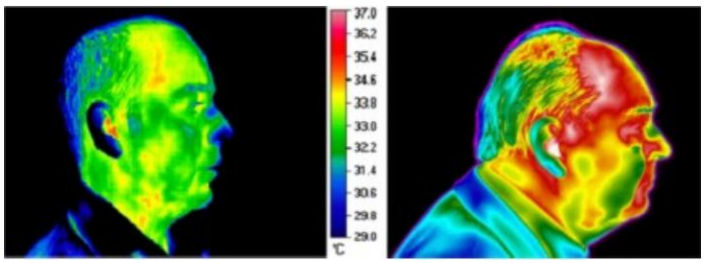


Figure I. 13 : La thermographie faciale [6]

➢ **Avantages et inconvénients de la thermographie faciale**

Le tableau I.10 ci-dessous présente certains avantages et inconvénients de la thermographie faciale [6] :

Avantages	Inconvénients
▪ Non intrusive. ▪ Simple à utiliser, sans coopération de la personne, qui la rend plus acceptable. ▪ La chirurgie plastique n'a que peu d'influence sur les thermogrammes faciaux. ▪ La capture peut se faire dans n'importe quelle condition d'éclairage et même dans le noir complet.	▪ Les conditions de prise de vue peuvent conduire à des erreurs. ▪ La précision de cette technique est faible, car l'état physique de la personne (malade, fait du sport …etc.) influe sur la chaleur dégagée de son corps. ▪ Elle n'est pas fiable, le taux d'erreur est très élevé.

Tableau I.10 : Avantages et inconvénients de la thermographie faciale

I.5.3.4. Multi modalité

Certaines méthodes unimodales ont un système d'identification difficilement contournable, mais en conséquence, il est invasif et assez coûteux à mettre en place, tandis que d'autres sont soit Performances insatisfaisantes ou fraude facile par enregistrement, copie, etc.

Pour pallier les difficultés liées aux systèmes antérieurs, la première solution consiste à combiner la biométrie avec une identification à base de connaissances ou possessive, comme des mots de passe ou des codes PIN (identification à deux facteurs). Cette méthode peut améliorer la sécurité du système, mais elle présente des faiblesses inhérentes à la reconnaissance basée sur la connaissance ou la possession. La deuxième solution est la multimodalité, une alternative, qui peut combiner plusieurs systèmes biométriques pour améliorer le système Analyser les performances du système biométrique système. Performance, nous nous référons à la précision du système, mais aussi à son efficacité, notamment en mode reconnaissance. En fait, différents classificateurs produisent généralement des erreurs différentes, et cette complémentarité peut être utilisée pour améliorer les performances globales du système. [6]

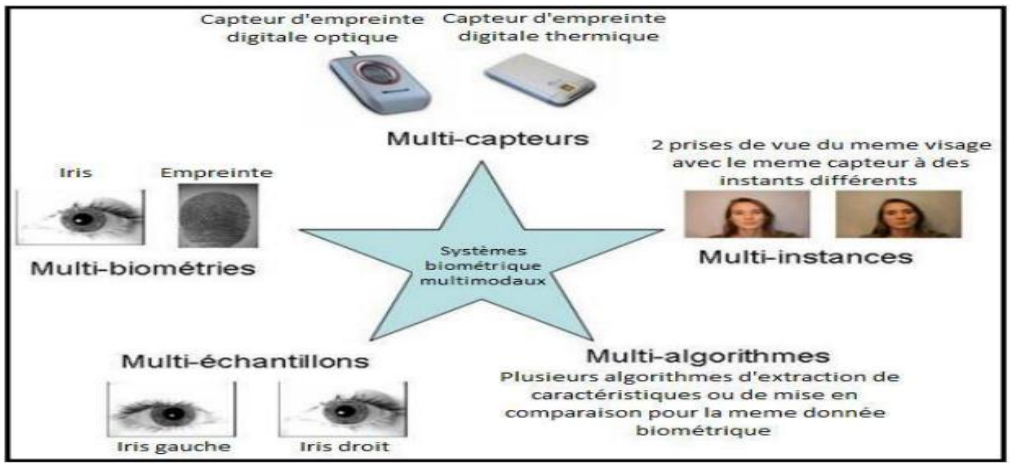


Figure I. 14 : Les différents systèmes multimodaux [8]

I.5.4. Modalités cachées

Ces modalités sont un concept biologique puissant. Par rapport aux méthodes biométriques traditionnelles qui constituent la base des caractéristiques visibles du corps humain, les méthodes cachées prennent en compte les caractéristiques intrinsèques et invisibles du corps humain.

Tout signal physiologique ou organe humain serait potentiellement candidat à des applications biométriques. Dans la première catégorie, nous pouvons employer l'électrocardiogramme (ECG), l'électromyogramme. (EMG). Dans la deuxième catégorie,

nous pouvons considérer, comme exemple, la morphologie ou la texture du cerveau humain. Voici quelques exemples de ces modalités :

I.5.4.1. Electrocardiogramme ECG

L'ECG est un signal représentant l'activité du cœur. Il est principalement employé dans des applications cliniques pour diagnostiquer les maladies cardio-vasculaires. Le signal d'ECG est caractérisé par la forme de ses battements composés de cinq vagues typiques, à savoir P, Q, R, S, et T ou parfois la vague U (Figure I.15).

La biométrie par ECG a fait l'objet d'un certain nombre de travaux. L'utilisation de l'ECG en biométrie est relativement nouvelle. En fait, il existe plusieurs méthodes biométriques basées sur l'ECG. Il y a des approches qui sont basées sur l'analyse de l'ECG. D'autres basées sur l'intégration des caractéristiques analytiques et d'apparence extraite des signaux ECG [1]

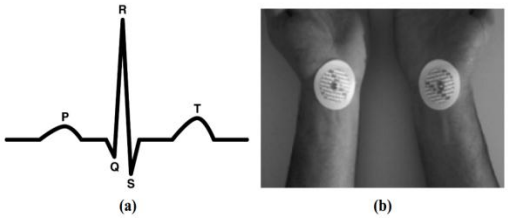


Figure I.15: Biométrie par ECG : (a) Signal d'ECG avec le rythme régulier (b) positionnement des électrodes sur les avant-bras pour la capture d'ECG [1]

I.5.4.2. Biométrie du cerveau avec des images IRM

Dans des applications médicales, l'IRM (imagerie par résonance magnétique) est une technique de formation image non envahissante employée pour visualiser des images en 2D ou 3D des organes du corps humain (par exemple cerveau, muscles, et cœur) avec une résolution relativement élevée. Ceci est rendu possible avec l'utilisation d'un champ électromagnétique puissant et constant, produit par un supraconducteur.

La Biométrie par le cerveau cherche à caractériser le cerveau humain à travers des images IRM 2D et 3D. Depuis les images IRM 2D (**Figure I.16.a**), on peut faire la reconstruction en 3D (**Figure I.16.b**) du cerveau pour avoir des informations sur la texture. Ainsi d'autres caractéristiques géométriques du cerveau peuvent être considérées comme le rapport isopérimètre et la courbure extérieure corticale.

En fait, la quantité de paramètres qui peuvent être extraits à partir d'une image du cerveau 3D est plus grande que ce que nous pouvons extraire à partir d'autres modalités

classiques. On peut aussi définir ce qu'on appelle *brain code* ou code du cerveau à travers une segmentation de la zone d'intérêt du cerveau (**Figure I.16.c**)

L'avantage principal de ce type de modalité cachée est le fait que le cerveau est totalement protégé contre toutes sortes de changements. Il est difficile d'imaginer qu'un individu modifie la structure de son propre cerveau pour usurper l'identité d'un autre individu. Cependant, l'inconvénient principal de cette modalité est la non-disponibilité de systèmes d'IRM robuste consacrés à la biométrie. [1]

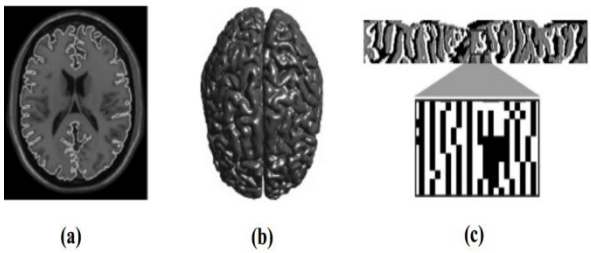


Figure I.16: Biométrie du cerveau avec des images IRM : (a) Extraction des textures de cerveau par segmentation (b) reconstruction de 3D d'image de cerveau montrant les circonvolutions qui peuvent être employées pour identifier des individus
(c) extraction du Brain Code [1]

I.6. Les applications de la biométrie

Les technologies biométriques sont appliquées dans plusieurs domaines et couvriront probablement tous les domaines de la sécurité où il est nécessaire de connaître l'identité des personnes. Ces applications sont divisées en trois groupes principaux :

▪ **Application commerciale :** telles que l'accès au réseau informatique (Lancement du système d'exploitation, Accès au réseau), la sécurité de données électroniques, l'ecommerce, l'accès d'internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distances, etc.…

▪ **Applications de gouvernement :** telles que la carte nationale d'identifications, le permis de conduite, la sécurité sociale, le contrôle de passeport, etc.…

▪ **Applications légale (juridiques) :** telles que l'identification de corps, la recherche criminelle, l'identification de terroriste, les enfants disparus, etc.[8]

Figure I.17 : Applications biométriques. [11]

➢ **Application de la biométrie :**

- **Contrôle d'accès aux locaux:**

- Salles informatiques.

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

- **Equipements de communication:**

- Terminaux d'accès.

- Téléphones portables.

- **Systèmes d'informations:**

- Lancement du système d'exploitation,

- Accès au réseau.

- Transaction (financière pour les banques, données entre entreprises).

- **Machines & Equipements divers:**

- Distributeur automatique de billets.

- Lieu sensible (club de tir, police).

- Contrôle des adhérents dans les clubs privés.

- Contrôle des temps de présence.

- **Etat/Administration:**

- Fichier judiciaire.

- Services sociaux (sécurisation des règlements).

- Système de vote électronique. [11]

I.7. Les avantages et les limites de la biométrie

La technologie biométrique peut rendre la vie plus confortable, mais elle n'est pas sans inconvénients. Les consommateurs peuvent bénéficier d'un équilibre entre les avantages d'un système de sécurité biométrique et les inconvénients potentiels.

I.7.1. Les avantages de la biométrie

La biométrie est une nouvelle technologie et les principaux fabricants d'ordinateurs ont commencé à l'adopter. L'utilisation de la biométrie complète l'utilisation de méthodes d'authentification telles que les mots de passe, les badges et les cartes à puce.. [11]

- Suppression des mots de passe, Suppressions des clés :

Au lieu de retaper son mot de passe dès que le PC se met en veille, une simple pression de l'empreinte digitale sur le capteur suffit et permet facilement de changer la session d'utilisateur. [11]

- Utilisation d'une signature biométrique:

Grande sécurité, intransmissible à une autre personne.

Une identité vérifiée (Le destinataire est bien la personne autorisée à visualiser ou à utiliser les données).

Lors de transactions financières, il est capital de savoir quel moyen de paiement du consommateur est le plus sûr.

La biométrie offre le chaînon manquant dans la triade du problème de sécurité:

- Diminution de la fraude.
- Rehaussement de l'intégrité des informations et la sécurité.
- Réduction des attaques à l'égard des programmes gouvernementaux.
- Croissance de la confiance envers les systèmes de sécurité.
- Diminution des frais administratifs.
- Accélération des services. [11]

I.7.2. Les limites de la biométrie

La biométrie est une technologie émergente qui propose de nouveaux facteurs d'authentification pour des applications variées. Les schémas actuels sont basés sur de multiples modalités allant de la reconnaissance faciale, les empreintes digitales jusqu'à la biométrie comportementale comme la dynamique de frappe sur un clavier.

Le développement important des systèmes biométriques s'accompagne également de plusieurs menaces spécifiques à cette technologie, car les données biométriques sont des données personnelles, non-révocables et donc particulièrement sensibles. Parmi les limites et inconvénients de la biométrie, on trouve les limites fonctionnelle, techniques et juridiques :

- **Les limites fonctionnelles :** La biométrie présente malheureusement un inconvénient majeur, en effet aucune des mesures utilisées ne se révèle être totalement exacte, car il s'agit bien là d'une des caractéristiques majeures de tout organisme vivant : on

s'adapte à l'environnement, on vieillit, on subit des traumatismes plus ou moins importants, on évolue et les mesures changent, à cause de ça un système non performant va laisser la place à des erreurs (Faux rejets et fausses acceptations).

- **Les limites techniques et d'usage :**

- **L'usurpation d'identité :**

Le fraudeur se fait passer pour un utilisateur légitime. Par exemple, en compromettant le modèle biométrique stocké dans la base de données, il est possible de reconstituer un signal artificiel proche du signal d'origine capable de franchir avec succès le seuil de décision de validation.

- **L'irrévocabilité :**

Le principal inconvénient de la biométrie est que si le formulaire biométrique est mal utilisé ou compromis, il ne peut pas être annulé, remplacé ou mis à jour.

- **Les limites juridiques :**

- **La violation de la vie privée :**

Utiliser le corps humain comme outil d'identification et le conserver dans des bases de données, parfois au-delà des frontières, pose un réel problème éthique. En outre, étant donné que la biométrie comprend des données personnellement identifiables et donc des données sensibles, leur collecte, leur stockage et leur utilisation devraient être soumis à des juridictions légales. Si l'unicité de la biométrie est vue comme un avantage, elle peut aussi être vue comme une opportunité d'identifier et de surveiller les traits d'une personne, menaçant sa liberté individuelle. Ainsi, la mise en place d'un système de biométrie doit reposer sur un impératif fort de préservation de la vie privée. Compte tenu des risques présentés, un système biométrique avant d'être déployé doit être soumis à diverses restrictions de sécurité et de confidentialité. Il est devenu impératif d'assurer la sécurité des systèmes biométriques et de protéger l'identifiant biométrique par des contre-mesures robustes. [8]

I.8. Comparaison entre les modalités biométrique

De la description précédente des différentes méthodes biométriques, nous pouvons voir qu'elles ont chacune des avantages et des inconvénients et que certaines applications nécessitent de choisir une méthode plutôt qu'une autre. Ce choix se fait principalement en prenant en compte un certain nombre de paramètres tels que l'origine de l'application, son coût, les performances attendues du système et l'acceptation de la méthode par l'utilisateur. [1]

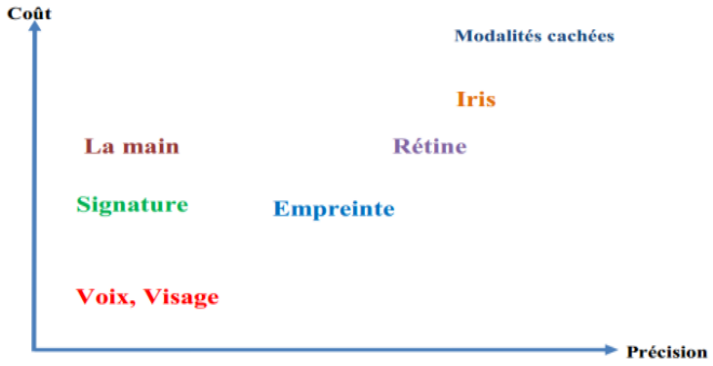


Figure I.18: Classement des modalités biométriques selon le coût et la précision. [1]

Ainsi, dans le tableau suivant, en plus de la précision de chaque modalité, on a ajouté d'autres paramètres de comparaison qui sont la simplicité d'utilisation et l'acceptation par l'utilisateur.

Type	Modalité	Précision	Simplicité d'utilisation	Acceptation par l'utilisateur
Morphologique	**Empreinte**	**Haute**	**Moyenne**	**Basse**
	Iris	**Haute**	**Moyenne**	
	Rétine	**Haute**	**Basse**	**Basse**
	Visage	**Basse**	**Haute**	
	Voix	**Moyenne**	**Haute**	**Haute**
	Géométrie de la main	**Moyenne**	**Haute**	**Haute**
Comportementale	**Frappe au clavier**	**Basse**	**Haute**	**Moyenne**
	Démarche	**Basse**	**Moyenne**	**Moyenne**
	Signature	**Moyenne**	**Moyenne**	**Haute**
Cachée	**ECG, EMG**	**Haute**	**Moyenne**	**Moyenne**
	Cerveau	**Haute**	**Basse**	**Basse**

Tableau I.11: Comparaison entre les modalités biométriques en matière de simplicité et acceptabilité [1]

I.9. Evaluation des performances des Systèmes biométriques

Chaque méthode biométrique a ses forces et ses faiblesses, et le choix dépend de l'application envisagée. Aucune méthode biométrique unique ne devrait répondre efficacement aux exigences de toutes les applications. En d'autres termes, il n'existe pas de système biométrique «parfait ». La correspondance du système biométrique d'une

application dépend du mode de fonctionnement de l'application et des caractéristiques biométriques sélectionnées. Plusieurs études ont été menées pour évaluer les performances des systèmes biométriques selon les critères suivants:

▪ **Intrusivité :** C'est l'absence ou la présence de contact direct entre le capteur utilisé par la méthode d'identification et l'individu à identifier (l'utilisateur).

▪ **Fiabilité :** dépend de la qualité de l'environnement dans lequel l'utilisateur se trouve (l'éclairage ...).

▪ **Coût :** dépend du coût de technologie implémentée (les capteurs utilisés, le matériel de traitement de données…).

▪ **Effort :** c'est la facilité ou la difficulté de l'utilisation de la méthode de reconnaissance choisie, et qui doit être facile. [8]

I.9.1. Mesure de performance des systèmes biométriques

I.9.1.1. En mode vérification

La performance d'un système biométrique est un élément essentiel à prendre en compte dans le choix d'un tel système. La mesure de performance d'un système biométrique s'articule autour de trois critères [8] :

A. Le FRR ou le TFR ((False Rejet Rate ou Taux de Faux Rejets)

Considéré comme le premier critère. Ce taux représente le pourcentage de personnes censées être reconnues mais qui sont rejetées par le système.

$$\boldsymbol{TFR = \frac{nombre\ des\ clients\ rejeté\ (FR)}{\text{nombre total de test clients}}}$$

Tel que FR Le faux rejet correspond au cas où le système rejette un client légitime **[14].**

B. Le FAR ou le TFA (False Acceptance Rate ou Taux de Fausse Acceptation)

Représente le deuxième critère. Ce taux représente le pourcentage de personnes censées ne pas être reconnues mais qui sont tout de même acceptées par le système.

$$\boldsymbol{TFA = \frac{\text{nombre des imposteurs accepté (FA)}}{\text{nombre total de test imposteurs}}}$$

Tel que FA correspond au cas où le système accepte un individu qui a proclamé une identité qui n'est pas la sienne **[14].**

C. Le taux d'égale erreur (« Equal Error Rate » ou EER)

Correspond au point FAR=FRR, 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 . Cependant, il est important de souligner que l'EER ne résume en aucun cas toutes les caractéristiques d'un système biométrique, il ne donne que le meilleur compromis entre les faux rejets et les fausses acceptations.[8]

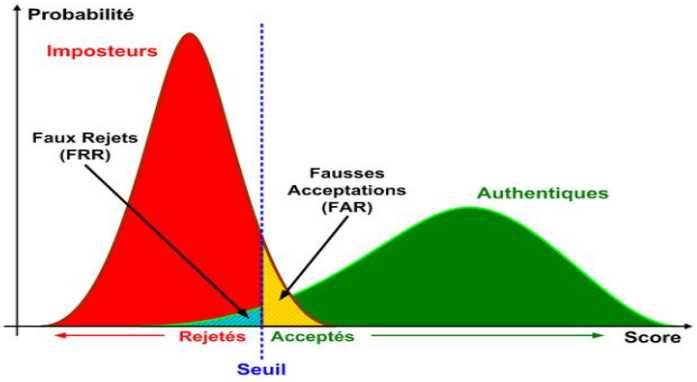


Figure I. 19 : Courbe de distribution des imposteurs et des authentiques et les taux d'erreurs (FAR ET FRR), pour un seuil donne [11].

I.9.1.2. En mode Identification

Est le taux auquel un sujet (utilisateur authentique) dans une base de données biométriques est correctement identifié

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

Selon la nature (authentification ou identification) du système biométrique, il existe deux façons d'en mesurer la performance :

Lorsque le système opère en mode authentification, on utilise ce que l'on appelle une courbe ROC (pour "Receveur Operating Caractéristique" en anglais). La courbe ROC trace le taux de faux rejet en fonction du taux de fausse acceptation. Plus cette courbe tend à prendre la forme du repère, plus le système est performant, c'est-à-dire possédant un taux de reconnaissance global élevé. [1 8]

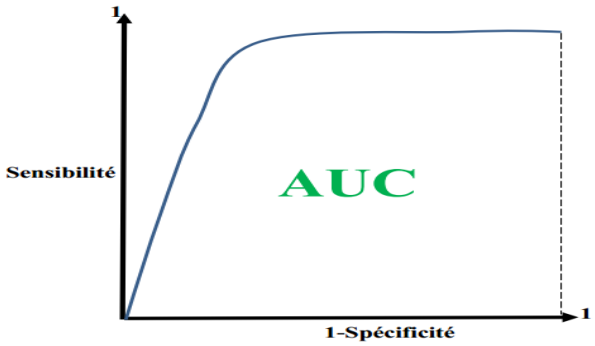


Figure I. 20 : Courbe ROC [1].

En revanche, dans le cas d'un système utilisé en mode identification, on utilise ce que l'on appelle une courbe CMC (pour "Cumulative Match Caractéristique" en anglais). La courbe CMC donne le pourcentage de personnes reconnues en fonction d'une variable que l'on appelle le rang. On dit qu'un système reconnaît au rang 1 lorsqu'il choisit la plus proche image comme résultat de la reconnaissance. On dit qu'un système reconnaît au rang 2, lorsqu'il choisit, parmi deux images, celle qui correspond le mieux à l'image d'entrée, etc. On peut donc dire que plus le rang augmente, plus le taux de reconnaissance correspondant est lié à un niveau de sécurité faible. [8]

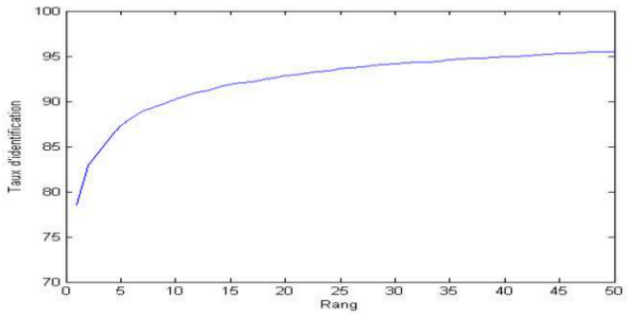


Figure I. 21 : Exemple de courbe CMC [8]

• **La courbe DET (*Detection error tradeoff*) :** Cette courbe illustre la relation entre le FRR et le FAR. Elle est obtenue en faisant varier le seuil de décision et en calculant à chaque fois les deux valeurs FRR et FAR[1]

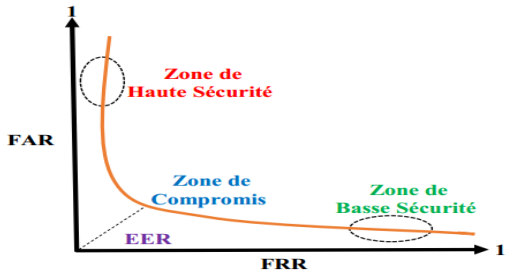


Figure I.22 : Exemple d'une courbe DET. [1]

I.10. Conclusion

Dans ce chapitre nous avons présenté la biométrie. Nous avons vu en premier une définition de la biométrie et son historique, ensuite quelques modalités biométriques les plus connues par famille et les caractéristiques biométriques ensuite l'évolution du marché de la biométrie et ses domaines d'application et à la fin, nous avons vu l'architecture et le principe de fonctionnement des systèmes biométriques, ainsi que l'évaluation et la Mesure de performance, les avantages et les limites de ces systèmes.

Chapitre II
La reconnaissance de visage

II.1. Introduction

Durant la vie quotidienne chacun de nous identifie tout au long de la journée différents visages. Ainsi lorsque nous rencontrons une personne, notre cerveau va chercher dans notre mémoire et vérifie si cette personne est répertoriée ou non, c'est une tâche aisée pour les humains. En est-il de même pour une machine ?

Dans ce premier chapitre, nous allons justement présenter les grandes lignes de notre travail, nous allons ainsi expliquer des notions générales sur la reconnaissance faciale, le fonctionnement d'un système de reconnaissance faciale, On va aussi aborder quelques techniques utilisées, des exemples et les domaines d'application.

II.2. La reconnaissance de visage

La reconnaissance faciale est une technologie basée sur les traits du visage, Elle peut :

- Vérifier une personne : c'est-à-dire vérifier qu'une personne est bien cette personne il prétend être (dans le cadre du contrôle d'accès)

Ou alors :

- Identifier une personne : c'est-à-dire trouver une personne dans un groupe Image ou base de données en un seul endroit.

En fait, il peut être reconnu à partir d'images fixes (photos) ou d'images animées (enregistrements vidéo). Le processus de reconnaissance est divisé en deux étapes :

1. Selon l'image, un modèle ou « gabarit » représentant les traits du visage du point de vue d'un ordinateur est réalisé. Les données extraites constituant le modèle sont des données biométriques.
2. Ensuite la phase de reconnaissance en comparant ces modèles, elle a été réalisée à l'aide d'un modèle calculé en temps réel à partir du visage présent sur l'image candidate.

Dans le cas de l'authentification, le système vérifie si la chose alléguée est vraie en comparant le modèle de visage présenté avec le modèle précédemment enregistré correspondant à l'identité. Dans le cas de l'identification, le système vérifie si le modèle du visage présenté correspond à l'un des modèles contenus dans la base de données.

Les résultats de la comparaison correspondent à celui ou ceux présentant le score de similarité le plus élevé parmi ceux dépassant un certain seuil prédéterminé. La reconnaissance faciale ne doit pas être confondue avec la détection de visage qui

caractérise la présence ou non d'un visage dans une image indépendamment de la personne à qui il appartient.[15]

- **Pourquoi choisir le visage**

Au cours des deux dernières décennies, la technologie de reconnaissance faciale automatique a devenu un enjeu clé, notamment dans le domaine de l'indexation de documents multimédia, notamment en termes de sécurité, en raison des besoins du monde d'aujourd'hui et de ses avantages, notamment :

- Disponibilité, simplicité et coût d'acquisition des équipements Frêle.
- Système passif : Le système de reconnaissance faciale ne nécessite aucune coopération de la part de l'individu, comme placer les doigts ou les mains sur un appareil spécifique ou parler dans un microphone. En effet, la personne n'a qu'à se tenir debout ou à marcher devant la caméra pour être reconnue par le système.

De plus, cette technique est très efficace pour les situations non standard, telles que dans les situations où la coopération d'une personne identifiée ne peut être obtenue, comme lors de l'arrestation d'un criminel.

Bien que comparée à d'autres technologies biométriques, la reconnaissance faciale n'est pas la plus fiable, mais elle peut être la plus fiable si une méthode plus efficace est utilisée en plus de la sélection et de la reconnaissance correctes des caractéristiques représentant le visage concerné. [16]

II.3. Historique

La reconnaissance faciale est une technique biométrique relativement récente. Alors que la prise d'empreintes digitales était la technique biométrique la plus inventée en 1903 pour trouver des criminels, la reconnaissance faciale a été développée par « Benton et Van Allen » en 1968 pour évaluer la probabilité.

Il ne s'agit pas d'un test de reconnaissance du ménisque de visages familiers ou inconnus, mais d'un test consistant à associer des photographies de visages inconnus présentés sous différentes lumières et sous différents angles et qui nécessite des capacités visio-spatiales intégrées. [17]

L'utilisation des techniques de reconnaissance faciale a été démontrée en milieu d'année 90 avec l'utilisation efficace des nouvelles technologies, en particulier des capacités informatiques et de traitement d'images numériques.

L'utilisation de ces techniques existe depuis en supposant qu'une machine comprend ce qu'elle "voit" lorsqu'elle a une ou plusieurs caméras, c'est-à-dire que le premier test date dans les années 1970, basées sur des méthodes heuristiques, basées sur propriétés mesurables du visage telles que la distance entre les yeux, les lèvres, la position du menton, la forme, etc. [18]

Ces méthodes ne sont pas très puissantes, car elles font de nombreuses hypothèses en étant placées dans des situations très face-à-face, de bonnes conditions d'éclairage, etc. L'une des premières tentatives de reconnaissance de visage est faite par TakeoKanade en 1973 lors de sa thèse de doctorat à l'Université de Kyoto [19] [20].

II.4. Domaines de la Reconnaissance Faciale

De nos jours, la reconnaissance faciale est principalement utilisée pour des raisons de sécurité. Il peut être utilisé à des fins multiples. Par exemple, l'authentification, le contrôle d'accès (autorisation) et la vidéo de surveillance.

Un bon exemple de l'utilisation des applications d'identification est le nouveau tunnel qui sera installé à la fin de l'été, situé à Dubaï, qui est le premier tunnel du genre au monde. Il s'agit d'un système biométrique qui peut identifier les passagers lors du passage dans les tunnels, améliorant ainsi l'efficacité des points de contrôle de sécurité. Ils n'ont même pas besoin de montrer leur passeport. Le travail de cet outil est dû à la reconnaissance de l'iris et du visage. Ce processus prend environ 15 secondes.

La reconnaissance faciale est également utilisée dans les applications militaires. Un bon exemple dans ce domaine est l'utilisation de lunettes « Robocop » dans l'US Navy avec une petite caméra d'une portée de 19,3 kilomètres, qui peut également être un composant optique sur un soldat. Les bras. Avec cet équipement, les soldats peuvent identifier l'ennemi en quelques secondes sans réseau à large bande.

D'autre part, un autre domaine d'application de ces systèmes peut être distingué, à savoir l'aide aux utilisateurs. Les systèmes de reconnaissance faciale font de plus en plus leur apparition dans la vie quotidienne. Par exemple, ils sont utilisés sur les réseaux sociaux sur Internet pour identifier quelqu'un sur une photo, et sur un smartphone pour le déverrouiller.

La nouveauté dans la reconnaissance faciale arrive grâce au développement de nouvelles caméras de type 3D. Ces caméras obtiennent de meilleurs résultats que les caméras classiques, parce qu'elles acquièrent une image tridimensionnelle de chaque

visage (perspectives)pour identifier une personne lorsqu'elle passe par le portail d'authentification. [21]

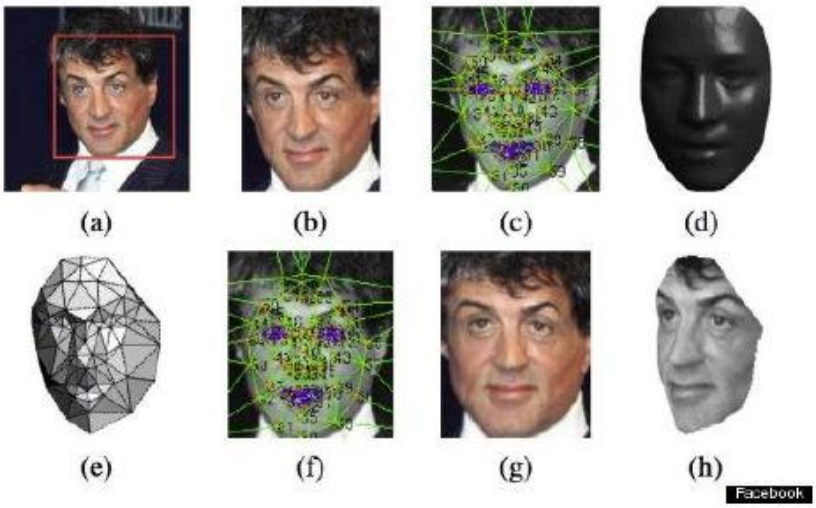


Figure II.1 : La procédure de DeepFace pour la reconnaissance [21]

II.5. Etapes de la reconnaissance de visage

La reconnaissance faciale est un système permettant d'identifier et de confirmer les personnes en contrôlant si celles-ci appartiennent à la base de données du système. L'image suit un processus de reconnaissance faciale spécifique contenant plusieurs étapes qui peuvent être illustrées dans le diagramme de la figure1 ci-dessous : [22]

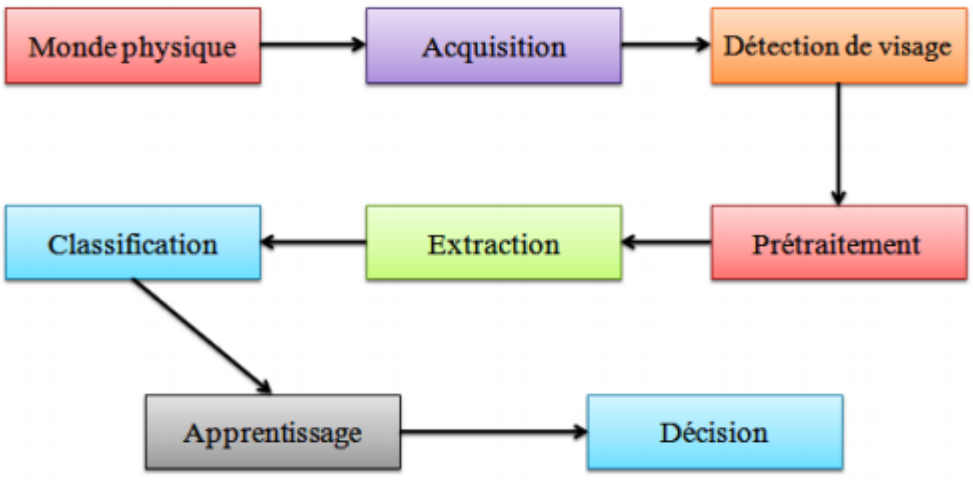


Figure II.2 : Processus d'un système de reconnaissance de visage.

II.5.1. Le monde physique

C'est le monde réel en dehors du système pré-visuel. Dans cette étape, nous prenons généralement en compte les trois éléments essentiels : la lumière, le changement de posture

et les proportions. La variation de l'un de ces trois paramètres peut se faire dans la distance entre deux images du même individu, au point de séparer deux images de deux individus différents, identifiant ainsi mal [22].

II.5.2. Acquisition

Cette étape donne lieu à une représentation 2D (la matrice des niveaux de gris) pour un objet 3D (le visage), l'acquisition de l'image et sa digitalisation comporte un risque de bruit.

Cette opération peut être statique : Appareil Photo, Scanner… etc. ou dynamique : Caméra, Webcam, dans ce cas on aura une séquence vidéo. À ce niveau on aura une image brute la figure II.3 [26].

Figure II.3: Exemple d'acquisition d'une image.[22]

II.5.3. Détection de visage

Il s'agit d'un problème de classification dans lequel l'image est affectée soit à une classe de visage, soit à une classe de non-visage.

Dans l'étape de détection, nous identifions et localisons le visage dans l'image résultante au départ, quelles que soient l'échelle, l'orientation et la lumière...

Son efficacité a un effet direct sur les performances du système de reconnaissance faciale.[26]

Figure II.4 : Détection de visage.[22]

II.5.4. Le prétraitement

Les données délivrées par les capteurs primaires ne sont pas la représentation originale de ces capteurs, donc nécessaires au traitement. Les images brutes peuvent être affectées par divers facteurs qui entraînent une perte de qualité, peuvent être bruyantes, c'est-à-dire contenir de fausses informations pour les appareils optiques ou électroniques.

Le rôle de cette étape est de supprimer le bruit d'image causé par la qualité de ces appareils, ceci est nécessaire car l'image ne peut jamais être bruyante en arrière-plan et l'éclairage est généralement il existe plusieurs types de traitement et d'optimisation de la qualité d'image, tels que la normalisation, les graphiques, la correction gamma ou des méthodes plus complexes telles que le lissage anisotrope.[22]

II.5.5. Extraction des paramètres

L'extraction paramétrique est au cœur du système d'extraction d'informations d'image qui sera stocké en mémoire pour une utilisation ultérieure dans l'étape de décision.

La sélection de ces informations utiles réside dans le modèle de visage, qui doit être discriminatoire.

Cette analyse est appelée propriétés d'indexation, de représentation ou d'extraction. L'efficacité de cette étape a un impact direct sur les performances du système de reconnaissance faciale.[22]

II.5.6. Classification

Lorsque les formulaires sont stockés dans la base de données, le système comprend des formulaires similaires provenant de plusieurs personnes ainsi qu'une liste limitée de candidats

Cette étape consiste à modéliser les paramètres extraits ou les visages de chaque individu selon des caractéristiques communes. Un modèle est une collection d'informations utiles, uniques et périodiques qui identifient une ou plusieurs personnes.[22]

II.5.7. Apprentissage

La formation consiste à retenir les modèles calculés lors de l'analyse de personnes connues. Le modèle est une représentation intégrée de l'image pour faciliter mais aussi la quantité de données stockées sous l'un ou l'autre. Cette étape correspond aux références interactives proprement dites qui sera dans la base de données des données comme indiqué dans le 4 suivant :[22]

Figure II.5: Phase d'apprentissage.[22]

II.5.8. La base des données

Une base de données est un centre de données pour collecter, coordonner, stocker et utiliser des informations. Il peut stocker et récupérer des données brutes ou des informations sur le sujet actif.

Dans la majorité des cas, ces informations sont organisées, toutes les données étant placées au même endroit sur le même support. La création d'une base de données pour les systèmes de reconnaissance faciale est un travail très compliqué car il existe de nombreux facteurs pour obtenir les données et nécessite une application stricte du protocole pour pouvoir obtenir les images obtenues.[22]

II.5.9. Décision

La décision fait partie du système par lequel nous savons si l'individu appartient à tous les visage sou non. Dans cette phase, le système de reconnaissance consiste à trouver des motifs qui correspondent à des visages récupérés auprès de personnes dans une base de données, en l'occurrence son identité.

Par conséquent, la résolution est le point culminant de ce processus. Il peut être évalué au taux de résolution de décision déterminé par le taux d'identification.[22]

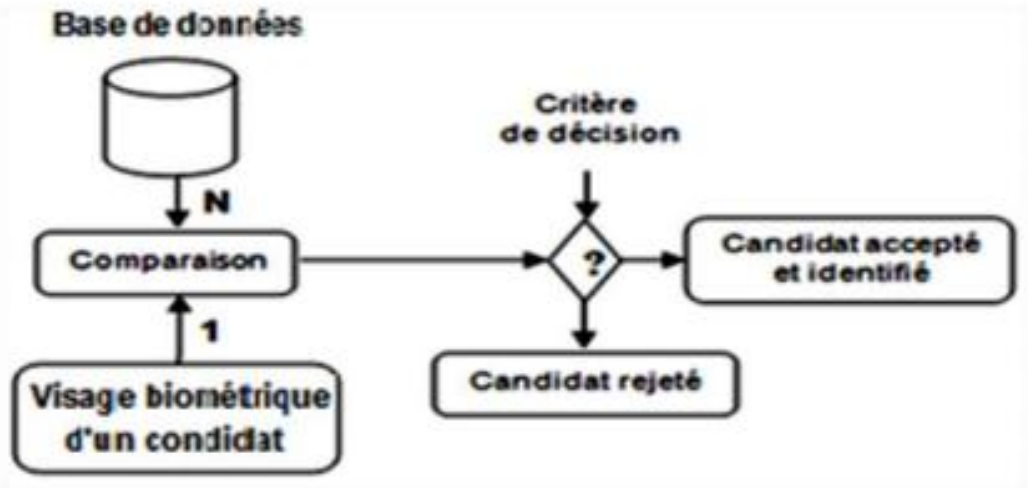


Figure II.6 : Architecture d'un système biométrique en mode identification.[22]

II.6. 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. Le schéma de la figure II.7 représente une classification détaillée de ces trois groupes. [23]

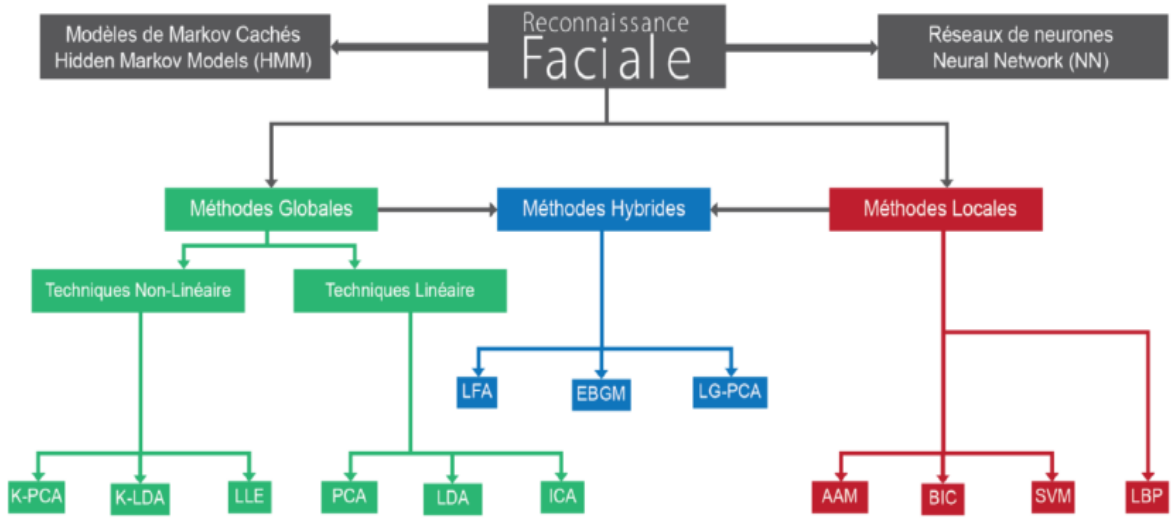


Figure II.7 : Différents méthodes d'extraction de caractéristiques. [23]

II.6.1. 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'éclairement, 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), l'Analyse Discriminante Linéaire (ADL) [23]

II.6.2. 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 étudiées dans ce travail font partie de cette catégorie. [23]

II.6.3. 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'éclairement et d'expressions faciales.[23]

II.7. Problématique

Pour le cerveau humain, le processus de la reconnaissance de visages est une tâche visuelle de haut niveau. Bien que les êtres humains puissent détecter et identifier des visages dans une scène sans beaucoup de peine, construire un système automatique qui accomplit de telles tâches représente un sérieux défi. Ce défi est d'autant plus grand lorsque les conditions d'acquisition des images sont très variables. Il existe deux types de variations associées aux images de visages : inter et intra sujet. La variation inter sujet est limitée à cause de la ressemblance physique entre les individus. Par contre la variation intra sujet est plus vaste. Elle peut être attribuée à plusieurs facteurs. Chaque visage individuel peut générer une grande variété d'images différentes. Cette grande diversité d'images de visages rend l'analyse difficile. Outre les différences générales entre les faces des variations dans l'apparence d'images de visage posent de grands problèmes à l'identification. Ces variations sont recensées comme suit :

- Changements d'éclairage influencent l'apparition d'un visage, même si la pose de la face est fixée.
- Variations de pose peuvent entraîner des changements dramatiques dans les images.
- Les expressions faciales un outil important dans la communication humaine sont une autre source de variations dans les images. Seuls quelques points de repère du visage qui sont directement couplés avec la structure osseuse du crâne, comme la distance

interoculaire ou la position générale de l'oreille sont constants dans un visage. La plupart des autres caractéristiques peuvent changer leur configuration spatiale ou position en raison de l'articulation de la mâchoire ou à l'action des muscles, comme les sourcils mobiles, les lèvres ou les joues.

- À long terme un visage change en raison du vieillissement, à une coiffure de changer ou selon maquillage ou accessoires. L'isolement et la description explicite de toutes ces différentes sources de variations doivent être le but ultime d'un système d'analyse du visage. [24]

II.7.1. Changement d'illumination

Certains facteurs tels que l'éclairage (répartition de la source de lumière, intensité, spectre) et les caractéristiques de la caméra affectent l'apparence d'un visage dans l'image acquise, comme le montre la figure II.8 suivantes :[8]

Figure II.8 : Exemples de changement d'illumination.[22]

II.7.2. Variation de pose

Les performances du système de reconnaissance faciale sont considérablement réduites lorsqu'il y a des changements de posture. Les différentes poses se produisent à partir d'un changement de perspective ou lorsque la tête est tournée vers l'intérieur. Ainsi, certains traits du visage tels que les yeux ou les yeux peuvent être partiellement masqués. [27]

Figure II.9 : Exemples de variation de pose. [27]

II.7.3. Expressions faciales

La déformation faciale due aux expressions faciales affecte principalement la partie inférieure du visage. L'information faciale trouvée en haut du visage reste presque constante, ce qui est habituellement suffisant pour mener à bien le processus d'identification. Cependant, puisque l'expression faciale modifie l'apparence du visage, elle

entraîne nécessairement une diminution du taux de reconnaissance. L'identification faciale avec l'expression faciale est un problème difficile qui est toujours pertinent et reste non résolu, la figure II.10 ci-dessous montre quelques expressions faciales.[22]

Figure II.10 : Exemples de variation d'expressions.[22]

II.7.4. Présence ou absence des composants structurels

Des aspects particuliers tels que la barbe, la moustache et les lunettes, comme le montre la figure II.11, provoquent des changements importants dans les composants structuraux du visage, notamment la forme, la couleur, la taille, etc. [22]

Figure II.11 : Exemples de composants structurels.[22]

II.7.5. Les occultations

Les visages peuvent être partiellement masqués par d'autres objets qui couvrent le visage. En effet, dans une image qui contient un groupe de personnes, par exemple, le visage peut masquer partiellement d'autres visages.[22]

Figure II.12 : Exemples d'occultation

II.8. La nouvelle tendance de la reconnaissance faciale (Deep Face Recognition)

La reconnaissance faciale profonde applique un traitement à plusieurs niveaux pour apprendre la représentation des données avec une extraction de caractéristiques à plusieurs niveaux. Cette technologie émergente a remodelé le domaine de la recherche en reconnaissance faciale depuis son lancement en 2014 par la percée de la méthode Deepface.

Depuis lors, la technologie de radiofréquence profonde, qui repose sur une architecture en couches pour assembler les pixels en une représentation constante du visage, a considérablement amélioré les performances de pointe et favorisé le succès des applications du monde réel.[25]

II.9. Avantages et inconvénients de la reconnaissance faciale

Le tableau 1 ci-dessous présente certains avantages et inconvénients de la technologie de reconnaissance faciale.[22]

Avantages	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. • Bien accepté par le public. • Aucune action de l'usager (n'implique pas de coopération de l'usager). • Pas de contact physique.	• Sensible à l'environnement d'acquisition (éclairage, position, expression du visage...) • Les vrais jumeaux ne sont pas différenciés. • Sensible aux changements (barbe, moustache, lunettes, piercing, chirurgie…)

• Technique peu coûteuse (Capteurs très bon marchés)	

Tableau II.1 : Avantages et inconvénients de la reconnaissance faciale.[22]

II.10. Conclusion

Dans ce chapitre, nous avons présenté la technologie de reconnaissance faciale pour reconnaître les personnes. Nous fournissons également un aperçu des étapes et des techniques reconnaissance de visage.

Cette recherche nous a fait savoir que la reconnaissance faciale est à l'origine de nombreux défis et obstacles techniques, ce qui a attiré davantage l'attention de la communauté scientifique.

Enfin, nous soulignons les différentes difficultés inhérentes à la reconnaissance faciale automatique qui nous permettent d'identifier les problèmes qui peuvent être résolus.

Chapitre III Normalisation d’illumination et méthode de texture locale

III.1. Introduction

La reconnaissance faciale varie considérablement en fonction de l'éclairage de la scène, pour l'œil humain, changer l'éclairage affecte la reconnaissance des personnes, plus l'image est grande et plus l'image est claire, plus la reconnaissance est de plus en plus facile. La reconnaissance faciale actuelle est très sensible aux changements d'éclairage.

Dans ce chapitre, nous essayons d'introduire les éléments complets et locaux tels que LBP, LPQ, MB-LPQ et BSIF. Ainsi les méthodes traditionnelles basées sur une compensation d'éclairement uniforme telles que la technique de normalisation TanTriggs (TT) et d'autres technique de normalisation de l'éclairage comme : la méthode de L'image du quotient de soi à échelle unique (SSQ), L'image du quotient de soi à plusieurs échelles (MSQ), Différence de Gaussian (DOG) qui est basées sur le modèle de réflexion de Lambertien.

III.2. Normalisation de l'illumination

Dans le domaine de la reconnaissance de visage, un certain nombre de méthodes de normalisation de l'illumination ont été présentées. Ces méthodes peuvent être classées en 2 grandes catégories, les méthodes basées sur la modification de la dynamique (égalisation d'histogramme, égalisation d'histogramme adaptative, transformation linéaire ou non linéaire de l'histogramme...) et des méthodes basées sur l'estimation de la réflectance de l'image (Retinex, MultiScale- Retinex, Weber face, méthodes basées sur l'isotropie de la luminance et d'autres sur l'anisotropie de la réflectance).

Les normalisations de l'état de l'art présentées dans ce chapitre sont les plus utilisées dans la reconnaissance du visage et font partie de ces deux catégories.

III.2.1. L'image du quotient de soi à échelle unique (SSQ)

L'image du quotient de soi a été développée par Wang dans 2004 et est basé sur le modèle de vision humaine de Land. De Éq : $I(x,y) = L(x,y)\,R(x,y)$. on peut en déduire que la réflectance est donnée par l'équation (1) :

$$\boldsymbol{I(x,ky)\frac{1}{L(x,y)} = R(x,y)} \qquad (1)$$

Parce que l'éclairage peut être considéré comme la basse fréquence composant alors, il peut être estimé comme :

$$\boldsymbol{L(x,y) \approx F(x,y) * I(x,y)}\,, \quad (2)$$

Avec F(x, y) est un filtre passe-bas. À partir des équations. (1) et (2) l'image du quotient de soi Q (x, y) est défini comme [28] :

$$\mathbf{Q(x,y)} = \frac{\mathbf{I(x,y)}}{\mathbf{F(x,y)} * \mathbf{I(x,y)}} \approx \mathbf{R(x,y)}. \quad (3)$$

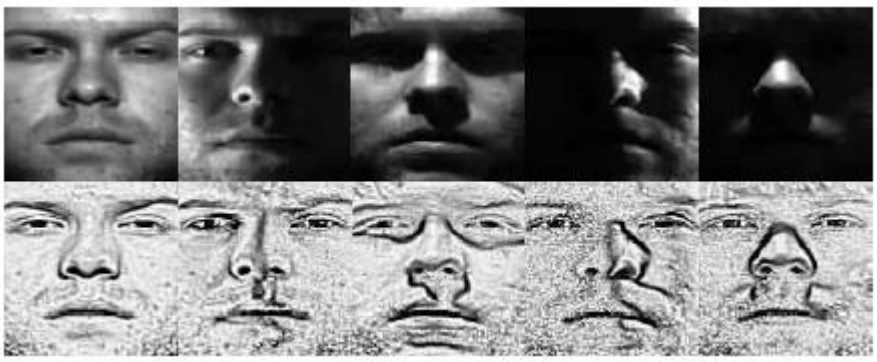


Figure III.1 : Exemples d'images traitées avec l'exemple de code : images originales (ligne supérieure), images traitées SSQ - les fonctions de réflectance (ligne inférieure) [29]

III.2.2. L'image du quotient de soi à plusieurs échelles (MSQ)

Les propriétés du $Q(x,y)$ précédent dépendent de la taille du noyau du filtre$F(x,y)$. S'il sera trop petit que $Q \approx 1$et toutes les informations de réflectance seront perdues.

De l'autre main si la taille du noyau sera trop grande alors apparaîtra un halo effets près des bords. Pour éviter ces problèmes, Wang propose approche multi-échelle où :

$$Q(x,y) = \sum_{k=1}^{n} mkT\,\{Qk(x,y)\}, \qquad (4)$$

Où : $\boldsymbol{mk}$ sont des facteurs de pondération, T est une fonction non linéaire et $\boldsymbol{Qk}$ sont des images de quotient correspondant à l'échelle.

$$Qk(x,y) = \frac{I(x,y)}{\left(\frac{1}{N} WkGk\right) * I(x,y)} \;, K = 1, \ldots\ldots, n \qquad (5)$$

Où :N est le facteur de normalisation,$WkGk$ sont des noyaux gaussiens pondérés [28].

Figure III.2 : Exemples d'images traitées avec l'exemple de code : images originales (ligne supérieure), images traitées MSQ (ligne inférieure) [29]

III.2.3. Filtrage homomorphe (HOMO)

Le filtrage homomorphe utilise le même Dans la méthode précédente, cette réflectivité et cette haute la fréquence.

Dans ce cas, le filtre passe-haut est le domaine fréquentiel de la transformée de Fourier. Traité L'image peut être trouvée par l'équation suivante :

$$\boldsymbol{I' = e^{Re}\,(IFT(FT(logI) * H))} \qquad (6)$$

Où : H est un filtre passe-haut de Butterwoth, FT la transformée de Fourier, IFT la transformée de Fourier inverse.

Dans la figure III.3 sont montrés deux exemples d'images reçues de filtrage homomorphe. [28]

Figure III.3: Deux exemples d'images reçues de HOMO [28]

III.2.4. La méthode Tan et Triggs (TT)

- **Chaîne de prétraitement :**

Cette section décrit notre approche de la normalisation de l'éclairage. Il s'agit d'une chaîne de prétraitement effectuée avant l'extraction des caractéristiques, qui contient une série d'étapes conçues pour compenser les effets des différents éclairages, des ombres locales et des reflets, tout en conservant les éléments de base de l'apparence visuelle.

La figure III.4 illustre les étapes principales et leur impact sur les images de visage typiques. Bien que motivée par l'intuition et la recherche expérimentale plutôt que par la biologie, la chaîne mondiale rappelle les premiers stades de la rétine des mammifères et du traitement visuel LGN. Les étapes spécifiques sont les suivantes : [30]

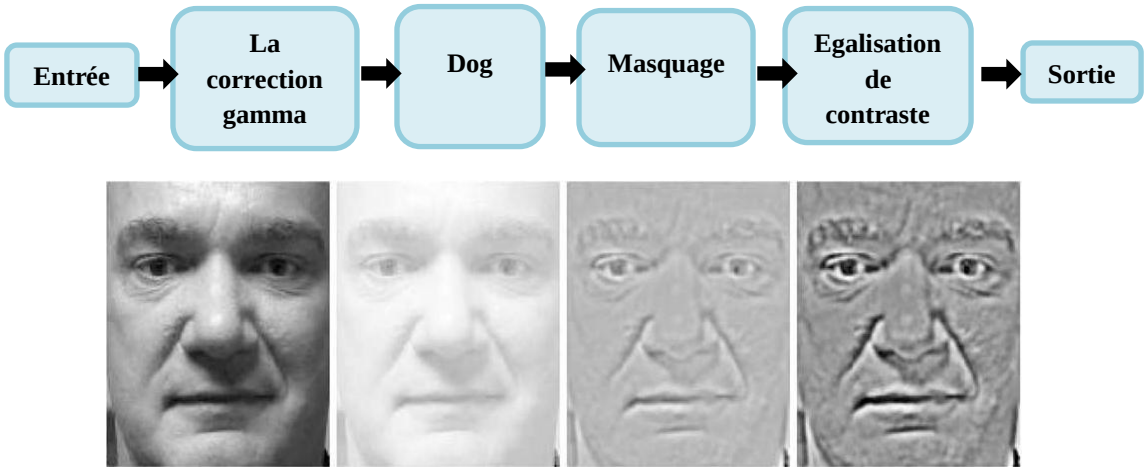


Figure III.4 : (En haut) les étapes de notre pipeline de prétraitement d'image, et (en bas) un exemple de l'effet des trois étapes — de gauche à droite : image d'entrée ; image après correction gamma ; image après filtrage DoG ; image après normalisation de contraste robuste. [30]

III.2.4.1. La correction gamma

Est une transformation de niveau de gris non linéaire qui remplace le niveau de gris I avec I^{γ} (pour $\gamma > 0$) ou $\log(I)$ (pour $\gamma = 0$), où $\gamma \in [0,1]$ est un paramètre défini par l'utilisateur.

Cela améliore la plage dynamique locale de l'image dans les régions sombres ou ombragées tout en la compressant dans les régions claires et dans les hautes lumières. Le principe sous-jacent est que l'intensité de la lumière réfléchie par un objet est le produit de l'éclairage incident et de la réflectance de surface locale.

On veut récupérer des informations au niveau de l'objet indépendamment de l'éclairement, et la prise de logs facilite la tâche en convertissant le produit en une somme :

pour un éclairement local constant, Une étape de réflexion donnée produit une étape particulière dans $log(l)$ indépendamment de l'intensité réelle de l'éclairage.

En pratique, une transformation log complète est souvent trop forte, tendant à suramplifier le bruit dans les zones sombres de l'image, mais une loi de puissance avec un exposant dans la plage [0, 0,5] est un bon compromis. Ici, nous utilisons γ comme paramètre par défaut. [30]

III.2.4.2. La technique Différence Of Gaussien (DoG)

Afin de rendre l'image capturé lisible par le système de reconnaissance, un près traitement sur l'image original est nécessaire, certaines images prisent dans des conditions d'éclairage non contrôlés dégrade considérablement le taux de la reconnaissance, et pour rendre l'image exploitable on utilise des filtres de lissage telle que le filtre gaussien.

III.2.4.2.1 Filtre Gaussien

Le filtre gaussien est un filtre linéaire, il signifie moyenne pondérée. Parce que les poids dans le filtre calculé selon une distribution gaussienne, il est nommé d'après le célèbre scientifique Carl Gauss. Ce filtre a un autre le nom est flou gaussien.

Nous pouvons lisser l'image en prenant un pixel comme valeur moyenne de ses pixels environnants. Si nous supposons que le point central est 2, les points environnants sont 1 et le point central prendra la valeur moyenne de ses points environnants, ce sera 1.

La fonction de densité appelle la fonction gaussienne. La forme 1-D est représentée dans l'équation suivante :

$$\boldsymbol{G(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-(x-a)^2/2\sigma^2}} \qquad (7)$$

Ici, a est la moyenne de x, car le point central est à la fois l'origine du point lors de calcul d'une valeur moyenne, donc a est égal à 0, la fonction sera comme suivant :

$$\boldsymbol{G(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{-x^2/2\sigma^2}} \qquad (8)$$

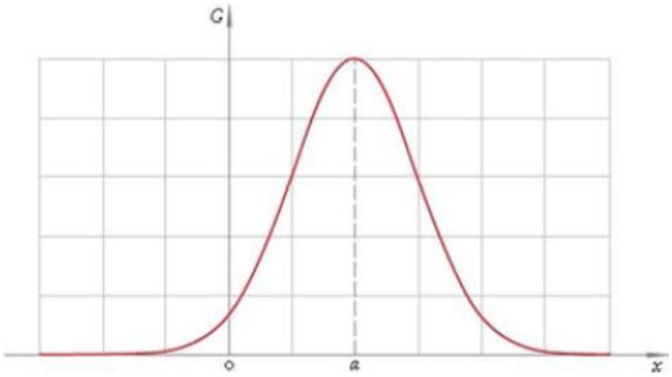


Figure III.5 : la distribution Gaussienne [33].

Si chaque point obtenait la valeur moyenne des points environnants, comment devrions-nous attribuer le poids ? Si nous utilisons simplement une moyenne simple, ce n'est pas raisonnable, car les images sont continuées, plus les points sont proches, plus la relation entre les points est proche.

La moyenne pondérée est donc plus logique que la moyenne simple, plus les points sont proches de la distance, plus le poids est important [32].

III.2.4.2.2 Principe de La technique Différence de Gaussienne (DOG)

La technique de normalisation basée sur le filtrage (DOG) est une technique de normalisation qui s'appuie sur la différence de filtre de Gaussiens pour produire l'image normalisée. Fondamentalement, il applique un filtre passe-bande à l'image d'entrée et en produit une version normalisée [33].

III.2.4.2.3 Formulation de Différence Of Gaussien (DOG)

Les DoGs ont été introduites initialement comme une représentation mathématique de la forme des champs récepteurs des cellules ganglionnaires de la rétine Le profil de luminance de la DoG issu de la différence de deux Gaussiennes est montré suit :

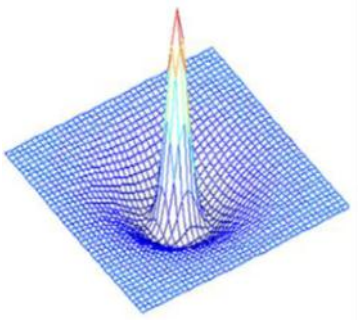


Figure III.6: Réponse fréquentielle d'une Différence de Gaussienne -DoG- [34]

Dans le plan spatial, aussi appelé plan d'image, la fonction de la DOG est donnée par l'équation

$$\boldsymbol{G_{\sigma_1\sigma_2}(x,y) = \frac{1}{2\pi\sigma_1} e^{-(x^2+y^2)/2\sigma_1^2} - \frac{1}{2\pi\sigma_2} e^{-(x^2+y^2)/2\sigma_2^2}} \qquad (9)$$

Où x et y sont les coordonnées du pixel d'une image de taille $M \times M$; a est l'échelle de la DoG, la fréquence maximale des filtres étant proportionnelle a $\frac{1}{a}$; σ_1, σ_2 représente la différence d'entendue spatiale entre les deux gaussiennes et la valeur choisie (telle que $\sigma^2 = 2.25$) correspond aux données neurophysiologiques sur les réponses des champs récepteurs des cellules ganglionnaires selon des travaux antérieurs sur la modélisation du système visuel humain ,les valeurs $C_1 = 1.8$ et $C_2 = 0.8$ sont déterminées de telle façon que la transformée de Fourier des DoG soit nulle pour la fréquence spatiale nulle ($u = v = 0$).

Pour passer d'une échelle a l'échelle suivante ; une multiplication par 2 de l'échelle initiale permet l'augmentation octave par octave, en pratique l'intervalle des échelles de décomposition dépend de la taille de l'image.

Etant donnée une échelle initiale a_1 , le nombre total d'échelles m_t est donné par l'équation (9) les échelles de la DoG sont des puissances de 2 appartenant a l'intervalle $[a_1, M/2]$; ou a_1 peut être inferieur a 1. La valeur de l'échelle a_m relative à la m^{ieme} ondelette est donnée par l'équation

$$\boldsymbol{m_t = log_2(M/a_1)} \qquad (10)$$

$$\boldsymbol{a_m = 2^{log_2(a_1)+m-1}} \qquad (11)$$

Ici, nous faisons un calcul direct dans le plan de Fourier en utilisant la formule analytique de la DoG (l'Eq (12)).

$$\boldsymbol{DoG(u,v) = K\left[exp\left(-\frac{2(\pi a)^2}{\left(\frac{u}{l}\right)^2-\left(\frac{v}{h}\right)^2}\right) - exp\left(-\frac{2(\pi a)^2}{\sigma^2\left(\left(\frac{u}{l}\right)^2-\left(\frac{v}{h}\right)^2\right)}\right)\right]} \qquad (12)$$

Avec K = -1 une constante utilisée pour la normalisation des ondelettes dans le plan de Fourier, et ($h \times l$) la taille de l'image **[34].**

Figure III.7: Exemples d'images traitées : images originales (ligne supérieure), images traitées par DOG (ligne inférieure) [2]

III.2.4.3. Masquage

Si des régions du visage (coiffure, barbe,) qui sont jugées non pertinentes ou trop variables doivent être masquées, le masque doit être appliqué à ce stade.

Dans le cas contraire, soit de forts bords de niveaux de gris artificiels sont introduits dans la convolution DoG, soit des régions invisibles sont prises en compte lors de l'égalisation de contraste.

Le bruit de grenaille, la principale source de bruit dans les capteurs CCD modernes, est proportionnel à la racine carrée de l'éclairement, ce qui le rend approximativement uniforme.

Curieusement, pour certains jeux de données, cela aide également à décaler le centre du plus grand filtre de 1 à 2 pixels par rapport au centre du plus petit, de sorte que le préfiltre final est effectivement la somme d'un DoG centré et d'un filtre spatial passe-bas, dérivé.

La meilleure direction pour le déplacement est quelque peu variable mais typiquement diagonale. L'effet n'est pas assez cohérent pour être une pratique recommandée, mais cela pourrait rapporter une enquête plus approfondie [30].

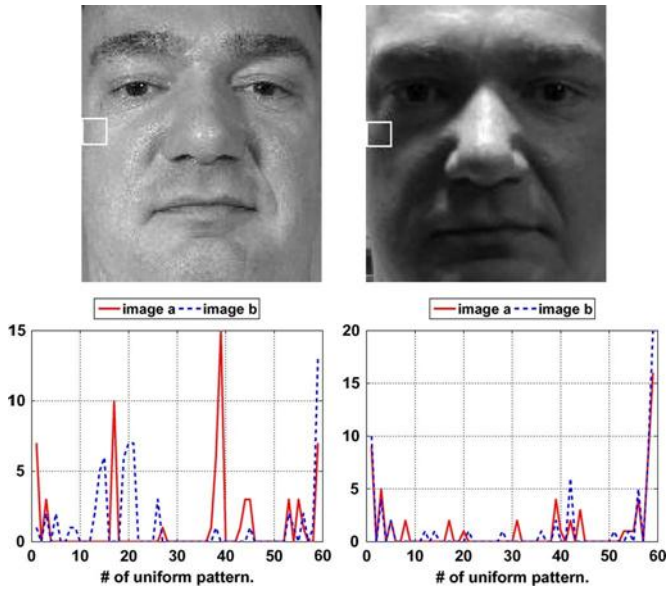


Figure III.8 : (En haut) deux images du même sujet de l'ensemble de données FRGC-204. (En bas) les histogrammes LBP des régions d'image marquées, (à gauche) sans prétraitement, (à droite) après prétraitement. [30]

III.2.4.4. Égalisation de contraste

La dernière étape de notre chaîne de prétraitement redimensionne les intensités de l'image pour standardiser une mesure robuste du contraste global ou de la variation d'intensité.

Il est important d'utiliser un estimateur robuste car le signal contient généralement des valeurs extrêmes produites par des hautes lumières, de petites régions sombres comme les narines, des ordures aux bords de l'image, etc.

On pourrait utiliser (par exemple) la médiane de la valeur absolue du signal pour cela, mais ici nous avons préféré une approximation simple et rapide basée sur un processus en deux étapes comme suit :

$$I(x,y) \leftarrow \frac{I(x,y)}{(mean\,(|I(x',y')|^{a}))^{1/a}} \qquad (13)$$

$$\mathbf{I(x,y)} \leftarrow \frac{\mathbf{I(x,y)}}{(\mathbf{mean}\,(\mathbf{min}(\tau, |\mathbf{I(x',y')}|)^{a}))^{1/a}} \qquad (14)$$

Ici, est un exposant fortement compressif qui réduit l'influence des grandes valeurs, τ est un seuil utilisé pour tronquer les grandes valeurs après la première phase de normalisation, et la moyenne est sur l'ensemble (partie non masquée de l'image).

Par défaut, nous utilisons :

$\alpha = 0.1$ et $\tau = 10$.

L'image résultante est bien mise à l'échelle mais elle peut encore contenir des valeurs extrêmes.

Pour réduire leur influence sur les étapes ultérieures du traitement, nous appliquons un mappage non linéaire final pour compresser les valeurs trop grandes. La forme fonctionnelle exacte n'est pas critique.

Ici, nous utilisons la tangente hyperbolique

$\boldsymbol{I}(\boldsymbol{x},\boldsymbol{y}) \leftarrow \boldsymbol{\tau}\, \boldsymbol{tanh}(\boldsymbol{I}(\boldsymbol{x},\boldsymbol{y})/\boldsymbol{\tau})$, limitant ainsi à la plage $(-\tau,\tau)$ [30].

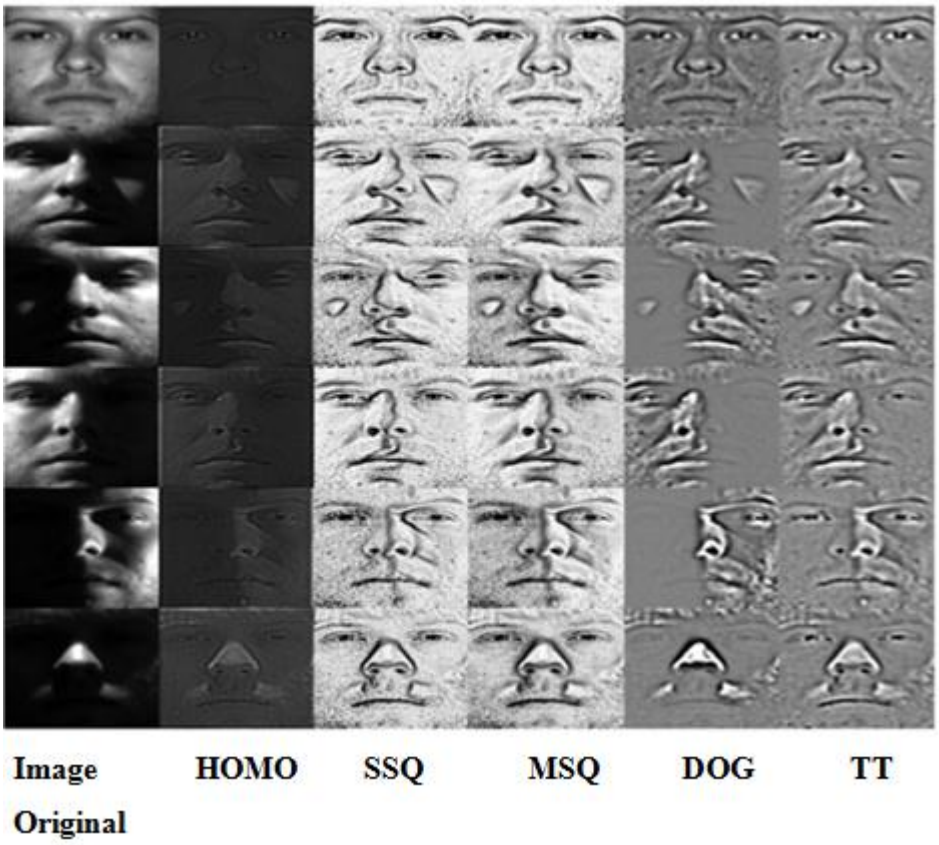


Figure III.9 : exemple de quelque méthodes de gauche à droite : Image Originale, HOMO,SSQ,MSQ, DOG,TT

III.3. Les Méthodes de Descripteurs De Textures Local

Les méthodes locales utilisent des caractéristiques faciales locales pour la reconnaissance faciale.

Dans cette méthode, le visage est représenté par un ensemble de vecteurs de caractéristiques de faible dimension au lieu d'un seul vecteur de grande dimension.

Les méthodes géométriques et basées sur des graphes ne sont pas divisées en deux catégories (descripteur de motif binaire local (LBP), descripteur de quantification de phase locale LPQ, descripteur de caractéristique d'image binaire statique (BSIF), descripteur de quantification de phase locale multibloc (MB-LPQ).

III.3.1. Descripteur Motif Binaire Local (LBP)

Cette méthode est le principe proposé par Ojala en 1996. Elle contrôle et analyse le niveau de gris de chaque pixel de l'image et donne une valeur représentative, le motif local proche du pixel.Ces valeurs ne sont pas calculées par le niveau de gris à calculer la méthode LBP.Attribuez un code binaire à chaque pixel en fonction de ses voisins.

Le code décrivant la texture locale de la région est calculé en seuillant le voisinage avec le niveau de gris du pixel central.

Il existe un mode binaire, si leur valeur de gris est supérieure ou égale au pixel courant, la valeur est "1", si l'inverse, la valeur est "0". Multipliez les pixels en mode binaire par le poids et additionnez-les pour obtenir le code LBP du pixel courant. Appliquez cette méthode aux autres pixels de l'image.

Pour les images 8 bits ordinaires pour obtenir des pixels avec une intensité comprise entre 0 et 255, vous pouvez sélectionner la dimension L'histogramme avec une valeur de 255 est utilisé comme descripteur de texture au lieu de décrire l'image par séquence de motifs LBP [34].

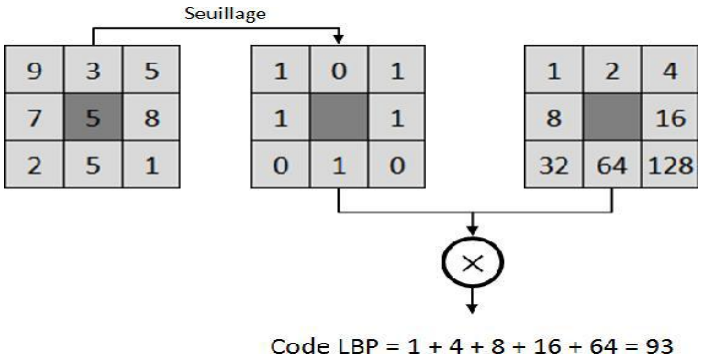


Figure III.10: Construction d'un motif binaire et calcul du code LBP **[34].**

La technologie LBP a ensuite été étendue en utilisant des quartiers de différentes tailles. Dans ce cas, prenez la valeur du cercle de rayon R autour du pixel central et le point P échantillonné au bord du cercle, et comparez avec la valeur du pixel central. Pour obtenir

la valeur de P points échantillonnés au voisinage de tout rayon R, une interpolation est nécessaire.

Nous utilisons le symbole (P, R) pour définir le voisinage de P points avec un rayon de pixel de R.

La Figure III.11 : Les voisinages pour des valeurs de R et P différentes **[34].**

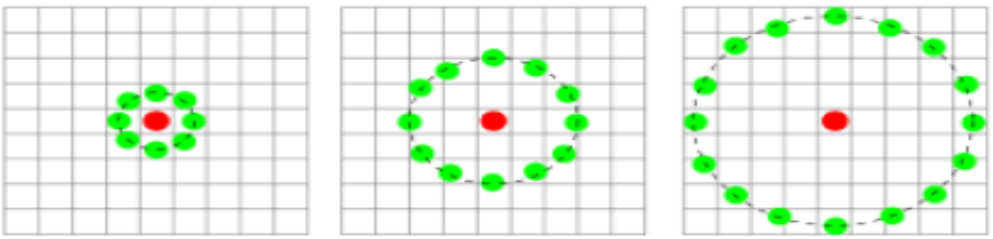


Figure III.12 : Textures particulières détectées par LBP [34]**.**

Soient gc le niveau de gris du pixel central, gp ($P = 1 \ldots P$) les niveaux de gris de ses voisins. L'indice LBP du pixel courant est calculé comme :

$$\boldsymbol{LBP_{P,R}(x_c, y_c) = \sum_{P=1}^{P} S(g_p, g_c) 2^{P-1}} \qquad (15)$$

Où

$$\boldsymbol{S(x) = \begin{cases} 1 \; si \; x \geq 0 \\ 0 \; si \; x < 0 \end{cases}} \qquad (16)$$

Ou (x,y) sont les coordonnées du pixel courant ,LBP P,R est le code LBP pour le rayon R et le nombre de voisins P. l'opérateur LBP obtenu avec P=8 et R=1 (LBP8,1) est très proche de l'opérateur LBP d'origine .

La principale déférence est que les pixels doivent d'abord être interpolés pour obtenir les valeurs des points sur le cercle (voisinage circulaire au lieu de rectangulaire).

Une autre extension à l'opérateur d'origine est le LBP uniforme. Un code LBP est uniforme s'il contient aux plus deux transitions de bits de 0 à 1 ou vice-versa lorsque la chaîne binaire est considérée circulaire. Par exemple, 00000000, 00011110 et 10000011 sont des codes uniformes.

L'utilisation d'un code LBP uniforme, noté LBPu2 a deux avantages. Le premier est le gain en mémoire et en temps de calcul. Le deuxième est que LBPu2permet de détecter uniquement les textures locales importantes, comme les spots, les fins de ligne, les bords et montré que les LBP uniformes contiennent plus de 90% de l'information d'une image.

La propriété importante du code LBP est que ce code est invariant aux changements uniformes globaux d'illumination parce que le LBP d'un pixel ne dépend que des différences entre son niveau de gris et celui de ses voisins **[35].**

III.3.2. Descripteur Quantification De Phase Locale LPQ

Cette méthode a été proposée par Ojansivu et Heikkila pour la description de la texture, l'opérateur s'est révélé robuste pour brouiller et surpasser l'opérateur de motif binaire local dans la classification des textures.

Le descripteur de quantification de phase locale est basé sur la quantification de la phase de transformée de Fourier dans les voisinages locaux.

La fréquence locale pourrait être calculée en utilisant une transformée de Fourier à court terme sur les locaux M × M, et le voisinage Np pour chaque pixel P de l'image définie par :

$$\boldsymbol{F(u,p) = \sum_{y \in Np} f(p-y) e^{-j2\pi u^T y}} \qquad (17)$$

La transformation est évaluée efficacement pour toutes les positions

$P \in \{p1, p2, p3, \ldots . pN\}$ En utilisant des convolutions 1-D pour les lignes et colonnes successivement.

Dans LPQ, seuls quatre coefficients complexes sont considérés, correspondant aux fréquences

2D$u_1 = [a, 0]^T$, $u_2 = [0, a]^T$, $u_3 = [a, a]^T$, $u_4 = [a, -a]^T$ ou est un scalaire suffisamment petit pour satisfaire $H(u_i) > 0$ soit :

$$\boldsymbol{F_p^c = [F(u_1, p), F(u_2, p), F(u_3, p), F(u_4, p)]} \text{ et } \mathbf{F_p = \left[R_e\{F_p^c\}, Im\{F_p^c\}\right]^T} \quad \textbf{(18)}$$

Ou R_e et la partie réelle et Im la partie imaginaire d'un nombre complexe, la correspondant matrice de transformation 8 par M2 est

$$\boldsymbol{W = [R_e\{w_{u1}, w_{u2}, w_{u3}, w_{u4}\}, Im\{w_{u1}, w_{u2}, w_{u3}, w_{u4}\}]^T} \qquad (19)$$

$$\text{Alor : } F_p = W\ f_x \qquad (20)$$

Les informations de phase dans les coefficients de Fourier sont enregistrées en regardent les signes des partie réelles et imaginaires de chaque composant dans Fp cela se fait en utilisant un simple scalaire quantificateur.

$$q_j = \begin{cases} 1 , g_j \geq 0 \\ 0 , g_j < 0 \end{cases} \quad (21)$$

Ou j et la composante du vecteur $\boldsymbol{G(p) = [R_e\{F(p)\}, Im\{F(p)\}]}$ les résultats des huit binaires coefficients $q_j(p)$ sont représentés comme des valeurs entre 0-255 en utilisant le codage binaire

$$\boldsymbol{f_{LPQ}(p) = \sum_{j=1}^{8} q_j 2^{j-1}} \quad (22)$$

Et comme résultat en obtient l'image d'étiquette f_{LPQ} dont les valeurs sont les étiquettes LPQ invariables de flou **[4].**

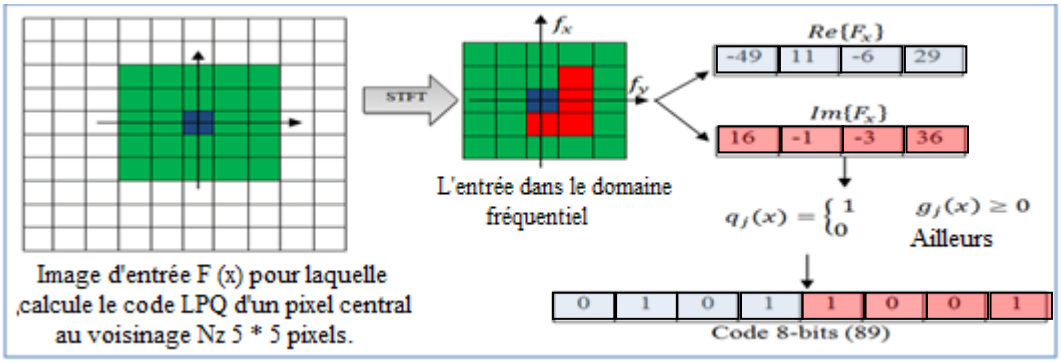


Figure III.13 : Operateur LPQ **[4].**

III.3.2.1. Descripteur Quantification De Phase Locale Multi-Bloc (MB-LPQ)

Dans ce descripteur nous avant divisé l'image acquissent en régions d'intérêt en (n x n) sous-blocs et on applique la méthode de LPQ sur chaque sous-bloc n = 1,2,3,4 et 5. Cette méthode est appelée LPQ Multi-Blocs **[34].**

III.3.3. Descripteur De Caractéristiques Statiques Binarisées De l'image (BSIF)

Cette méthode utilise un ensemble fixe des filtres à partir d'un petit ensemble d'images naturelles, ce qui prouve que les filtres pré-appris peuvent être utilise pour les déférentes

applications, contrairement aux méthodes LBP ou LPQ qui utiliser des filtres fabriqués-à-la-main.

Le principe et de calculer une chaine binaire pours les pixels d'une image d'entrée .la valeur de code d'un pixel est considérée comme un descripteur local du motif d'intensité d'image dans l'environnement du pixel plus loin.

Les histogrammes des valeurs de code des pixels permettent de caractériser les propriétés de texture au sein des sous régions d'images.

La valeur de chaque élément (bit) dans la chaîne de code binaire est calculée en binarisation de la réponse d'un filtre linéaire avec un seuil à zéro. Chaque bit est associé à un filtre différent et la longueur souhaitée de la chaîne de bits détermine le nombre de filtres utilisés. L'ensemble de filtres est appris à partir d'un ensemble d'apprentissage de correctifs d'image naturelle en maximisant l'indépendance statistique des réponses de filtre. Par conséquent, les propriétés statistiques des correctifs d'image naturels déterminent les descripteurs et par conséquent, les appelons caractéristiques d'image statistique binarisées (BSIF). Supposant une image d'entre X de taille $l * l$ et un filtre linéaire W_i de la même taille la réponse de filtre et donnée par :

$$\boldsymbol{S_i = \sum_{u,v} W_i(u,v) X(u,v) = w_i x} \qquad (23)$$

Où les vecteur w et x contiennent les pixels de W_i et X.

Et la caractéristique binarisée b_i est calculer par la proposition

$$\begin{cases} \boldsymbol{b_i = 1 \, , si \;\; S_i > 0} \\ \boldsymbol{b_i = 0 \, , si \;\; S_i \leq 0} \end{cases} \qquad (24)$$

Les filtres Wisont appris en utilisant l'analyse en composantes indépendantes (ICA) en maximisant l'indépendance statistique.

Le descripteur BSIF possède deux paramètres qui sont : la taille du filtre l et la longueur n de la chaîne binaire. Les filtres originaux proposés par Kannala et Rahtu (2012) ont été appris avec 50 000 patchs d'images **[36].**

III.4. Conclusion

La reconnaissance faciale devient difficile dans certaines conditions telles que le changement d'éclairage, le changement d'expression, etc.

Dans ce chapitre, nous avons présenté les méthodes les plus utilisées pour normaliser l'éclairement, aussi les méthodes de textures locales qui présentent une bonne robustesse pour les variations d'aspect locale.

Chapitre IV Méthodologie et conception

IV.1 Introduction

La capture d'images dans des conditions d'éclairage non contrôlées suspend les énormes difficultés de la reconnaissance faciale et reste un domaine de recherche. Bien que de nombreuses techniques aient été proposées pour résoudre ce problème, aucune d'entre elles ne peut atteindre les performances attendues.

Dans ce chapitre, nous proposons une technique pour standardiser la luminosité de l'image pour faire face aux différents changements d'éclairage ; la technique TanTriggs est combinée avec le descripteur de quantification de phase locale LPQ.

Nous allons vérifier attentivement ses résultats sur deux bases de données ; Yale B et Yale B Extended, voyons quel effet cela a pour améliorer la reconnaissance faciale sous un éclairage variable.

IV.2 Méthode D'illumination Proposée

Nous avons vu la méthode TanTriggs qu'elle est constituée de trois étapes détaillées au chapitre III : la correction gamma, le filtrage avec un filtre à Différence de Gaussiennes (DoG) et enfin une normalisation.

Dans ce chapitre, nous testerons la robustesse de ces techniques, lorsqu'elles sont combinées avec le descripteur de quantification de phase locale LPQ.

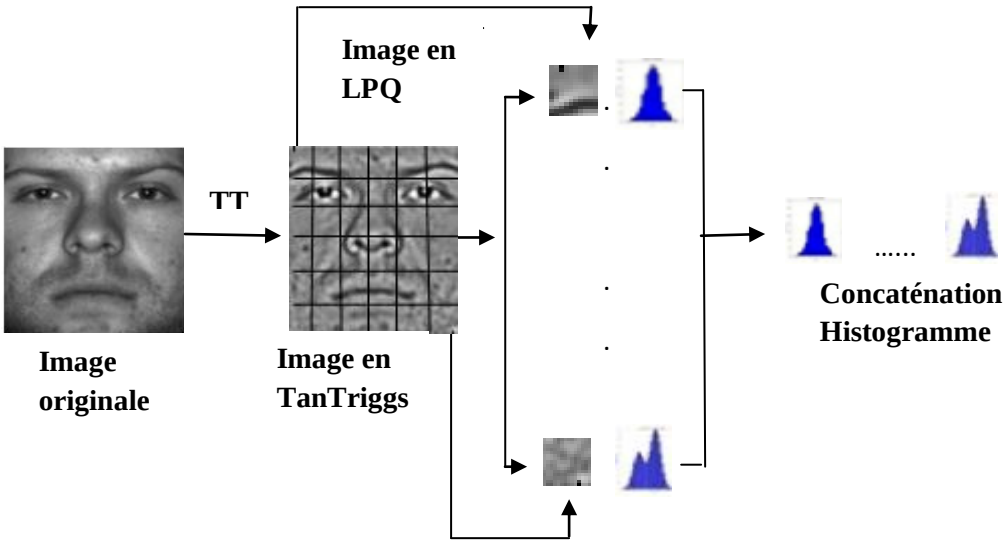


Figure IV.1 : Les différentes étapes de la méthode proposée (TT)

Tout d'abord, nous allons traiter l'image via la méthode TT, puis la diviser en sous-blocs de pixels, puis appliquer le descripteur LPQ à chaque bloc, ensuite on extraire l'histogramme de

chaque bloc, enfin Les histogrammes obtenus pour tous les blocs, sont concaténés en un vecteur caractéristique qui sera finalement utilisé comme descripteur final du visage. Le classificateur (kppv) va classer ce dernier avec la distance chi-square.

IV.3 La base de données Yale B

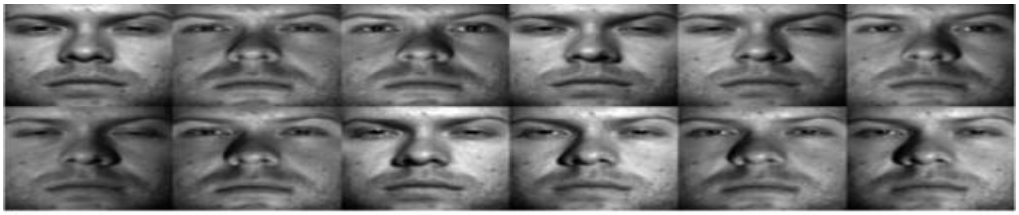
La base de données Yale B contient 10 personnes, pour chaque personne 9 poses sont prises sous 64 différents conditions d'illumination. Seulement les images frontales sont utilisées dans notre expérience. Donc, Il y a 640 images frontales qui ont divisées en cinq sous ensemble qui sont accordées suivant l'angle entre la direction de la source de la lumière et l'axe central de la caméra.

IV.4 La base de données Yale B étendue

La base Yale B créée par l'université de Yale, est la base standard pour évaluer la robustesse des systèmes de biométrie faciale en cas d'illumination variable. Elle se compose de 5760 images faciales de 10 individus capturées sous 9 poses et 64 conditions différentes d'éclairage. Récemment, elle a été mise à jour en ajoutant de nouveaux individus pour conduire à la base Yale B étendue qui contient des images de 38 individus et est donc plus difficile que la base Yale B. Pour cette base, c'est sur toute la partie avec les variations d'illumination qui est utilisée car d'autres bases telles que la base FERET sont beaucoup complètes pour l'étude des variations de pose.

Dans ces bases Yale B, nous ne nous sommes intéressés qu'aux images de face. Pour chaque individu, les images de face ont été divisées en 5 groupes selon l'angle d'éclairage : groupe 1 (0° à 12°), groupe 2 (13° à 25°), groupe 3 (26° à 50°), groupe 4 (51° à 77°) et groupe 5 (plus de 78°). La figure IV.3 montre un exemple d'images de chaque groupe pour un individu donné. Au total, dans la base Yale B, les groupes 1, 2, 3, 4 et 5 contiennent respectivement 70, 120, 120, 140 et 190 images alors que dans la base Yale B étendue, ces groupes contiennent respectivement 263, 456, 455, 526 et 714 images [38].

Sous-ensemble (S1) (0°-12°)



Sous-ensemble (S2) (13°-25°)

Sous-ensemble (S3) (26°-50°)

Sous-ensemble (S4) (51°-77°)

Sous-ensemble (S5) (> 78°)

Figure IV.2 : Les sous ensemble de la base Yale B

IV.5 Réglage des paramètres

Dans la méthode TanTriggs, le paramètre gamma pour la fonction de correction gamma, le paramètre sigma pour la méthode Différence of Gaussien (DoG) et le paramètre alfa pour la méthode d'égalisation de contraste sont définis expérimentalement.

IV.6 Ajustement de gamma

Sur des images de taille 100*100, on a changé les valeurs de gamma pour obtenir des meilleurs taux de reconnaissance. D'après la figure IV.3 on a trouvé le meilleur taux pour la valeur de gamma=0.1. Le tableau IV.I présente les taux selon les différentes tailles d'image après la fixation de gamma.

Taille d'image	Taux de reconnaissance(%)
64*64	98.26
100*100	99.68
120*120	99.71

Tableau IV.1 : Résultats de l'ajustement de gamma sur les différentes tailles d'image

Sur la base de ces résultats, nous conserverons cette valeur tout au long des prochaines expérimentations

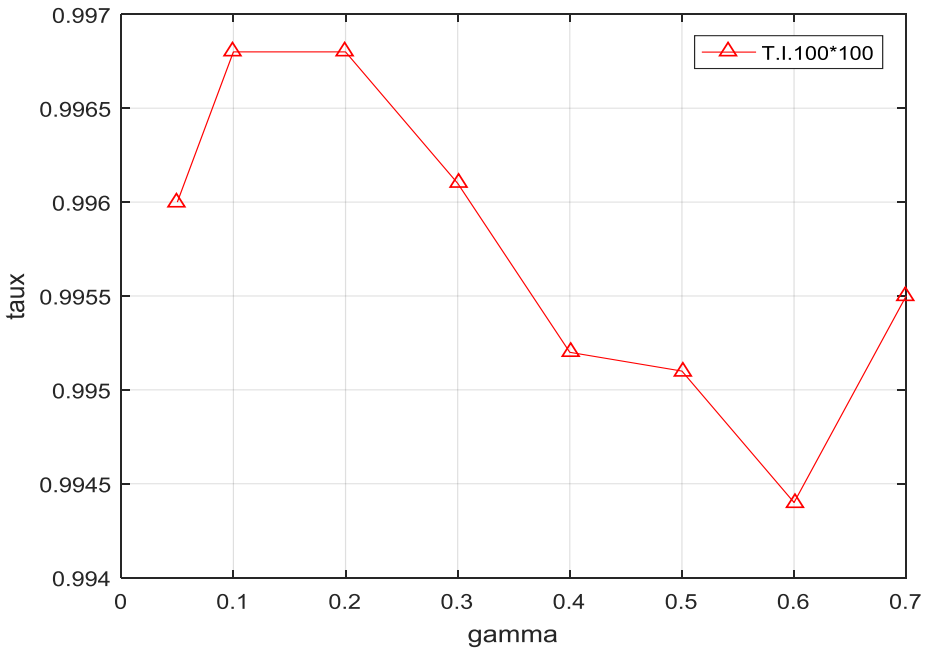


Figure IV.3 : Ajustement de gamma (T.I : Taille d'Image 100*100)

IV.7 Ajustement de sigma

Avec la méthode proposée on cherche les meilleures valeurs de taux de reconnaissance quelle peut fournir par sigma. Après la variation de sigma, la valeur de sigma =1.45 donne les meilleurs taux de reconnaissance, Où nous obtenons les résultats suivants :

Taille d'image	Taux
64*64	0.9826
100*100	0.9974
120*120	0.9971

Tableau IV.2 : Résultats de l'ajustement de sigma=1.45 sur les différentes tailles d'image

IV.8 Ajustement d'alfa

La meilleure valeur d'alfa qui nous donne le meilleur taux de reconnaissance sa change selon la taille d'image comme montre la figure IV.4 et d'après les résultats on a obtenu trois meilleures valeurs voire tableau IV.3 :

Taille d'image	Valeurs d'Alfa	Taux de reconnaissance(%)
64*64	1.7	98.54
100*100	0.7	99.82
120*120	0.4	99.79

Tableau IV.3 : Résultats de l'ajustement d'alfa sur les différentes tailles d'image

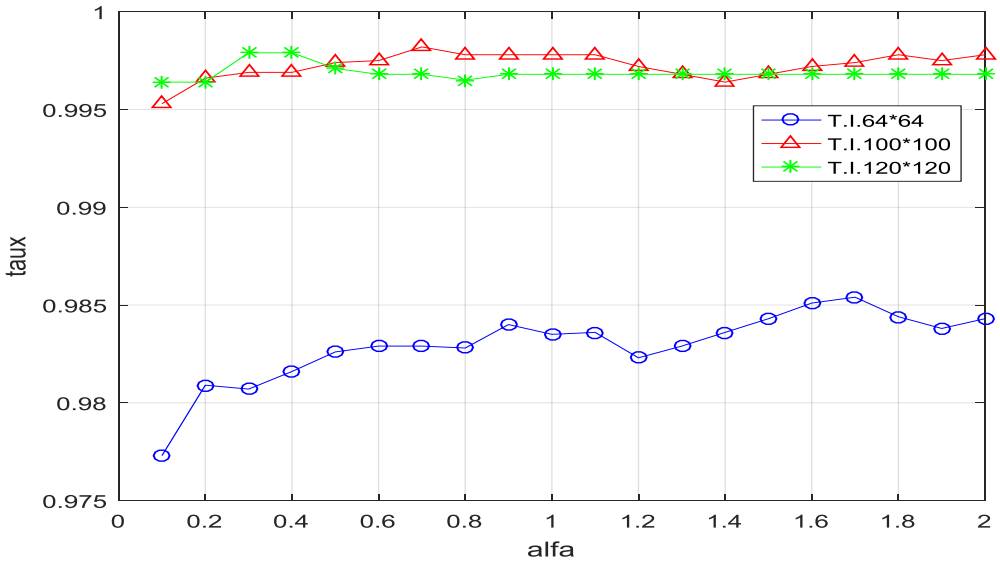


Figure IV.4 : Ajustement de d'alfa

IV.9 Ajustement de bloc

Dans cette expérience, nous avons fixés notre meilleure valeur de gamma, sigma et alfa. Pour obtenir un meilleur taux de reconnaissance pour des différents taille de bloc ou nous obtenons des résultats différents avec une taille d'image comme les résultats ci-dessus et on a montré sa dans la figure IV.5.

Taille d'image	Taille de bloc	Taux de reconnaissance (%)
64*64	H= 7	98.54
100*100	H= 10	99.82
120*120	H= 10	99.79

Tableau IV.4 : Résultats de l'ajustement de bloc sur les différentes tailles d'image

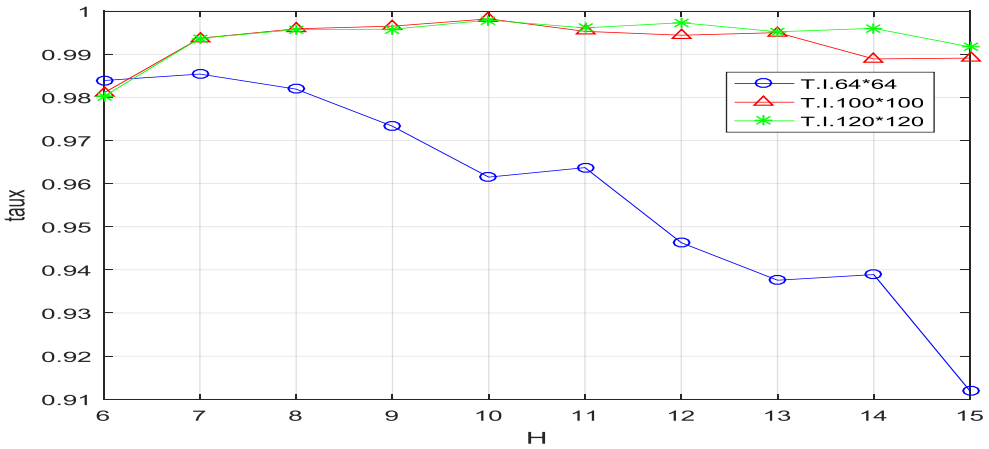


Figure IV.5 : Ajustement de bloc

IV.10 Résultats En Yale B

Après la fixation des valeurs de Gamma, Sigma, Alfa et la taille du bloc sur les résultats trouvés précédemment (Gamma=0.1, Sigma=1.45, Alfa=0.4 et taille de bloc). Le tableau IV.5 illustre les résultats obtenus aux différentes tailles des images comparé avec d'autres travaux récents. On note que les méthodes proposées permettent généralement d'avoir les taux de reconnaissance moyens les plus élevés.

		Taux de reconnaissance (%) utilisant la base de données Yale B					
Méthodes	**Size**	**S1**	**S2**	**S3**	**S4**	**S5**	**Moy.**
Notre méthode	64×64	100	100	99.17	94.29	95.79	97.85
AHFSVD-face [39]	100×100	100	99.62	96.82	91.87	99.88	94.57
AREC&SIG_SVD face [40]		100	96.64	90.12	94.94	99.36	95.76
GWLNN-face ($\delta^2 = 1$) [39]		100	100	100	98.57	97.37	98.73
Notre méthode		100	100	100	97.86	100	99.57
	120×120	100	100	100	98.57	100	99.71
	128x128	100	100	100	98.57	99.47	99.61
	192×168	100	100	100	100	98.95	99.79

Tableau IV.5: Résultats obtenus aux différentes tailles d'image sur Yale B.

IV.10 Résultats en Yale B étendue

Cette fois ci, l'efficacité de notre méthode proposée sera testée sur la base de données Yale B étendue. Le tableau IV.6 représente clairement que les taux de reconnaissance moyens obtenus en utilisant la méthode proposée surpassent toutes les autres méthodes et ce, pour tout type de tailles d'images.

	Taux de reconnaissance (%) utilisant la base de données Yale B étendue						
Méthode	**Taille d'image**	**S1**	**S2**	**S3**	**S4**	**S5**	**Moy.**
AWOGBF [41]	64×64	100	99.34	94.96	90.04	83.93	93.65
Notre méthode		100	100	100	95.06	96.22	98.26
WT [42]	100×100	98.44	97.85	97.02	96.24	95.29	96.97
TCPLRGF [43]		100	98.45	98.01	96.17	97.81	98.09
LEP+CBIS+SF [44]		100	100	99.70	93.77	94.44	97.58
Notre méthode		100	100	100	99.24	99.44	99.74
WF [45]	120×120	98.44	100	95.94	99.41	97.55	98.33
WGWF [46]		100	100	100	97.53	95.66	98.64
BLCP [47]		100	100	99.60	95.60	96.20	98.30
Notre méthode		100	100	100	99.81	98.74	99.71
LMZ MPM_CNN [48]	128×128	100	100	99.50	98.75	98.24	99.29
CAS_PEAL [49]		100	100	95.80	96.20	94.50	97.30
Notre méthode		100	100	100	99.43	98.88	99.66
LG_face [50]	192×168	99.95	100	99.54	93.89	93.17	97.31
AWF [51]		100	100	99.76	99.78	98.19	99.55
GDMQI+HE [52]		100	100	99.90	99.80	98.99	99.49
Notre méthode		100	100	100	99.62	98.04	99.53

Tableau IV.6 : Résultats obtenus aux différentes tailles d'image sur Yale B étendue.

D'après les résultats présentés dans les deux tableaux IV.5 et IV.6 qui résument les taux de reconnaissance obtenus on peut déduire que la méthode proposée donne des résultats plus performants que celle trouvé précédemment, et que pour la taille 100x100 le taux de reconnaissance atteint 99.74 sur la base Yale B étendue, et il atteint 99.79 pour la taille 192×168 sur la base Yale B.

IV.11. Conclusion

Nous proposons une méthode invariante par illumination pour la reconnaissance de visage qui s'inspire des propriétés de Tan et Triggs (TT).

Elle utilise le prétraitement de l'éclairage et l'extraction de caractéristiques invariants de l'éclairage avec le descripteur LPQ pour obtenir différentes informations de l'image du visage.

Notre méthode améliore considérablement le taux de reconnaissance par rapport les autres méthodes de reconnaissance faciale existante sur un seul échantillon sous un éclairage variable.

Conclusion générale

La biométrie est un domaine passionnant et complexe. Elle essaie de distinguer les individus à travers des outils mathématiques généralement très avancés. Cette technologie est principalement utilisée pour des raisons de sécurité et de confidentialité, nous obligeant à travailler dans un contexte très diversifié en fonction des nombreux avantages apportés (moins cher, pas de contact physique, pas de coopération personnelle). Ce mémoire appartient au domaine de la recherche biométrique ou de la reconnaissance automatique des personnes, sous les différents problèmes d'éclairage.

Notre travail de fin d'étude s'est terminé par l'amélioration des performances du système de reconnaissance faciale et la résolution des problèmes rencontrés dans le fonctionnement de ces systèmes (problèmes de vieillissement, problèmes d'expression, problèmes, éclairage...etc.), et les chercheurs en algorithmes conçus ont donné de très bons résultats, mais il n'a pas été éliminé à 100 %. Et pour résoudre le problème de luminosité dans les images on a utilisé principalement la technique TanTriggs (TT) qu'elle est constituée de trois étapes : la correction gamma, le filtrage avec un filtre à Différence de Gaussiennes (DoG) et enfin une normalisation, et qui permis de reconnaître un individu par son visage dans des conditions d'éclairage mauvaise.

Après avoir traité l'image par la méthode TT, nous la divisons en blocs de sous-pixels, puis appliquons le descripteur LPQ à chaque bloc.

puis testé cette technique sur les deux bases de données universel Yale B et Yale B étendu avec des déférents tailles des images, le taux de reconnaissance a u une nette amélioration par apport les autres méthodes faites dans des grands laboratoires de recherches, qui travaillent sur la normalisation de l'luminance qui on améliore considérablement la reconnaissance des visages sur la même base de donnée qui contiens les défirent conditions d'éclairage, la méthode TT présente un utile principale dans le traitement des problème dé lumination des images, qui rend la reconnaissance des visages dans des condition d'éclairage dégrader possible et efficace, et le champ reste ouvert pour améliorer ses performances en la combinaison avec d'autre descripteurs.

Bibliographies

[1] Hafs Toufik, «Reconnaissance Biométrique Multimodale Basé Sur La Fusion En Score De Deux Modalités Biométriques ; L'empreinte Digitale Et La Signature Manuscrite Cursive En Ligne », Thèse, Université Badji Mokhtar-ANNABA-2016.

[2] A. Chaari, « Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée », Thèse de doctorat, Université d'Evry Val d'Essonne, 2009.

[3] N. Morizet, « Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris », Ecole Nationale Supérieure des Télécommunications, 2009.

[4] SOUHILA GUERFI ABABSA, « Authentification d'individus par reconnaissance de caractéristiques biométriques liées aux visages 2D/3D » , Thèse, université d'evry val d'essonne ,2008.

[5] BettaharAbdessettar, SaberFathi, « Extraction Des Caractéristiques Pour L'analyse Biométrique D'un Visage », Mémoire Master, Université Kasdi Merbah Ouargla, 2014.

[6] Boussa Rahim Ryad, Boussad Faouzi, « Développement d'un système biométrique multimodal basé sur la fusion des scores de matching », Mémoire Master, université mouloud mammeri de tizi ouzou, 2020

[7] N. Rudin, K. Inman, G. Stolovitzky, and I. Rigoutsos. « Biometrics: Personal Identification in Networked Society», chapter DNA Based Identification, pages 287–309. Kluwer Academic Publishers, 2002

[8] Mlle KACEL Thinhinane, « Développement d'un système biométrique pour la reconnaissance de visages basé sur la transformée en ondelettes, les réseaux de neurones Feed-Forward et les réseaux de neurones récurrents », Mémoire Master, université mouloud mammeri de tizi ouzou,2019

[9] Zitouni Sif Eddine, Saci Abdelmoumen, « Authentification Et Identification Biométrique Des Personnes Par Les Empreintes Palmaire » Mémoire Master, Université Kasdi Merbah OUARGLA-2016.

[10] G. Bahtiyar. «Holistic Face Recognition by Dimension Reduction», Master's thesis, Department of Electrical and Electronics Engineering, Graduate School of Natural and Applied Sciences of the Middle East Technical University, September 2003.

[11] BENCHENNANE Ibtissam, « Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus », Thèse, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf.2015/2016

[12] A. K. Jain and A. Ross, «Multibiometrics systems», Communications of the ACM, special issue on multimodal interfaces, Vol. 47, No. 1, pp. 34–40, 2004.

Bibliographies

[13] Mejdoub, M, Amar, C.B, «Classification improvement of local feature vectors over the KNN algorithm», Multimedia tools, vol. 64, pp.197–218, 2013

[14] Dammak, M.,Mejdoub, M. Zaied, M, «Feature vector approximation based on wavelet network», In Proceedings of the 4th International Conference on Agents and Artificial Intelligence, Vilamoura, Portugal, 6–8 February 2012; pp. 394–399.

[15] un article https://www.cnil.fr/fr/definition/reconnaissance-faciale.

[16] DJOUADI Naima, MANA Zohra, «Authentification des personnes par reconnaissance de caractéristiques des visages en utilisent le réseau de neurones». Mémoire de Fin D'étude Présenté pour l'obtention du Diplôme de MASTER ACADEMIQUE. UNIVERSITE ECHAHID HAMMA LAKHDAR - EL OUED. 2016-2017.

[17] Cabal (Christian), 2003. «Rapport sur les méthodes scientifiques d'identification despersonnes à partir de données biométriques et les techniques de mise en œuvre». Officeparlementaire d'évaluation des choix scientifiques et technologiques. Enregistré à la présidencede l'Assemblée nationale Le 16 juin 2003 sous N° 938.

[18] site internet https://www.biometrie-online.net/technologies/visage

[19] reconnaissance faciale [en ligne] https://labiometrie.wordpress.com/2017/02/12/reconnaissance-faciale/

[20] F. Perronnin and J.-L. Dugelay. «Introduction à la biométrie –Authentification des individuspar traitement audio-vidéo». Traitement du signal, Vol. 19, No. 4, 2002.)

[21] Boukerrouche Youssouf, Zerriouh Ahmed. «Mise au point d'une application de détection et reconnaissance faciale». Mémoire de fin d'études pour l'obtention du diplôme de Master en Informatique. UNIVERSITÉ ABOU BEKR BELKAID DE TLEMCEN. 2017-2018

[22] BRAHMIN MOUSTAFA, GUERROUDJ BENCHERKI, «Implémentation d'un système de reconnaissance de visages à base de PCA», Mémoire du projet de fin d'études pour l'obtention du diplôme de Master. Université Djilali, BounaamaKhemis Miliana. 2017/2018

[23] El Joud Mohamed Yahye, Benamiour Ibrahim. «Mise au point d'un système de reconnaissance de visage basée Arduino», Mémoire présenté en vue de l'obtention du diplôme Master en Automatique. Université Mohamed Seddik Ben Yahia – Jijel. 2019.

[24]Mébarka BELAHCENE. «Authentification et identification en Biométrie», Thèse présentée en vue de l'obtentiondu diplôme de doctorat en sciences en Automatique. Université MohamedKhider Biskra. 2013.

[25] BouzitDhikra. «Reconnaissance de visage basée sur une approchetriangulaire» Mémoire de Find'études Master. Université de 8 Mai 1945 – Guelma -Juillet 2019.

Bibliographies

[26] Melle Arfaoui Nahla, Melle Benassou Nabila, « Système de reconnaissance de visage par la transformée en cosinus discrète», Mémoire de Find'études Master. Université de 8 Mai 1945 – Guelma - Juin 2013.

[27] BERKANE Chahrazed, BERKANI Afef. « La détection des visages», Mémoire de Find'études Master. Université Larbi Ben M'hidi Oum El Bouaghi. : 2014-2015

[28] Mariusz Leszczyński, «Image Preprocessing for Illumination Invariant Face Verification», article, Institute of Radioelectronics, Warsaw University of Technology, Warsaw, Poland

[29] Vitomir Struc, «The INface toolbox v2.0 The Matlab Toolbox for Illumination Invariant Face Recognition», University of Ljubljana Faculty of Electrotechnical Engineering

[30] X. Tan, B. Triggs. «Enhanced local texture sets for face recognition underdifficult lighting conditions», article, IEEE Transactions on Image Processing, Vol.19, No. 6, str. 1635–1650, 2010.

[31] Boukredine Yassine et Tobbeche Mohamed Seddik, « Reconnaissance Du Visage Dans Des Conditions Incontrôlée », Mémoire Master Académique, Université 8 Mai 1945 Guelma, Octobre 2020.

[32] Hameda Abd el FATEH et AL ,Article, « Edge Detection of an Image Based on Extended Difference of Gaussian », university aswan, Egypt ,2019

[33] Oktiana, et al, « Improved Cross Spectral Iris Matching Using Gradientface Based Normalization », article. Syiah Kuala University,2018

[34] Nefissa Khiari Hili. « Biométrie multimodale basée sur l'iris et le visage », These, Université Paris-Saclay; Université de Tunis El Manar, 2016.

[35] Nicolas MORIZET et al, article, « Revue des algorithmes PCA, LDA et EBGM utilisés en reconnaissance 2D du visage pour la biométrie », Institut Supérieur d' électronique de Paris (ISEP), 2006

[36] G. Guo, S.Z. Li, K. Cha, conférence,« Face Recognition by Support Vector Machines »,2000, France, pp. 196-201.

[37] Ngoc-Son Vu, « Towards unconstrained face recognition from one sample», Thèse, Institut National Polytechnique de Grenoble - INPG, 2010.

Bibliographies

[38] Changhui Hu, Xiaobo Lu, Mengjun Ye, Weili Zeng , « Singular value decomposition and local near neighbors for face recognition under varying illumination », Pattern Recognition 2016

[39] Yang Zhang et Changhui Hu et Xiaobo Lu, « Face recognition under varying illumination based on singular value decomposition and retina modeling », Springer Science+Business Media, LLC, part of Springer Nature 2018.

[40] Abdelhalim Boualleg, « An improved Weber-face-based method for face recognition under uncontrolled illumination conditions »,Int. J. Biometrics, Vol. 12, No. 2, 2020

[41] Hongtao Liang & Jie Gao & Ning Qiang, « A novel framework based on wavelet transform and principal component for face recognition under varying illumination ». Springer Science+Business Media, LLC, part of Springer Nature 2020.

[42] Arindam Kar & Pinaki Prasad Guha Neogi, (2019) « Triangular coil pattern of local radius of gyration face for heterogeneous face recognition ». Springer Science+Business Media, LLC, part of Springer Nature 2019.

[43] Kar, Arindam and Pramanik, Sourav and Chakraborty, Arghya and Bhattacharjee, Debotosh and Ho, Edmond S. L. and Shum, Hubert P. H.« LMZMPM'LMZMPM : Local Modied Zernike Moment Per-unit Mass for robust human face recognition. », IEEE transactions on information forensics and security., 16. pp. 495-509.2020

[44] Guangyi Chen, Tien D. Bui1, Adam Krzyżak, « Filter-based face recognition under varying illumination », journal institution of engineering and technology,2018

[45] Hiranmoy Roy, Debotosh Bhattacharjee, Senior Member, « Local-Gravity-Face (LG-face) for Illumination-Invariant and Heterogeneous Face Recognition ». Article in IEEE Transactions on Information Forensics and Security · July 2016

[46] Chao Yang, Shiqian Wu1,Hongping Fang,Meng Joo Er, « Adaptive Weber-face for robust illumination face recognition », Springer-Verlag GmbH Austria, part of Springer Nature 2019