République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche Scientifique
Université de Mohamed El Bachir El Ibrahimi de Bordj Bou Arréridj

Faculté des Mathématiques et d'Informatique
Département d'informatique

MEMOIRE

Présenté en vue de l'obtention du diplôme

Master en Informatique

Spécialité : Technologies de l'information et de la communication

THEME

Identification Biométrique Basée sur L'Illumination et la Réflectance

Présenté par :

-BOUSRI MEBARKA MAISSA ***- BAITICHE TAMIM***

Soutenu le : 29 JUIN 2022

Devant le jury composé de :

Président : Mr Attia Abd elouahab

Examinateur : Mme Bensefia Hassina

Encadrante : Mme BENABID SONIA

Promotion : 2021/2022

Remerciement

Après avoir rendu grâce à Allah le tout puissant et le miséricordieux, nous tenons à remercier :

Mme.BENABID Sonia, notre directrice de recherche, pour son soutien, ses conseils et toute l'aide qu'elle nous a apporté tout au long de la réalisation de ce projet,

Aux membres de jury, Mr. Attia Abdelouahan et Mme. Bensefia Hassina de nous avoir fait l'honneur d'examiner notre travail.

Nos familles qui nous ont été d'un énorme soutien durant toute la période de cette formation.

Et enfin, toute personne ayant contribué de près ou de loin à la réalisation de ce travail.

Dédicace

A l'âme de mes grands-pères et mères
A mes parents,
Dont l'amour, la patience, les sacrifices, le soutien et la présence
m'ont forgé

A mes sœurs et frères
Amir Zina, Rania, Soumia et Dounia

A mes petits neveux

Anes et acil

Je dédie ce travail

Bousri Mebarka Maissa

Dédicace

À l'être le plus cher de ma vie, ma mère
À celui qui m'a fait de moi un homme, mon père

À Mes chers frères et sœurs
Saber, Salim, Meriem et Houda

A ma petite nièce

Dorsaf

À tous mes amis de la promotion de 2éme année Master T.I.C en informatique
Je dédie ce travail

Baitiche Tamim

Résumé

Les systèmes biométriques sont de plus en plus utilisés **pour vérifier l'identité d'un individu**. Ces **systèmes présentent** un avantage majeur par rapport aux **systèmes d'authentification traditionnels**, dans la mesure où la relation entre l'authentifiant et l'individu ne peut pas être plus étroit. Compte tenu des enjeux liés à leur utilisation, notamment pour des applications dans le domaine du commerce électronique ou du **contrôle d'accès physique** (contrôle aux frontières), il est particulièrement important de disposer d'une méthodologie d'évaluation de tels systèmes. **. Le problème d'illumination** a été considéré comme celui de la plupart des **difficultés de reconnaissance faciale** et a reçu beaucoup d'attention ces dernières années. Il est bien connu que **la variation d'image résultant du changement de lumière** est plus importante que celle des différentes identités personnelles. Ces dernières années, de nombreux **algorithmes ont été développés, tels que l'algorithme SQI** pour une **reconnaissance faciale robuste** dans **diverses conditions d'éclairage**. Les propriétés invariantes et variantes **d'illumination** de **l'algorithme d'auto-quotient** sont analysées selon le modèle lambertien.

Abstract

Biometric systems are increasingly used **to verify an individual's identity**. These systems have a major advantage over traditional authentication systems, in that the relationship between the authenticator and the individual cannot be any closer. Given the issues related to their use, particularly for applications in the field of electronic commerce or physical access control (border control), it is particularly important to have a methodology for evaluating such systems. **The illumination** problem has been considered as the one **of most difficulties in face recognition** and has received much attention in recent years. It is well known that **image** variation resulting from **light change** is more significant than that from different **personal identities**. In recent years, many algorithms have been developed, **such as SQI algorithm for robust facial recognition under various lighting conditions.** The invariant and variant **illumination properties** of the **self-quotient algorithm** are analyzed according to the Lambertian model

ملخص

تستخدم أنظمة القياسات الحيوية بشكل متزايد للتحقق من **هوية الفرد**. تتمتع هذه الأنظمة بميزة رئيسية على أنظمة المصادقة التقليدية، حيث لا يمكن أن تكون العلاقة بين **المصدق والفرد أقرب.** بالنظر إلى القضايا المتعلقة باستخدامها، لا سيما للتطبيقات في مجال التجارة الإلكترونية أو مراقبة الوصول المادي (مراقبة الحدود)، من المهم بشكل خاص وجود منهجية لتقييم هذه الأنظمة. تعتبر **مشكلة الإضاءة** واحدة من أكثر الصعوبات في **التعرف على الوجوه** وقد حظيت باهتمام كبير في السنوات الأخيرة. من المعروف أن اختلاف **الصورة الناتج عن تغير الضوء** أكثر أهمية من اختلاف **الهويات الشخصية**. في السنوات الأخيرة، تم تطوير العديد من **الخوارزميات، مثل خوارزمية SQIالتعرف القوي على الوجوه في ظروف الإضاءة المختلفة. يتم تحليل خصائص الإضاءة الثابتة والمتغيرة لخوارزمية القيمة الذاتية وفقًا لنموذج لامبرت.**

ABREVIATION

ADN: Acid désoxyribonucléique ("Deoxyribonucleic Acid").

BSIF : Caractéristiques des images statistiques binarisées ("Binarized Statistical Image Features").

CMC : Caractéristique de correspondance cumulative ("Cumulative Match Characteristic").

DIP : articulation inter phalangienne distale ("distal interphalangeal joint").

EER : Taux d'erreurs égales ("Equal Error Rate").

FAR : Taux de Fausses Acceptations ("False Acceptance Rate").

FRR : Le taux de Faux Rejets ("False Rejection Rate").

FRVT : Face Recognition Vendor Test.

HTER : Taux d'erreur moyenne ("Half Total Error Rate").

IDS : système de détection d'intrusion ("Intrusion Detection System").

ICA : Analyse en composantes indépendantes ("Independent Component Analysis").

ICP : Point le plus proche itératif ("Iterative Closest Point").

LBP: Motif binaire local ("Local Binary Pattern").

LDA : Analyse Discriminante Linéaire ("Linear Discriminate Analysis").

LPQ : Quantification de phase locale ("Local phase Quantization").

PCA : Analyse en composantes principales ("Principal Component Analysis").

PhD : La boîte à outils de reconnaissance faciale (Pretty Helpful Development functions for).

ROC : Courbe représentant les taux d'erreur ("Receiver Operating Characteristic").

SVM : Machines à Vecteurs de Support

Table des figures

Table des tableaux

Table des matières

Introduction Générale

La biométrie est un groupe de technologies (appelées technologies biométriques) qui exploitent des caractéristiques humaines physiques ou comportementales telles que les empreintes digitales, la signature, l'iris, la voix, le visage, la démarche et les gestes de la main pour distinguer les personnes.

Ces données sont traitées par certaine série de processus automatisés utilisant des dispositifs tels que des scanners ou des caméras. Contrairement aux mots de passe, aux numéros d'identification personnels (PIN) faciles à oublier ou à abuser, aux clés ou aux cartes magnétiques qui doivent être portées par un individu et peuvent être facilement volées, copiées ou perdues, ces propriétés biométriques sont uniques à l'individu et il y a peu chance que d'autres individus parviennent à contourner ces caractéristiques, les technologies biométriques sont donc considérées comme les plus fortes en termes de sécurité.

De plus, la biométrie est pratique car elle n'a pas besoin d'être portée séparément. Ces fonctionnalités peuvent être bien utilisées pour obtenir une identité/authentification sur des systèmes d'accès tels que des guichets automatiques. La biométrie s'est également avérée être un puissant outil d'identification/vérification sur les scènes de crime dans le secteur médico-légal et le secteur juridique

Un système biométrique est essentiellement un système de reconnaissance de formes qui fonctionne en obtenant des données biométriques d'un individu, en extrayant un ensemble de caractéristiques à partir des données obtenues et en comparant ces caractéristiques avec la signature dans la base de données. Selon le contexte d'application, un système biométrique peut fonctionner en mode vérification ou en mode identification.

La reconnaissance faciale a progressé à pas de géant, Depuis son invention dans les années 70. Elle s'impose aujourd'hui comme la plus naturelle des mesures biométriques. Et pour cause : nous nous reconnaissons en regardant notre visage.

Problématique

La reconnaissance de visages pose de nombreux défis car les visages sont des objets déformables 3D et nous nous limitons dans ce travail à une reconnaissance à partir d'une image 2D de visage. a l'heure actuelle, il existe de nombreux algorithmes de reconnaissance de visage performants sous réserve que les conditions d'acquisition des visages soient contraintes, ce qui nécessite que les sujets soient coopératifs et veuillent se faire identifier.

Mais les problèmes de reconnaissance de visages en environnements non contrôlés ne sont pas encore résolus. Dans cette thèse, nous nous concentrerons sur des approches 2D de reconnaissance de visages en environnements non contraints (contexte de vidéosurveillance). De tels systèmes doivent pouvoir s'affranchir des problèmes suivants

Variations de pose

Variations d'illumination

Variations d'expression, d'âge

Occultation partielle du visage

Image de mauvaise qualité

Ces problèmes sont difficiles car les variations de l'apparence du visage d'une personne en conditions différentes sont souvent beaucoup plus importantes que les variations entre les images de visage de deux individus différents acquis dans les mêmes conditions (les variations intra-classes sont alors plus importantes que les variations interclasses) Et parmi tous ces problèmes, les variations d'illumination et de pose sont les deux défis les plus difficiles.

En effet, les performances de reconnaissance de visages chutent de manière très importante en cas des conditions d'illumination et/ou de pose variables. Pour résoudre le problème de ces variations intra-classes, il est communément admis que si un grand ensemble d'apprentissage comprenant l'ensemble des différentes images représentant ces variations pour chaque personne est disponible, on peut augmenter la robustesse du système de reconnaissance par la modélisation explicite de ces variations intra-classes pour chaque personne.

Cependant, nous ne pouvons pas nous placer dans ce cas-là. Il est possible de tenir compte de ces variations à plusieurs niveaux du système : au cours du prétraitement, lors de l'extraction des caractéristiques ou lors de la classification. Ce mémoire se concentre directement variations d'illumination. Grace à l'utilisation de l'algorithme SQI.

- Dans le premier chapitre nous allons introduire la biométrie avec ces caractéristiques et les différentes modalités, les systèmes biométriques avec les mesures de performances utilisées pour leur évaluation, ainsi que les avantages et les limitations de ces systèmes.
- Dans le deuxième chapitre nous allons introduire les systèmes de reconnaissance de visages, ces principales difficultés et enfin nous allons explorer les différentes techniques de reconnaissance.
- Dans le dernier chapitre nous allons voir l'algorithme utilisé sur des bases de données connu et le fonctionnement des systèmes de reconnaissance basés sur cette même modalité (le prétraitement, les méthodes d'extraction et les méthodes de comparaison).

Chapitre 1

Généralité sur l'identification biométrique

1. Introduction

La biométrie est le groupe de technologies qui utilisent des caractéristiques biométriques (physiques, comportementales ou biologiques) comme moyen d'identification des individus. Ces technologies exploitent les caractéristiques uniques des individus et ne peuvent être perdues, volées ou reconstruites, contrairement aux méthodes traditionnelles basées sur des mots de passe ou des cartes magnétiques. C'est pourquoi la biométrie semble être l'une des meilleures techniques contre l'usurpation d'identité [1].

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.

2. La Biométrie

Il existe trois façons générales de vérifier ou d'identifier une personne : ce que vous savez (PIN, mot de passe, etc.), ce que vous avez (badge, carte à puce, etc.) et) ce qu'est la personne et ce qu'elle peut faire (empreintes digitales), Ce dernier point fait référence à la biométrie. La biométrie est une Technique qui permet d'associer à une identité une personne voulant procéder à une action, grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques physiques et comportementales de cette personne préalablement enregistrées.

La biométrie désigne dans un sens très large l'étude quantitative d'une population à l'aide des mathématiques, et plus précisément dans le cas qui nous intéresse, la technologie qui analyse les caractéristiques physiques ou comportementales d'un individu et permettant la vérification de son identité.

2.1. Identification

Activité d'un sujet qui rapproche une information actuelle avec une information précédente, déjà élaborée sous forme de schème, de schéma ou de percept. (L'identification est à la base de la perception.)

2.2. Les Données biométrique

Définition

Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales…).

2.3. Système

Définition

Un système est un ensemble d'éléments qui interagissent les uns avec les autres selon certains principes ou règles. Un système est défini par : Un sous-système (ou module ou composant) est un système qui participe à un système de niveau supérieur

2.4. Système biométrique

Définition

Le système de contrôle biométrique est un système de mesure automatisé basé sur la reconnaissance des caractéristiques d'un individu.

3. Historique

Les premières formes d'utilisation de la biométrie remontent à bien plus longtemps que la plupart des gens ne le pensent. En fait, dès 3000 av. J.-C. les historiens ont des traces d'échanges commerciaux babyloniens utilisant les empreintes digitales dans les transactions de marchandises, comme bureau de signature, ou vers le VIIe siècle dans la Chine ancienne pour les mêmes raisons.

Des études scientifiques ont déjà commencé depuis le XVIIe siècle, le cas du médecin italien Marcello Malpighi (1628-1694), qui a découvert la couche basale de l'épiderme (en gros la couche la plus interne), suivi de plusieurs études par de nombreux chercheurs au fil du temps, de Johannes Evangelista Purkinje (1787 - 1869), le premier, en 1823, qui distingue les différences d'empreintes digitales. Il les classa en 9 classes de motifs jusqu'à Sir Francis Galton (1822-1911), physicien anglais qui présente ses études dans le livre "Fingerprints" et explique que les empreintes digitales sont propres à chaque être humain, qu'elles sont uniques et permanentes.

A la fin du XIXe siècle , Alphonse Bertillon (1853-1914) était un grand criminologue français, qui inventa un système (Bertillonnage 1882) permettant d'identifier les criminels en mesurant différentes parties du corps et leur morphologie et en notant les différents signes du corps que ce soit sa taille, ses cicatrices, ses taches de naissance...etc.

Et ce n'est qu'au début du XXe siècle que la recherche sur d'autres formes de reconnaissance biométrique (rétine, iris) a émergé, et avec l'arrivée des systèmes informatiques et du traitement numérique du signal à partir des années 60, a émergé l'approche informatique de la biométrie qui automatise immédiatement identification humaine [4].

Les systèmes de reconnaissance des locuteurs (1966) et de reconnaissance des empreintes digitales (1963) ont été parmi les premiers à être explorés

Les années 70 ont vu le développement et le déploiement de systèmes de géométrie de la main et le début des essais à grande échelle et l'intérêt croissant pour l'utilisation gouvernementale de ces technologies d'identification personnelle automatisée (1977) Les systèmes de vérification de signature (1983) sont apparus dans les années 80, suivis par des systèmes de visage (1981). Les systèmes de reconnaissance l'iris(1993) ont été développés dans les années 90

Au XXIème siècle d'autres systèmes biométriques plus innovants ont été développés tel que les battements de cœurs en 2012, le mouvement des yeux en 2013, la thermographie en 2014 ...etc. [4].

4. Les Modalités biométriques :

Les caractéristiques biométriques par lesquelles l'identité d'un individu peut être vérifiée sont appelées méthodes biométriques. Ces méthodes reposent sur l'analyse de données relatives à un individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique.

La biométrie biologique repose sur l'analyse de données biologiques relatives à un individu (salive, ADN, etc.).

La biométrie comportementale est basée sur l'analyse du comportement d'un individu (comment il marche, dynamique de frappe, etc.).

La biométrie morphologique repose sur certaines caractéristiques physiques permanentes et uniques à toute personne (empreinte digitale, visage, etc.).

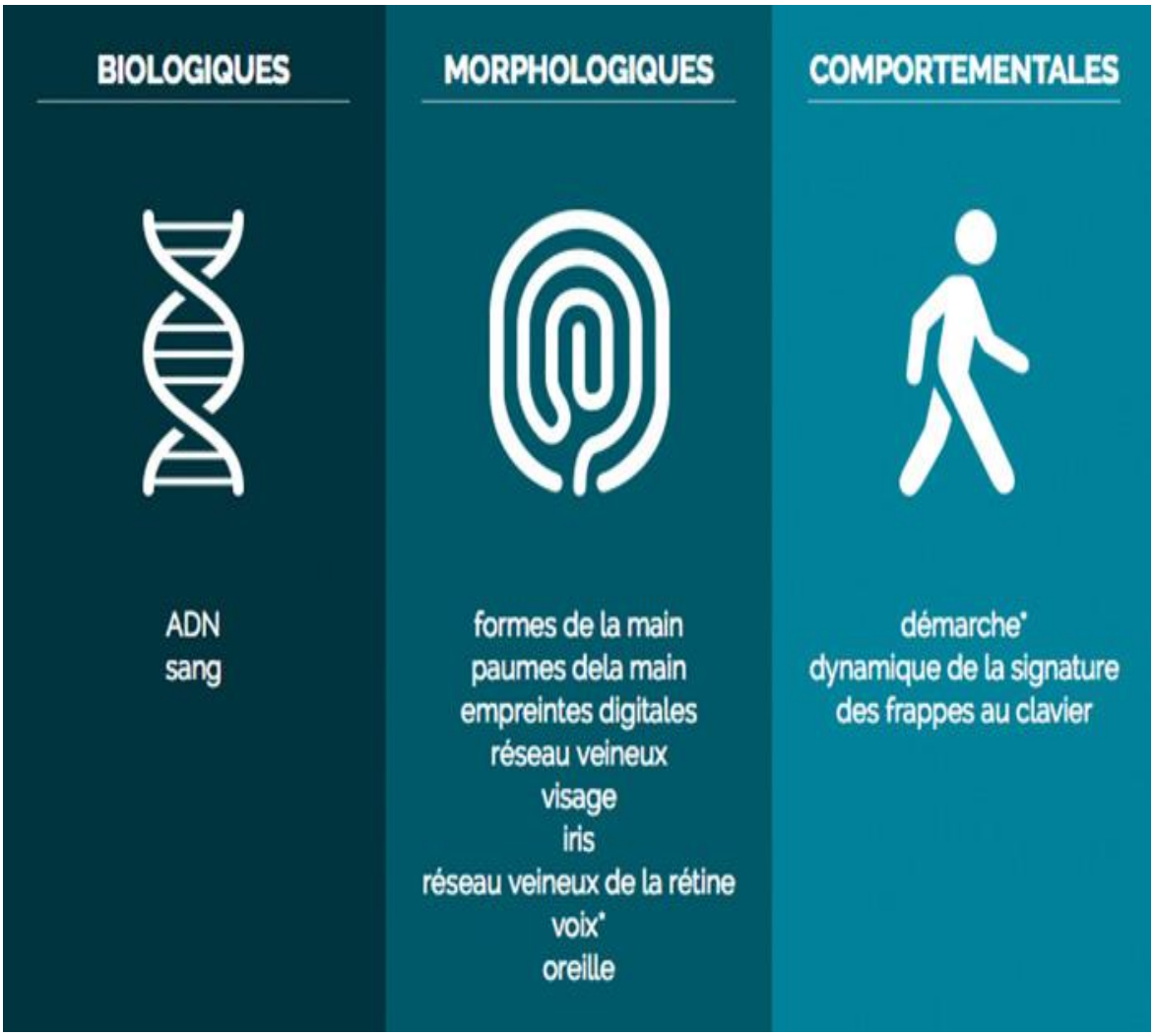

FIGURE 1 . LES MODALITES BIOMETRIQUES [W, 1]

4.1. Les Méthodes Morphologiques :

C'est la plus répandue pour sa facilité de mise en œuvre et son acceptation par le public, elle traite les caractéristiques physiques d'un individu, parmi eux citons :

A. L'empreinte Digitale :

L'empreinte digitale est le dessin formé par un doigt sur une surface suffisamment lisse pour que les dermatoglyphes y restent marqués et ils sont uniques à chaque individu et chaque doigt a sa propre empreinte. La probabilité que deux personnes aient les mêmes empreintes digitales est infinitésimale : une chance sur 64 milliards.

L'identification par cette caractéristique est la technique la plus ancienne utilisée. En fait, c'était encore le choix biométrique évident pour les services de police pendant plus de 100 ans. Il existe plusieurs types de système de capture d'empreintes digitales : optique, thermique, électromagnétique et ultrasonique.

FIGURE 2 . REPRESENTE L'EMPREINTE DIGITALE [W, 1]

Les avantages et les limites de la reconnaissance par l'empreinte digitale :

TABLEAU 1 . LES AVANTAGES ET LIMITES DE L'EMPREINTE DIGITALE.

Les Avantages	Les limites
• La plus ancienne et la plus connue des utilisateurs • Facile à mettre en œuvre • Faible coût • Technologie viable et exécution rapide	• Besoin de la coopération de l'utilisateur • Moyennement accepté par la société. • Problème d'universalité (Certaines personnes Ne possèdent ou pas d'empreinte digitales ou détruites dans le temps)

B. Le visage :

Le visage est le moyen le plus naturel d'identifier une personne, c'est pourquoi cette fonctionnalité est bien acceptée par les utilisateurs. L'image du visage peut être captée par un appareil photo numérique, ou une caméra pour en extraire un ensemble de facteurs considérés comme propres à chaque individu. [W, 1]

Au cours des 25 dernières années, les performances des systèmes de reconnaissance faciale se sont grandement améliorées, mais les résultats sont encore loin d'être parfaits.

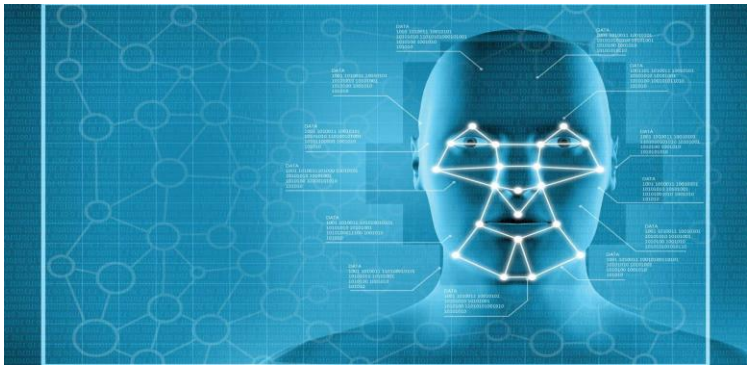

FIGURE 3 . REPRESENTE LA MODALITE VISAGE. [W, 1]

Les avantages et les limites de la reconnaissance faciale :

TABLEAU 2 . LES AVANTAGES ET LIMITES DE LA RECONNAISSANCE FACIALE

Les avantages	Les limites
• Aucun contact physique avec l'utilisateur • Faible coût • Très bien acceptées par les populations et très répandue • Performance élevées	• Sensible à l'environnement (éclairage, expression faciale…) • Impossibilité de distinguer entre deux vrais jumeaux • Sensible au changement moustaches, lunettes, barbe)

C. L'iris :

L'iris est la région annulaire entre la pupille et le blanc de l'œil. La biométrie par ce trait est récente puisqu'elle ne s'est vraiment développée que dans les années 80, et c'est une caractéristique très fiable, d'après les estimations de Daugmann, la probabilité de trouver 2 iris suffisamment identiques est d'environ 1 sur 1072, elle permet de différencier même entre jumeaux ou entre l'œil gauche et l'œil droit. L'image de l'iris est captée par une caméra standard contraignante (exemple la distance entre la caméra et l'iris ne dépasse pas un mètre), ce qui limite l'utilisation de cette modalité [W, 1]

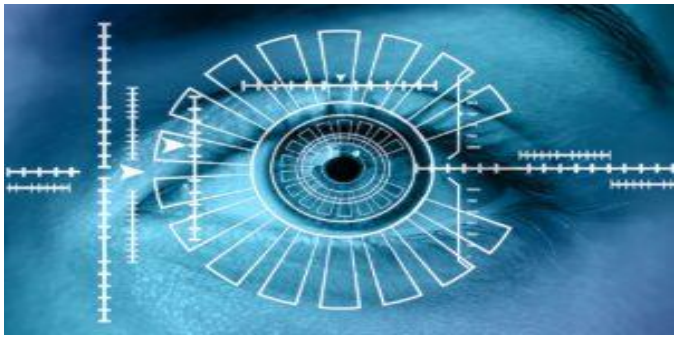

FIGURE 4 . REPRESENTE LA MODALITE IRIS [W, 1]

Les avantages et les limites de la reconnaissance de l'iris :

TABLEAU 3 . LES AVANTAGES ET LIMITES DE LA MODALITE IRIS

Les avantages	Les limites
• Performance et fiabilité très élevée • La texture de l'iris est parfaitement stable au cours du temps et passe à travers les lunettes, lentilles • Différencie entre deux vrais jumeaux	• Technologie très couteuse • Besoin de la coopération de l'utilisateur • La fiabilité diminue proportionnellement à la distance entre l'œil et le capteur

4.2. Les Méthodes comportementales :

Ce sont des méthodes qui se basent sur des éléments comportementales qui sont propres à l'individu, parmi eux citons :

A. La voix :

La voix humaine est une propriété biométrique qui ne nécessite aucun contact physique avec le système lecteur, elle dépend de la structure anatomique de l'individu, et elle est constituée de composantes physiologiques (tonalité, âge, sexe, fréquence, ton, harmoniques…) et comportementales (vitesse, rythme, etc.). En 1962, Lawrence Kersta démontre que la voix de chacun est unique et qu'elle peut être représentée graphiquement. Il existe deux façons principales de manipuler ce trait biométrique, la première étant basée sur le texte et la seconde (plus difficile) indépendante du texte. Bien que cette méthode ne nécessite pas d'équipement coûteux (microphone par exemple), le bruit ambiant et les propriétés acoustiques telles que la réflectivité et l'absorption influencent son efficacité. [W, 3]

FIGURE 5 . REPRESENTE LA MODALITE VOIX [W, 3]

Les avantages et les limites de la reconnaissance de la voix :

TABLEAU 4 . LES AVANTAGES ET LIMITES DE LA MODALITE VOIX

Les Avantages	Les limites
• 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)

B. Analyse de la démarche :

Elle consiste à identifier les individus par leurs manières de marché (mouvement du corps, longueur de pas…), qui est supposée unique pour chaque individu.

On distingue deux types de techniques de détermination de ce trait, l'approche « model-based » qui s'appuie sur certains paramètres comme la longueur des parties du corps, la longueur de la foulée, l'angle d'articulation, etc. L'approche « basée sur l'apparence » est une analyse directe de l'image par extraction de caractéristiques. Le principal avantage de ces biométries est qu'une personne peut être identifiée à distance.

FIGURE 6 . REPRESENTE LA DEMARCHE.

Les avantages et les limites de la reconnaissance de la démarche :

TABLEAU 5 . DES AVANTAGES ET LIMITES ANALYSE DE LA DEMARCHE

Les Avantages	Les limites
• 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

C. Dynamique de frappe au clavier

La dynamique de frappe est une forme de reconnaissance biométrique qui permet de vérifier l'identité d'un individu en analysant la vitesse et le rythme auquel cette personne tape. Des appuis sur les touches en passant par les fautes régulières, [W, 3] tout le monde est censé avoir une façon unique de taper. Le système basé sur cette dynamique ne nécessite aucun équipement particulier, seulement un ordinateur avec un clavier

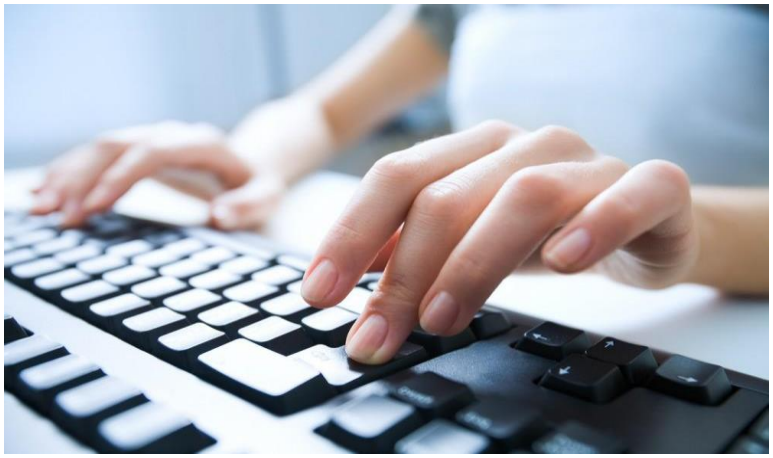

FIGURE 7 . REPRESENTE LA DYNAMIQUE DE FRAPPE AU CLAVIER [W, 3]

Les avantages et les limites de la reconnaissance de la démarche :

TABLEAU 6 . DES AVANTAGES ET LIMITES DE DYNAMIQUE DE FRAPPE AU CLAVIER

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

D. Dynamique de l'écriture (la signature) :

Chaque personne a un style d'écriture unique. On peut donc définir, à partir de la signature d'une personne, un modèle qui pourra être employé pour effectuer une identification. On distingue deux façons de capturer et de traiter une signature, soit avec des capteurs simples (scanners) et une analyse statique de la signature qui utilise la géométrie de la signature, soit par l'usage d'une palette graphique (ou équivalent) munie d'un stylo sensible à la pression et une analyse dynamique de la signature qui utilise les paramètres statiques ainsi que l'accélération, la vitesse et les profils de trajectoire de la signature.

FIGURE 8 . REPRESENTE LA DYNAMIQUE DE L'ECRITURE (LA SIGNATURE) [W, 3]

Les avantages et les limites de la reconnaissance de la dynamique de la signature :

TABLEAU 7 . DES AVANTAGES ET LIMITES DYNAMIQUE DE L'ECRITURE (LA SIGNATURE)

Les Avantages	Les limites
• 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

4.3. Les Méthodes biologiques :

Elle traite les composantes biologiques de l'individu comme :

A. L'ADN :

L'acide désoxyribonucléique ou ADN est une macromolécule biologique présente dans toutes les cellules d'un organisme et son analyse est une méthode d'identification très précise, issue directement de l'évolution de la biologie moléculaire. Or, l'identification d'une personne grâce à son ADN est très coûteuse à préparer et lente à réaliser. [W, 3]

L'information génétique d'un individu est unique (aucun membre de l'espèce ne possède la même combinaison de gènes codés dans l'ADN). Le profilage ADN, maintenant couramment utilisé pour les identifications médico-légales où il présente une percée majeure en criminalistique pour l'identification de personnes inconnues ou pour déterminer la source d'échantillons biologiques laissés sur les scènes de crime. Le profilage ADN a été officiellement introduit pour la première fois dans une affaire pénale en 1986 par l'universitaire anglais Alec Jeffreys

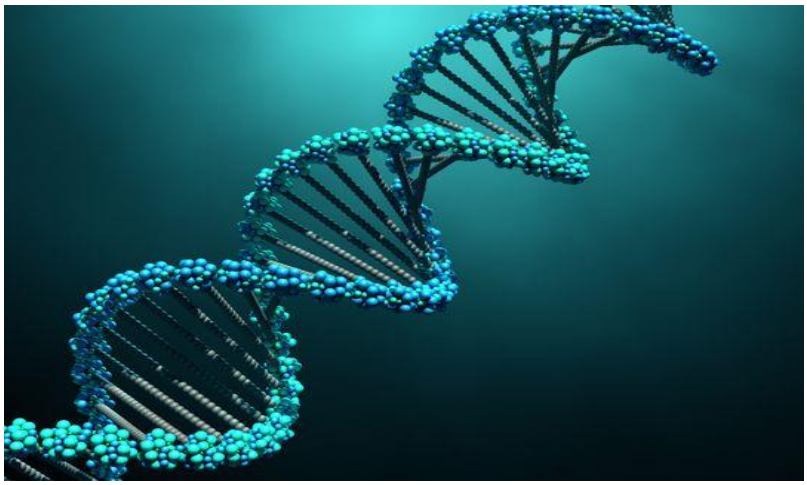

FIGURE 9 . REPRESENTE LA MODALITE BIOLOGIQUE ADN

B. La reconnaissance de la thermographie faciale :

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.

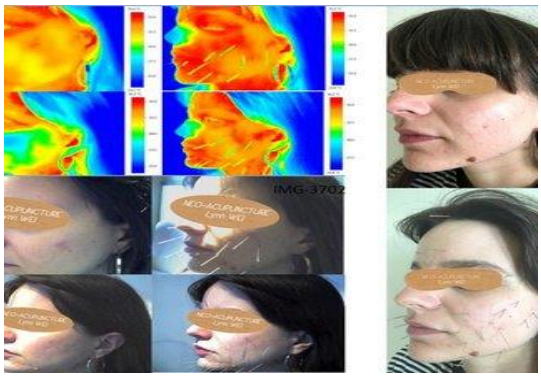

FIGURE 10 . REPRESENTE THERMOLOGIE DE VISAGE.

5. Les caractéristiques Biométriques

Presque toutes les caractéristiques Morphologiques ou comportementales peuvent être considérées comme une propriété biométrique, tant qu'elles satisfont aux caractéristiques suivantes :

Unicité : les informations doivent être aussi différentes que possible entre différentes personnes.

Universalité : toutes les personnes à identifier doivent la posséder.

Collectabilité : les informations doivent être collectables et mesurables pour pouvoir être utilisées dans des comparaisons.

Acceptabilité : le système doit répondre à certains critères (facilité d'acquisition, rapidité…) pour être utilisé.

Permanence : les informations collectées doivent être présentes tout au long de la vie de l'individu, et le système biométrique pratique doit avoir une précision acceptable et une vitesse de reconnaissance raisonnable vis-à-vis des ressources requises

La biométrie ne possède pas toutes ces propriétés, ou ne les possède qu'à des degrés divers. Aucune propriété n'est donc parfaite et elle peut être plus ou moins adaptée à certaines applications. Par exemple, l'analyse basée sur l'ADN est l'une des méthodes les plus efficaces pour vérifier ou identifier un individu.

Cependant, il ne peut pas être utilisé pour le contrôle d'accès logique ou physique pour des raisons de temps de calcul, mais aussi parce que personne ne serait prêt à donner du sang pour la vérification. Ainsi la méthode est choisie selon un compromis entre la présence ou l'absence de certaines de ces caractéristiques selon les besoins de chaque application.

A noter que le choix de la méthode biométrique peut également dépendre de la culture locale des utilisateurs.

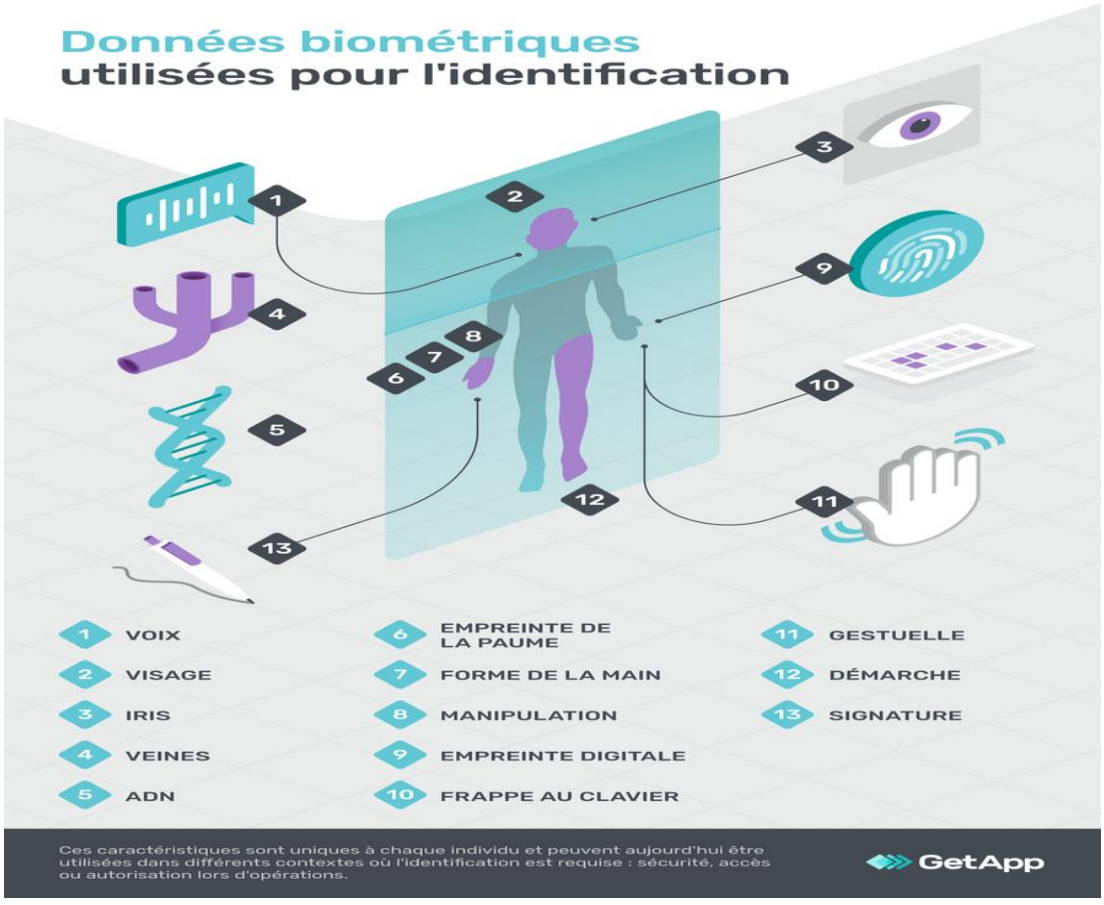

FIGURE 11 . LES DONNEES BIOMETRIQUES UTILISEES POUR L'IDENTIFICATION [W, 2]

6. Modèles Biométriques

Un modèle biométrique aussi appelé Template est l'ensemble des données utilisées pour représenter un utilisateur. Les caractéristiques biométriques acquises ne sont pas enregistrées et utilisées telles quelles. Une phase de traitement est réalisée pour réduire les données biométriques brutes et produire ainsi le modèle biométrique. Pour le stockage de ces modèles, il existe quatre emplacements principaux qui sont la clé USB, la base centralisée, la machine de travail individuelle et le capteur biométrique. Chacun de ces emplacements présente des avantages et des faiblesses en termes de temps de traitement, de confidentialité et de respect de la vie privée.

7. Utilisation de la biométrie

Le champ d'application de la biométrie est très large. En effet, tous les domaines nécessitant de vérifier ou de déterminer l'identité des personnes sont concernés. Il existe ainsi des applications de la biométrie pour gérer l'accès à des ressources physiques (comme l'accès à des lieux sécurisés) et logiques (comme le e-commerce). La biométrie intéresse également plusieurs pays (Europe, Etats-Unis, etc.)

7.1. Applications commerciales :

Telles que l'ouverture de réseau informatique, la sécurité de données électroniques, l'e-commerce, l'accès Internet, la carte de crédit, le contrôle d'accès physique, le téléphone cellulaire, la gestion des registres médicaux, l'étude à distance, etc.

7.2. Applications gouvernementales :

Afin de produire des documents d'identité plus sûrs, tels que la carte nationale d'identité ou le passeport biométrique. A noter qu'en Algérie, le passeport biométrique est désormais déployé. Il intègre une puce RFID qui contient au moins deux informations biométriques : une empreinte digitale et une image scannée du visage et même la signature numérique. Enfin, la biométrie n'a pas seulement des applications orientées vers la sécurité, mais aussi des applications qui facilitent le quotidien des utilisateurs. Les empreintes digitales restent les plus utilisées, suivies de la reconnaissance faciale. Ces deux modalités représentent les trois quarts du marché de la biométrie.

7.3. Applications juridiques :

Elles consistent généralement en l'identification de corps des victimes, la recherche criminelle, l'identification de terroriste … etc.

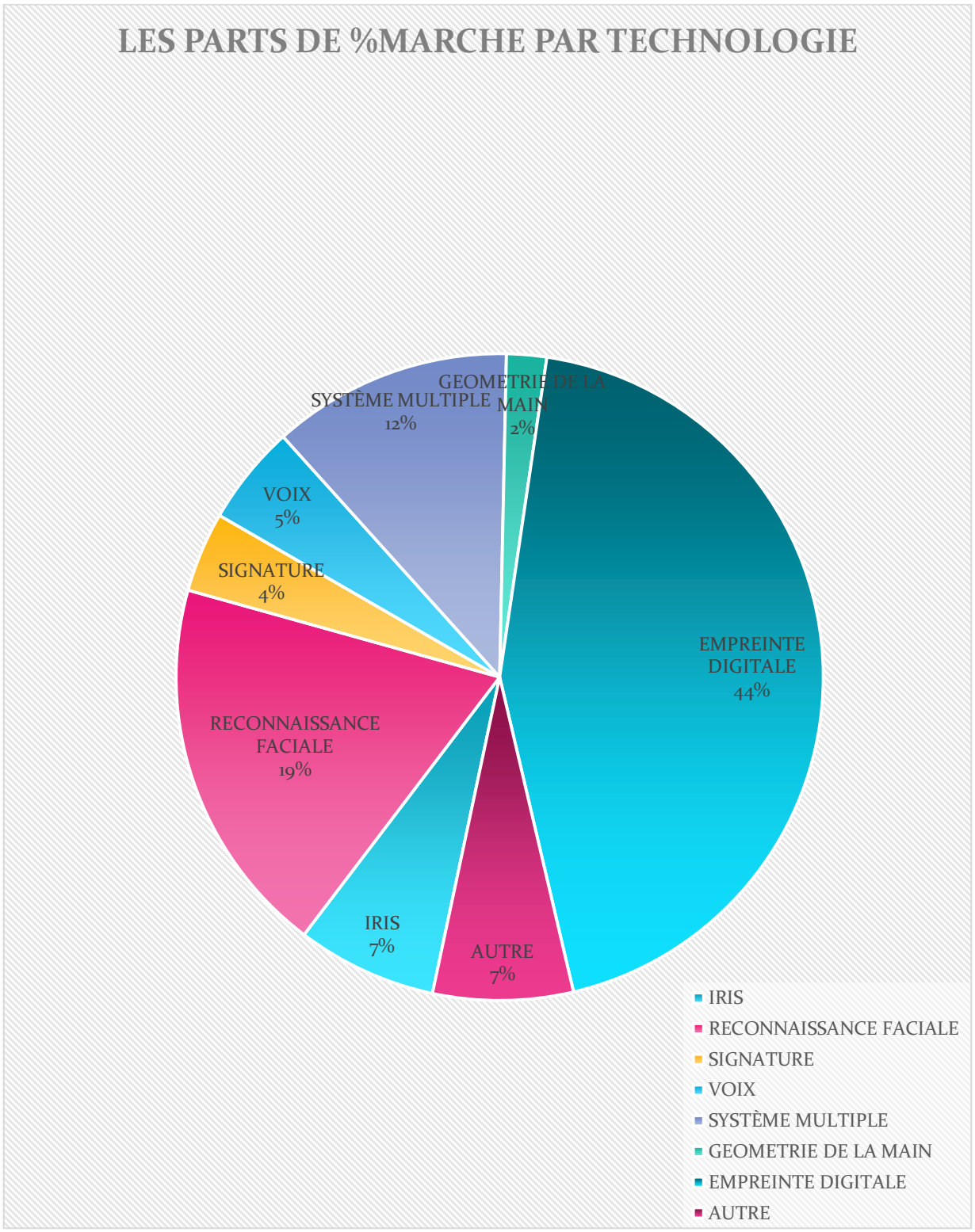

FIGURE 12 . DIAGRAMME CIRCULAIRE DES PARTS DE MARCHE PAR TECHNOLOGIE [W, 3]

8. Le fonctionnement de la biométrie

Les systèmes biométriques fonctionnent selon trois modes que sont L'enregistrement, la vérification d'identité et l'identification :

8.1. Enregistrement et Enrôlement

L'enregistrement ou enrôlement est la première étape de tout système biométrique. Il s'agit de l'étape à laquelle l'utilisateur s'enregistre pour la première fois dans le système. La vérification et l'identification sont courantes. Lors de l'enregistrement, la propriété biométrique est mesurée à l'aide d'un capteur biométrique pour en extraire la représentation numérique. Cette représentation est ensuite réduite, à l'aide d'un algorithme d'extraction bien défini, afin de réduire la quantité de données à stocker et ainsi faciliter la vérification et l'identification. Selon l'application et le niveau de sécurité requis, le gabarit biométrique sélectionné est stocké soit dans une base de données centrale, soit sur un objet personnel propre à chaque personne. [6]

8.2. La Biométrie par l'identification

En mode identification, le système biométrique identifie un individu inconnu à partir de la base de données des identités, on parle d'un test 1 : N. Dans ce cas, le système peut alors soit attribuer à l'individu non identifié correspondant au profil le plus proche trouvé dans la base de données (une liste Profils similaires), ou rejeter l'individu.

8.3. La vérification ou l'authentification

La vérification d'identité consiste à vérifier si la personne qui utilise le système est bien la personne qu'elle prétend être. Le système compare les informations biométriques acquises avec le modèle biométrique correspondant stocké dans la base de données, c'est ce qu'on appelle un test 1: 1. Dans ce cas, le système ne renvoie qu'une décision binaire (oui ou non) qui peut être pondérée.

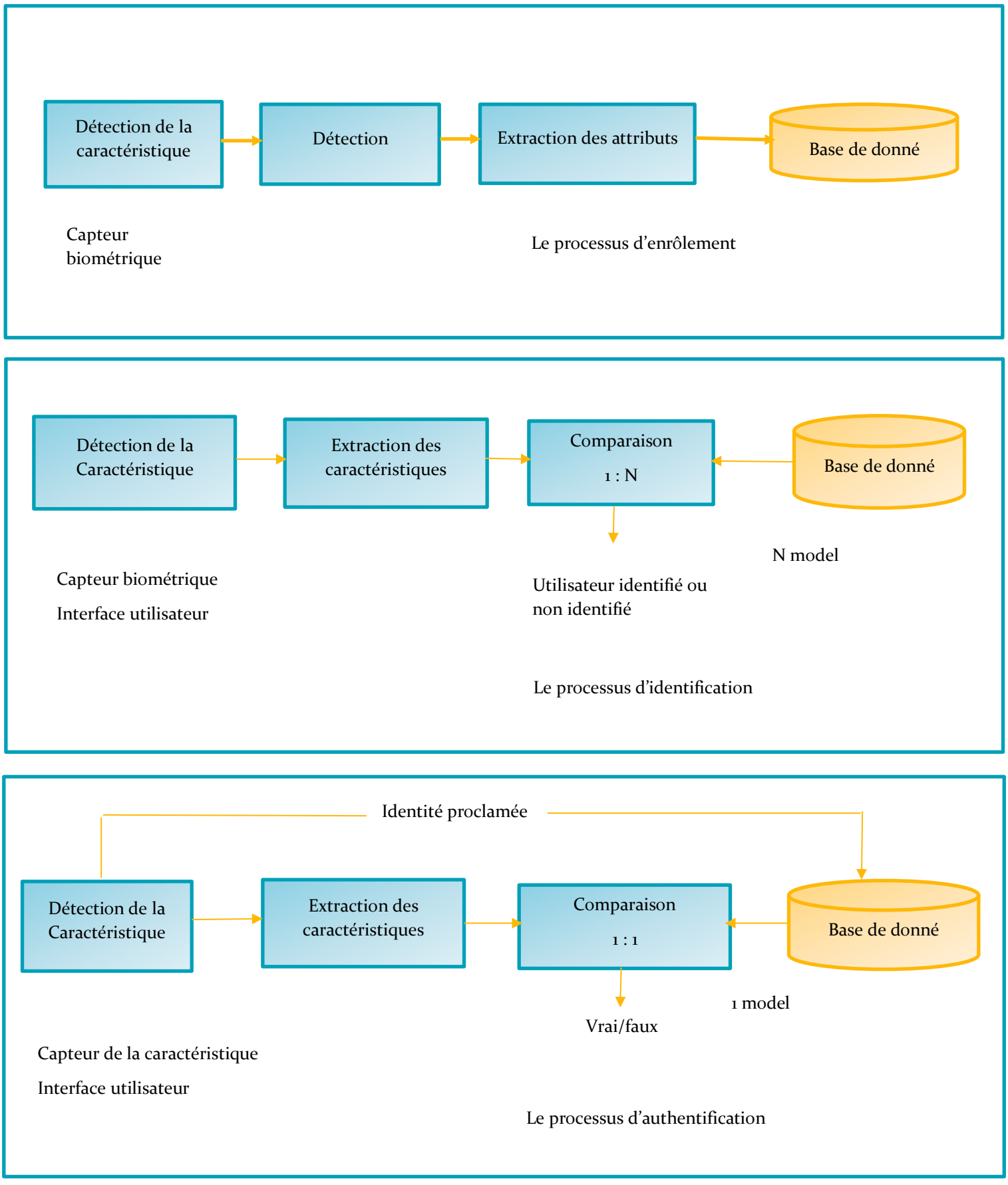

FIGURE 13 . SCHEMA FONCTIONNELLE DE L'IDENTIFICATION BIOMETRIQUE [6]

9. Les Modules d'un système biométrique :

- Module d'acquisition ou capture **:** Il s'agit d'un capteur biométrique (avec ou sans contact) qui permet d'acquérir une modalité spécifique d'une personne (caméra, microphone…etc.).

- Module de prétraitement **:** Les données brutes acquises sont prétraitées pour améliorer leurs qualités et facilité l'extraction des données discriminatoires pertinentes (caractéristiques).

- Module d'extraction de caractéristiques **:** Il détermine à partir de la donnée prétraitée la nouvelle représentation des données dite modèle ou Template. Cette nouvelle représentation doit être pertinente et idéalement unique pour chaque personne.

- Module de stockage **:** Contient les modèles biométriques des utilisateurs enroulés du système. Le système de stockage peut être par exemple, un simple fichier ou bien une base de données.

- Module de comparaison/similarité (Matching) **:** Compare les données extraites par le module d'extraction de caractéristiques à un ou plusieurs modèles préalablement enregistrés (Template). Ce module détermine ainsi le degré de similarité (ou de divergence).

- Module de décision **:** Il détermine si le degré de similitude retourné par le module de similarité est suffisant pour déterminer l'identité d'un individu. Généralement le degré est un nombre compris entre 0 (différence totale) et 1 (correspondance parfaite)

10. Architecture d'un système biométrique

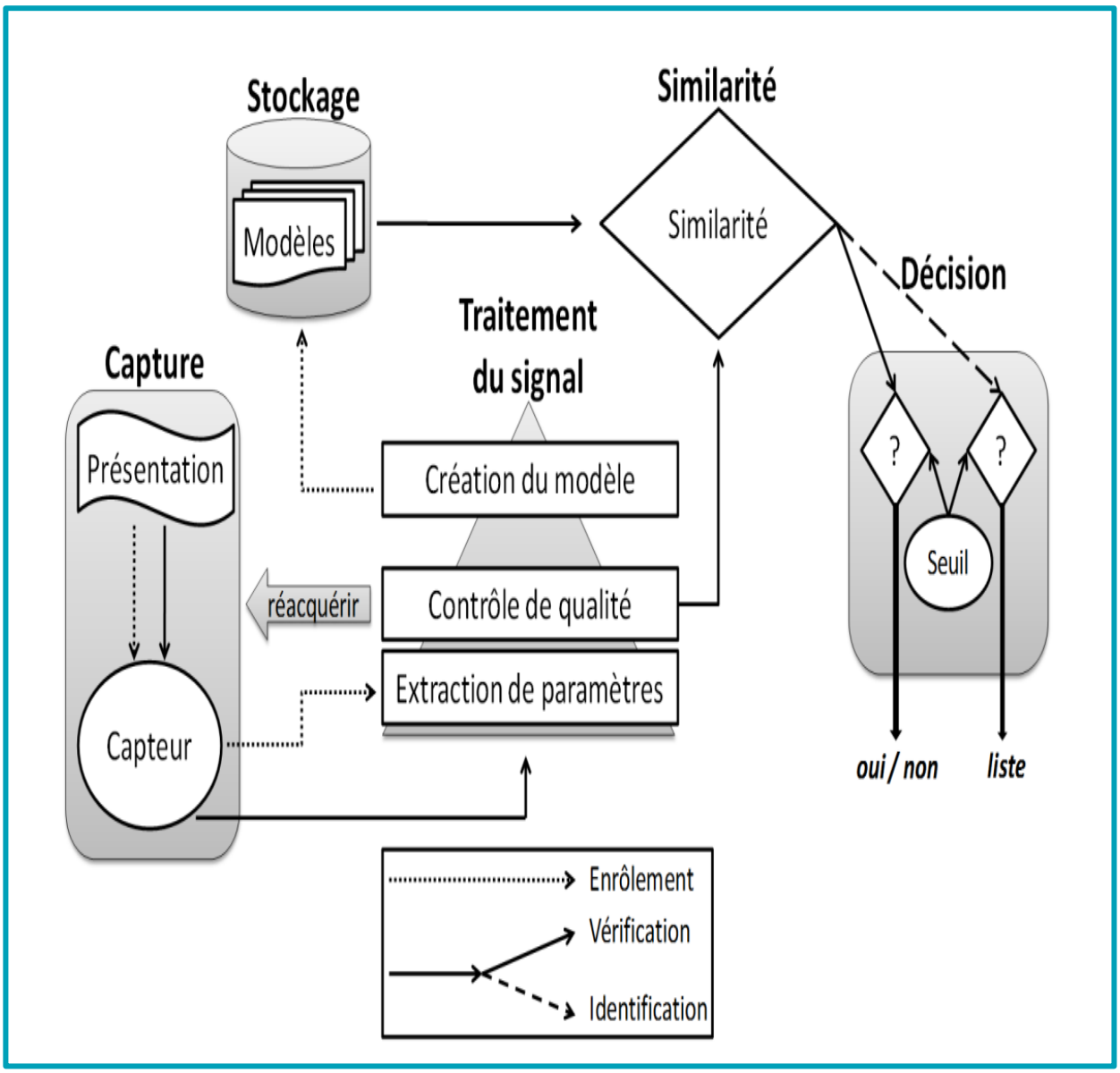

FIGURE 14 . L'ARCHITECTURE D'UN SYSTEME BIOMETRIQUE

11. Evaluation et mesure de performance :

En biométrie, nous distinguons deux types populations : les véritables clients (Genuine) qui sont autorisés à accéder dans la zone protégée et les imposteurs (Imposters) qui n'ont aucune autorisation, mais qui vont quand même essayer de rentrer d'où la performance d'un système biométrique est un élément essentiel à prendre en compte dans le choix d'un système. [10]

Il existe deux manières de présenter les performances d'un système biométrique selon le mode de fonctionnement l'application soit du type authentification ou identification :

A. Authentification :

Les indicateurs de performances dans ce mode sont

Le taux de faux rejet (« False Reject Rate » ou FRR) :

Ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés. Notons que le taux d'acceptations véritables (« Genuine Accept Rate » ou GAR) est égal à 1-FRR.

$$\boldsymbol{FRR} = \frac{nbr\ des\ imposteurs\ rejetés}{nbr\ totale\ d'accés\ \ imposteurs}$$

Le taux de faux accepté (« False Acceptance Rate » ou FAR) :

Ce taux représente le pourcentage d'individus reconnus par le système biométrique alors qu'ils n'auraient pas dû l'être.

$$\boldsymbol{FAR} = \frac{nbr\ des\ clients\ acceptés}{nbr\ totale\ d'accés\ \ imposteurs}$$

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

Ce taux représente un point de mesure de performance. Ce point correspond à L'endroit où FAR = FRR, il représente un compromis entre le nombre de faux acceptés et le nombre de faux rejetés.

$$\boldsymbol{EER} = \frac{nbr\ des\ fausses\ acceptions + nbr\ des\ faux\ rejets}{nbr\ totale\ d'accés}$$

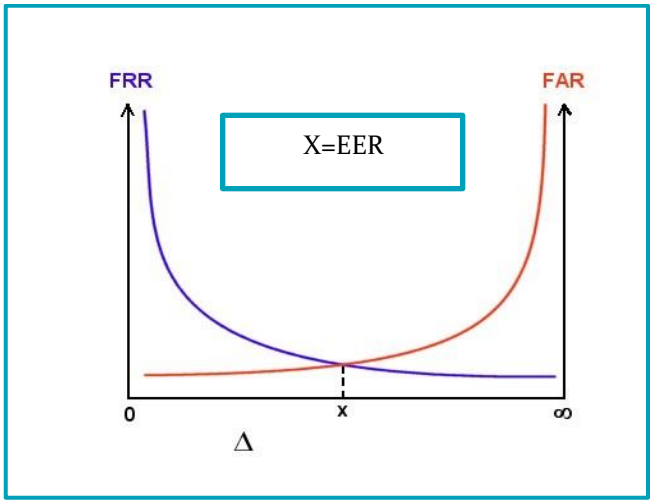

FIGURE 15 . GRAPHE DEMONSTRATIF DE L'EER

Lorsque le système opère dans ce mode, la courbe la plus couramment utilisée est appelée **courbe ROC** Receiver Operating Characteristic.

Une courbe ROC présente le taux de faux rejeté en Fonction du taux de faux accepté. Le taux d'égale erreur peut être facilement identifiable puisqu'il s'agit de l'intersection de cette courbe avec la droite d'équation $y = x$

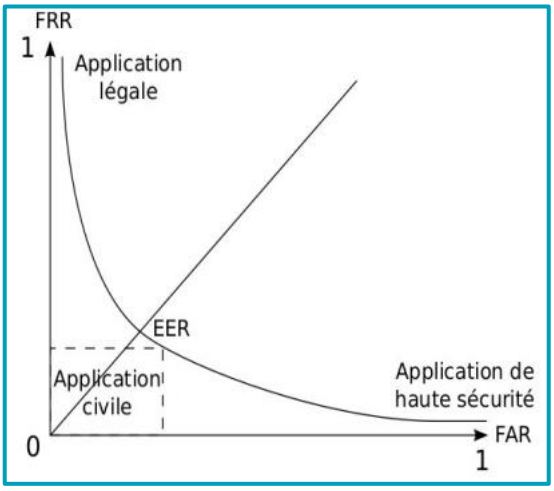

FIGURE 16 . COURBE ROC

HTER (Half Total Equal Error) : il représente la moyenne du FAR et FRR.

$$HTER = \frac{FRR + FAR}{2}$$

B. Identification

Lorsque le système opère dans ce mode on peut évaluer ses performances grâce à un seul indicateur

Le TID (Taux d'identification), c'est le pourcentage des personnes bien reconnus. La courbe la plus utilisée un test d'identification est appelée ***Courbe CMC*** (Cumulative Match Characteristic).

$$TID = \frac{nbr\ de\ test\ conducteur\ d'dentification\ correcte}{nbr\ totale\ de\ test}$$

La courbe CMC donne le pourcentage de personnes reconnues en fonction du rang, Le rang est une variable définissant à partir d'identification d'individu réalisée avec succès. On dit qu'un système reconnaît au rang 0 ou 1 selon les conventions lorsqu'il choisit la plus proche image comme résultat de la reconnaissance.

On peut donc dire que plus le rang n'est élevé, moins le système est fiable.

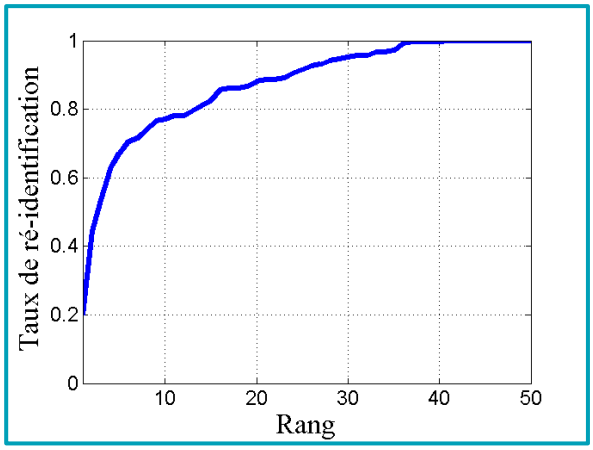

FIGURE 17 . COURBE CMC

12 Les Avantages et Limites des systèmes biométriques

A. Les Avantages

La biométrie est une technologie récente et adoptée par de grands constructeurs de matériel informatique L'usage de la biométrie est un complément ou une alternative de l'utilisation des méthodes d'authentification comme des mots de passe, des badges … etc.

Parmi les avantages de cette technique citons :

Vitesse et précision :

L'utilisation de mots de passe et de codes pour accéder de manière sécurisée à un site physique ou virtuel est assez simple, mais générique. En revanche, la technologie de sécurité biométrique désigne les mots de passe biologiques qui ne peuvent être falsifiés. En d'autres termes, l'identification et l'authentification d'un individu donné sont fiables. La reconnaissance d'iris ou faciale est de plus en plus souvent intégrée aux processus de sécurité, du fait de la rapidité et de la simplicité de la détection.

Sécurité et rentabilité :

Une fois le système de contrôle biométrique intégré, il n'y a plus besoin d'investissements infrastructurels supplémentaires. Les coûts d'investissement initiaux et récurrents chutent par conséquent de manière très nette. Ces systèmes contribuent en outre à prévenir les pertes dues à la fraude et aux entrées illégales. À lui seul, cet avantage permet d'économiser de l'argent et d'accroître la rentabilité.

Évolutif pour accompagner la croissance :

Au fur et à mesure que les entreprises grandissent, la sécurité doit impérativement évoluer avec elles. L'évolutivité constitue d'ailleurs l'un des principaux avantages des contrôles biométriques. La flexibilité de ces systèmes leur permet d'accepter facilement des données supplémentaires sur les employés. En clair, la sécurité grandit avec l'entreprise.

L'aspect pratique :

L'un des principaux avantages d'un système de contrôle biométrique tient à sa commodité. Les mots de passe n'ont pas besoin d'être réinitialisés. Une fois le test biométrique activé, la reconnaissance des empreintes digitales, de l'iris et du visage peut s'effectuer et les employés vaquer à leurs occupations. On peut même enregistrer les données et les vérifier selon les besoins.

B. Les Limites:

Bien que les applications biométriques soient constamment améliorées, ces derniers souffrent de plusieurs limites. Parmi les limites des systèmes biométriques citons :

Le bruit sur la donnée capturée :

Les données biométriques capturées peuvent être bruyantes ou endommagées, ces données bruitées risquent alors d'être mal appariées avec les modèles de la base de données aboutissant à un rejet incorrect d'un utilisateur autorisé. Des exemples de données bruitées sont une empreinte digitale avec une cicatrice, une voix altérée par un rhume mais généralement dues à des capteurs défectueux ou mal entretenus.

Les variations d'intra-classe :

Les données biométriques d'un individu acquises pendant l'authentification peuvent être très différentes des données enrôlées (Template) dans la base de données. Cette variation peut être causée par une mauvaise interaction entre l'utilisateur et le capteur (changement de pose), une variation des conditions de l'environnement ambiant (changements d'éclairage) ou même par une variation de la constitution psychologique de l'individu (expression faciale).

Unicité

Alors qu'un trait biométrique est censé être unique et variable d'un individu à l'autre, il peut y avoir de grandes similitudes interclasses par rapport à ce trait (apparence faciale des vrais jumeaux), ce qui risque d'augmenter le taux de fausse acceptation du système.

Non-universalité :

L'utilisation d'un système biométrique unimodal suppose que chaque individu de la population ciblée possède la modalité en question. Or, ce n'est pas toujours vrai et une partie de cette population (malades ou de handicapés) risquent d'être exclus.

Les attaques :

Il est vrai que les traits biométriques sont beaucoup plus difficiles à contrés que les moyens d'identification classiques (les mots de passe et les cartes d'accès). Cependant, les impostures existent en particulier dans les modalités comportementales telles que la signature et la voix. Les traits physiologiques sont également sensibles aux attaques d'usurpation (l'utilisation de silicone pour reproduire des empreintes digitales).

Conclusion

La biométrie continue de se démocratiser, elle peut apporter une sécurité accrue et une expérience utilisateur grandement améliorée, ce qui pourrait en faire le candidat idéal pour la sécurité des données.

Ainsi, l'intérêt principal des systèmes biométriques est de reconnaître automatiquement l'identité des individus à l'aide de leurs caractéristiques morphologiques ou comportementales. Ils donnent des bonnes performances avec des différents taux de reconnaissances.

Dans ce chapitre, nous avons présenté la biométrie. Nous avons d'abord vu une définition de la biométrie et son histoire, puis quelques-unes des modalités biométriques les plus connues par famille et les caractéristiques biométriques, puis l'évolution du marché de la biométrie et de ses domaines d'application et enfin, nous avons vu l'architecture et principe de fonctionnement des systèmes biométriques, ainsi que l'évaluation et la mesure des performances, les avantages et les limites de ces systèmes.

Dans le chapitre suivant, nous verrons l'état de l'art en matière de reconnaissance faciale.

Chapitre 2

La Reconnaissance Faciale

1. Introduction

La facilité de reconnaissance des personnes par leur visage et les développements technologiques survenus ces dernières années, notamment en informatique et en intelligence artificielle, ont suscité un grand intérêt parmi les scientifiques et les chercheurs pour développer des systèmes de reconnaissance automatique des visages, en fait depuis le début des années nonante il est devenu possible de créer ce système de reconnaissance

Bien que cette technologie soit efficace, performante et bénéfique pour certaines applications à des fins de sécurité, elle présente certaines difficultés techniques ou problèmes éthiques selon certaines personnes ou organisations, et le respect de la vie privée n'est plus garanti car les images faciales doivent être stockées et mémorisées dans des bases de données pour assurer la fonctionnalité du système de reconnaissance

Dans ce chapitre nous allons expliquer le principe de fonctionnement d'un système de reconnaissance automatique du visage, nous verrons par la suite les méthodes de reconnaissance de visage avec quelques techniques les plus connues pour chaque méthode.

2. Le visage

Le visage reste le moyen et la modalité de reconnaissance la plus naturel, et la plus acceptée parmi les autres modalités par la population car e permet une reconnaissance à distance (non intrusive) et ne nécessite aucune coopération de l'utilisateur, d'autre part, il est économiquement supérieurs aux autres méthodes, les capteurs sont très peu coûteux et faciles à mettre en place (une simple caméra suffit).

Cependant, il est nécessaire de prendre en compte les difficultés des systèmes existants (présence d'éléments structuraux, changement d'emplacement, éclairage) pour maximiser leurs performances

3. Système de reconnaissance du visage (faciale)

La reconnaissance faciale est une **technologie à même d'identifier ou de vérifier un sujet au moyen d'une image, une vidéo ou tout élément audiovisuel de son visage** apparue avec l'une des premières tentatives faite en 1973 par Takeo Kanade lors de sa thèse de doctorat à l'Université de Kyoto Basée sur l'intelligence artificielle.

Il s'agit d'une **méthode d'identification biométrique** qui utilise les mesures corporelles, dans ce cas, le visage et la tête, afin de **vérifier l'identité d'une personne grâce à sa disposition et ses données biométriques faciales**. La technologie recueille un ensemble de données biométriques uniques auprès de chaque personne, associées à son visage et expression faciale afin d'identifier, vérifier et/ou authentifier une personne

La procédure requiert tout simplement l'usage d'un dispositif disposant de la technologie photographique digitale aux effets de générer et d'obtenir les images et données nécessaires à créer et enregistrer la structure faciale biométrique de la personne devant être identifiée.

Contrairement à d'autres solutions d'identification telles que les mots de passe, la vérification moyennant e-mail, les solfies ou images, ou l'identification des empreintes digitales, la reconnaissance faciale biométrique utilise des modèles mathématiques et dynamiques uniques qui rendent ce système l'un des plus sûrs et effectifs

L'objectif de la reconnaissance faciale consiste en, à partir d'une image entrante, trouver une série de données appartenant au même visage dans un ensemble d'images d'apprentissage d'une base de données. La grande difficulté consiste en garantir que ce processus soit effectué en temps réel, ce qui n'est pas disponible chez tous les fournisseurs de logiciel de reconnaissance faciale biométrique.

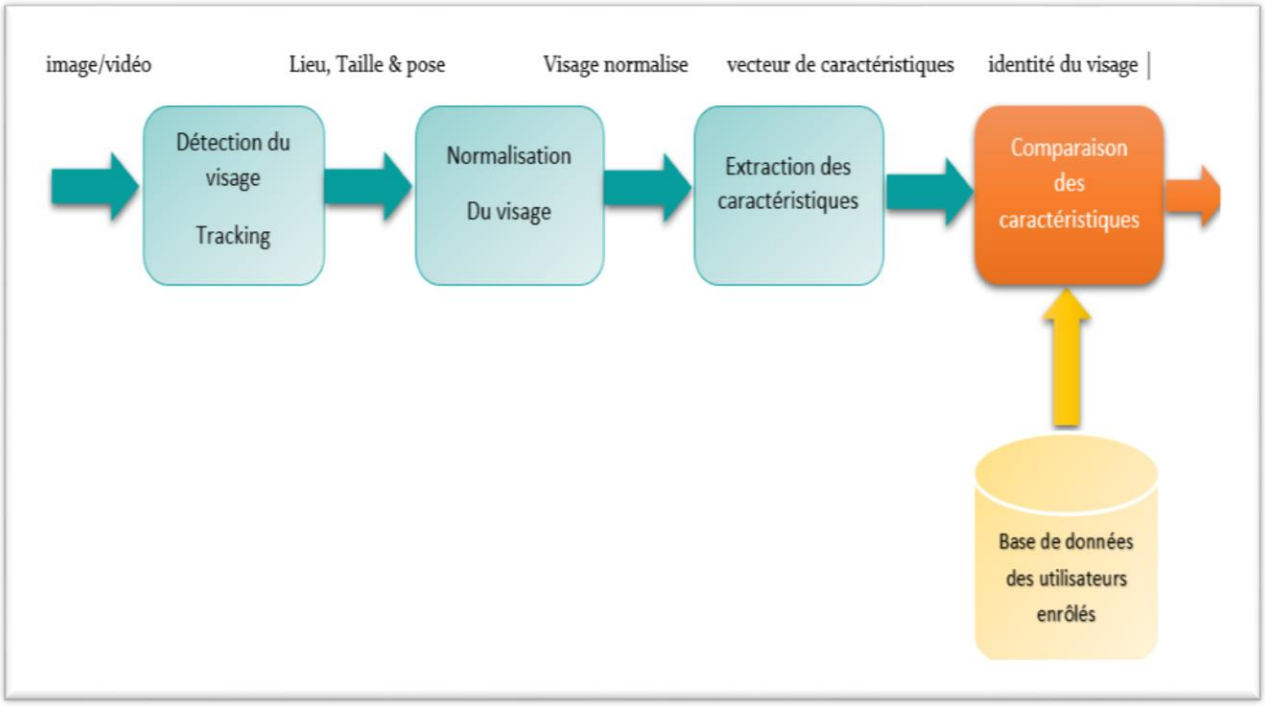

FIGURE 18 . PRINCIPE DE FONCTIONNEMENT DE BASE D'UN SYSTEME DE RECONNAISSANCE FACIALE.

4. Détection et acquisition de l'image :

Cette étape consiste à détecter et extraire l'image du monde physique (réel), elle permet d'avoir une représentation matricielle de l'image (matrice de niveau de gris), l'opération peut être statique ou dynamique selon le capteur utilisé.

4.1. Prétraitement :

Le rôle de cette étape est d'éliminer les parasites causés par la qualité des dispositifs optiques ou électroniques lors de l'acquisition de l'image d'entrée, dans le but de ne retenir que les informations de base et ainsi de préparer l'image pour l'étape suivante. C'est nécessaire car vous ne pouvez jamais obtenir une image sans bruit en raison de l'arrière-plan et de la lumière généralement inconnus. Il existe plusieurs types de traitement et d'amélioration de la qualité d'image, tels que : le lissage, l'équilibre et le filtre moyen. Cette étape peut également contenir la détection et la localisation du visage dans une image, notamment lorsque le décor est très complexe.

4.2. Normalisation

La normalisation assure l'homogénéité des données. Photo-normalisation est appliquée à une seule image. Bien que la normalisation s'applique à un ensemble d'images, nous supprimons la moyenne de cette composante de toutes les images pour chaque composante et la divisons par la dérivation standard.

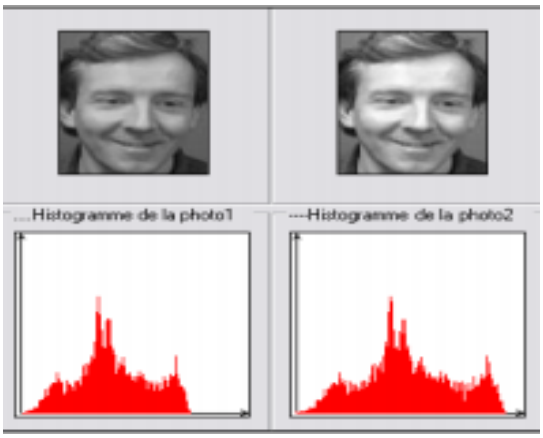

FIG : Normalisation d'une image

4.3. Égalisation d'histogramme :

Dans le traitement d'image, l'égalisation d'histogramme est une méthode de réglage du contraste d'une image numérique qui utilise des histogrammes. Elle consiste à appliquer une transformation à chaque pixel de l'image, obtenant ainsi une nouvelle image à partir d'une opération indépendante sur chaque pixel. Cette transformation est construite à partir de l'histogramme cumulatif de l'image de départ.

4.4. Filtrage

Afin d'améliorer la qualité visuelle de l'image, il est nécessaire d'éliminer les effets de bruit (parasites) en l'exposant à un traitement appelé filtrage. Le filtrage consiste à modifier la répartition fréquentielle des composantes du signal selon certaines spécifications. Ce filtre n'affecte pas les composantes basses fréquences des données d'image, mais doit atténuer les composantes hautes fréquences. Le lissage est souvent utilisé pour lisser le bruit et le bruit dans une image. Il peut être répété plusieurs fois, créant un effet flou. En pratique, il faut choisir un compromis entre la réduction du bruit et la préservation des détails et paramètres importants.

4.5. Extraction de paramètres

Outre la classification, l'étape d'extraction des paramètres est le cœur du système de reconnaissance, elle consiste à traiter l'image dans un autre espace de travail plus simple qui assure une meilleure exploitation des données, et permet ainsi l'utilisation de, uniquement, utiles, discriminants et non redondants informations

4.6. Apprentissage

C'est l'étape où les individus sont configurés pour apprendre le système, et elle consiste à conserver les paramètres, après extraction et classification, dans une base de données bien ordonnée pour faciliter l'étape de reconnaissance et de prise de décision, c'est en quelque sorte la mémoire du système.

4.7. La décision

C'est l'étape qui fait la différence entre un système d'identification des individus et un autre système de vérification. Dans cette étape, le système d'identification consiste à trouver le modèle qui correspond le mieux au visage pris en entrée de celui stocké dans la base de données, et se caractérise par son taux de reconnaissance.

En revanche, dans le système de vérification, il s'agit de déterminer si le visage saisi est bien le visage de l'individu déclaré (modèle) ou s'il s'agit d'une fraude, caractérisée par l'EER (Equal Error Rate)

5. Principales difficultés de la reconnaissance de visage

Pour le cerveau humain, la reconnaissance faciale est une tâche visuelle de haut niveau. Bien que les humains puissent détecter et identifier les visages dans une scène sans trop de difficulté, la construction d'un système automatisé qui accomplit de telles tâches est un défi de taille. Ce défi est d'autant plus grand que les conditions d'acquisition des images sont très variables.

Il existe deux variantes associées aux images faciales : un sujet intérieur et un sujet intérieur. La différence entre les sujets est limitée en raison de la similitude physique entre les individus. En revanche, la variation intra sujet est plus importante. Elle peut être attribuée à plusieurs facteurs. Chaque visage individuel peut créer une variété d'images différentes. Cette variété d'images faciales rend l'analyse difficile. Outre les différences générales entre les visages, les différences d'apparence des images faciales posent d'importants problèmes d'identification. Ces différences sont identifiées comme suit :

- Les changements d'éclairage affectent l'apparence du visage, même si la position du visage est fixe.

- les variations de position peuvent provoquer des changements drastiques dans les images.

- Les expressions faciales, un outil important dans la communication humaine, sont une autre source de différences dans les images. Seuls quelques traits faciaux directement liés à la structure osseuse du crâne, comme la distance entre les yeux ou la position générale des oreilles, sont fixés dans le visage. La plupart des autres caractéristiques peuvent changer leur configuration spatiale ou leur position en raison du mouvement de l'articulation de la mâchoire ou des muscles, comme le mouvement des sourcils, des lèvres ou le mouvement des joues.

- Le visage change à la longue en raison de l'âge, du changement de coiffure, ou en fonction du maquillage ou des accessoires. L'isolement et la description claire de toutes ces différentes sources de variation devraient être l'objectif ultime du système d'analyse faciale.

5.1. ILLuminance

L'apparence du visage dans l'image varie considérablement en fonction de l'éclairage de la scène au moment où l'image a été prise Les différences d'éclairage rendent la tâche de reconnaissance des visages très difficile. En fait, le changement d'apparence du visage dû à l'éclairage peut parfois être supérieur à la différence physique entre les individus et peut conduire à une mauvaise classification des images d'entrée. Ceci a été observé expérimentalement dans Adini et al où les auteurs ont utilisé une base de données de 25 individus.

La reconnaissance faciale en environnement non supervisé reste donc un domaine de recherche ouvert. Les évaluations FRVT ont révélé que la différence dans le problème de la lumière est un défi majeur pour la reconnaissance faciale.

FIGURE 19 . EXEMPLE DE VARIATION D'ECLAIRAGE.

5.2. Variation de la pose

Un changement de l'angle d'inclinaison du visage provoque plusieurs changements d'apparence dans le collage pour un placement stable du capteur. Ici, nous nous intéressons à la rotation du visage en profondeur comme les mouvements de geste ou de rejet.

En effet, l'étape initiale de normalisation des visages donnée au paragraphe vue précédemment permet de corriger toute rotation dans le plan image. Le taux de reconnaissance faciale chute considérablement lorsqu'il y a des différences de position dans les images. Cette difficulté a été démontrée par des tests d'évaluation développés sur les bases de données AR JAFFE ...etc. La rotation en profondeur obscurcit certaines parties du visage, comme pour les trois quarts des vues. D'autre part, ils entraînent des différences de profondeur, qui apparaissent sur le plan bidimensionnel de l'image, ce qui entraîne des distorsions qui modifient la forme générale du visage. Ces déformations se produisent dans le resserrement de certaines parties du visage et la compression d'autres zones.

Les distances entre les traits du visage varient également. Si la forme du visage interrogé diffère considérablement des visages enregistrés, les performances des systèmes de reconnaissance chutent considérablement. En effet, la rotation de la tête ne réduit pas significativement les taux de reconnaissance jusqu'à ±25°. Lorsque ce seuil est dépassé, il y a une baisse des performances. .Il s'avère que si le seul facteur de différence entre l'image enregistrée et l'image demandée est une rotation tête basse inférieure à 30°, alors les taux de reconnaissance des systèmes actuels sont de l'ordre de 90%. Une rotation plus importante entraîne une forte baisse des performances

Lorsque le visage est de profil dans le plan image (l'orientation est inférieure à 30°), il peut être normalisé en détectant au moins deux traits du visage (passant par les yeux). Cependant, lorsque la rotation est supérieure à 30°, la normalisation géométrique n'est plus possible.

FIGURE 20 . EXEMPLE DE VARIATION DE POSES. [W, 1]

5.3. Expressions faciales

Les visages ne sont pas des choses solides. L'expression faciale de l'émotion, ainsi que la parole, peuvent entraîner des changements importants dans l'apparence des visages.

Le nombre de configurations possibles est infini. Il est donc difficile d'évaluer l'effet des expressions faciales sur la reconnaissance. Étant donné que les expressions faciales affectent la géométrie et le positionnement des traits du visage, il est logique que les technologies universelles ou hybrides y soient plus puissantes que la plupart des technologies d'ingénierie.

On dit que les expressions faciales n'ont pas d'impact significatif sur les algorithmes de reconnaissance, tant qu'elles sont raisonnables. Alors que dans les cas extrêmes, il génère des déformations importantes de la bouche (comme des pleurs) et le rétrécissement ou la fermeture des yeux entraîne complètement une détérioration significative des performances de la reconnaissance automatique. Il peut être utile d'identifier ces expressions problématiques avant de les reconnaître. Si l'on est capable de classer les expressions faciales de la requête, il y a deux manières possibles. Plusieurs modèles faciaux ont été appris, un pour chaque catégorie d'expression faciale. Dans ce cas, il sera possible de comparer le profil du visage test avec une base de données de visages affichant la même expression. En revanche, avec une technique générative utilisant un modèle facial suffisamment précis, il sera possible de transformer le visage-test de manière à ce qu'il se présente dans des conditions moins difficiles et plus favorables.

La déformation du visage qui est due aux expressions faciales est localisée principalement sur la partie inférieure du visage. L'information faciale se situant dans la partie supérieure du visage reste quasi invariable. Elle est généralement suffisante pour effectuer une identification. Toutefois, étant donné que l'expression faciale modifie l'aspect du visage, elle entraîne forcément une diminution du taux de reconnaissance.

FIGURE 21 . EXEMPLE D'EXPRESSION FACIALE. [W, 1]

5.4. Présence ou absence des composants structurels

La présence de composants structuraux tels que la barbe, la moustache ou les lunettes peut modifier considérablement les caractéristiques faciales telles que la forme, la couleur ou la taille du visage. De plus, ces composants peuvent masquer les caractéristiques faciales de base, provoquant l'échec du système de reconnaissance. Par exemple, des verres opaques rendent difficile la distinction de la forme et de la couleur des yeux, et une moustache ou une barbe modifie la forme du visage.

FIGURE 22 . EXEMPLE SUR PRESENCE OU ABSENCE DES COMPOSANTS STRUCTURELS

5.5. Occultations partielles

Le visage peut être partiellement masqué par des objets présents dans la scène, ou par le port d'un accessoire comme des lunettes, un foulard, masque médicale etc.

Dans le cadre de la biométrie, les systèmes proposés doivent être non intrusifs, c'est-à-dire qu'il ne faut pas compter sur la collaboration active du sujet. Par conséquent, il est important de pouvoir reconnaître les visages partiellement masqués. Gross et al ont étudié l'effet du port de lunettes de soleil et d'un cache nez qui masque la partie inférieure du visage sur la reconnaissance faciale. Une demande est faite à la base de données AR. Les résultats expérimentaux semblent indiquer que dans ces conditions les performances des algorithmes de reconnaissance restent faibles.

FIGURE 23 . EXEMPLE OCCULTATIONS PARTIELLES

5.6. Vieillissement et le changement d'aspect

Les visages changent d'apparence avec le temps. Les changements concernent la tension des muscles, l'aspect de la peau (apparition de rides), le port de lunettes, éventuellement le maquillage ou la présence d'une frange masquant une partie du front.

Sur la base AR, où le délai entre les deux sessions de prises de vue est seulement de deux semaines, la baisse des taux de reconnaissance est estimée à 20%.les systèmes de reconnaissance ont réalisé plus de progrès pour gérer au mieux le délai de temps entre deux prises de vue. Les systèmes ont du mal à reconnaître ces dernières.

Cela provient certainement des changements dans les conditions de prises de vue, et non d'un vieillissement des visages. Dans le cadre de l'évaluation FRVT 2002, la baisse des taux de reconnaissance des meilleurs algorithmes testés a été estimée à 5% par année d'écart entre l'image de référence et l'image à reconnaître

FIGURE 24 . EXEMPLE DE VIEILLISSEMENT ET LE CHANGEMENT D'ASPECT

6. Méthodes de reconnaissances :

La performance des systèmes de reconnaissance faciale s'est significativement améliorée depuis les premiers travaux qui ont été menés dans les années 60-70 et de nombreux algorithmes de reconnaissance du visage ont été proposés depuis.

Certaines méthodes se basent sur une photographie (2D) du visage tandis que d'autres méthodes prennent en compte des informations 3D de celui-ci. On peut également noter qu'il existe d'autres méthodes (parfois appelées 2.5D) qui effectuent la reconnaissance du visage en se basant la plupart du temps sur l'information de profondeur.

Cependant, ces dernières méthodes peuvent demander un coup de déploiement élevé dû à l'investissement de scanners 3D coûteux.

Un autre inconvénient majeur concerne le grand volume de données tridimensionnelles qu'il est souvent nécessaire de convertir afin de pouvoir les traiter convenablement, ce qui implique une utilisation encore relativement inadaptée à des contraintes temps-réel, contrairement au traitement de photographies 2D.

Enfin, à notre connaissance, il n'existe pas de bases de données officielles 3D comprenant un nombre suffisamment élevé d'utilisateurs pour pouvoir évaluer le rapport entre la performance gagnée par l'utilisation d'une troisième dimension et les coûts supplémentaires en termes de ressources et de temps de calcul. Par conséquent, pour la partie concernant la reconnaissance faciale, nous privilégierons l'étude des méthodes 2D.

Les méthodes de reconnaissance faciales peuvent être séparées en trois grandes familles, les méthodes globales (ou holistiques), les méthodes locales et les méthodes hybride, basées sur des modèles.

Le choix a été fait de se concentrer sur ces trois types d'approches fondamentales et de n'aborder ni les réseaux neuronaux (plus adaptés à la détection des visages), ni les modèles cachés de Markov (plus utilisés en reconnaissance de la parole) car ces deux dernières techniques rencontrent des problèmes lorsque le nombre d'individus augmente (les calculs deviennent très importants).

De plus elles ne conviennent pas aux systèmes de reconnaissance basés sur une seule "image modèle" car de nombreuses images par personne sont nécessaires pour entraîner les systèmes afin de configurer leurs paramètres de façon optimale.

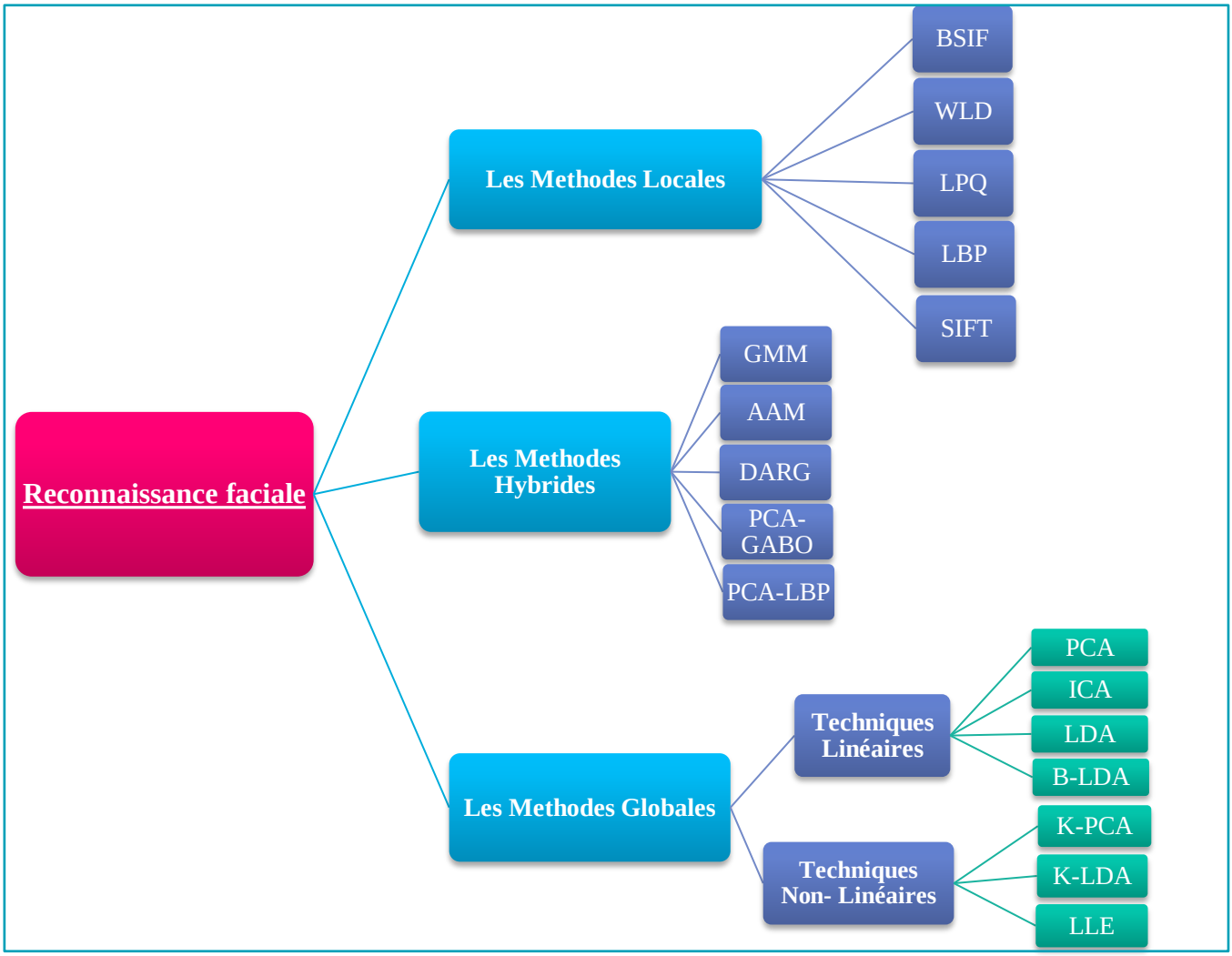

FIGURE 25 . SCHEMA DES METHODES DE RECONNAISSANCE FACIALE. [2]

6.1. Les Méthodes Globales

Le principe de ces approches est d'utiliser toute la surface du visage comme source d'information sans tenir compte des caractéristiques locales comme les yeux, la bouche, etc...L'une des méthodes la plus largement utilisée pour la représentation du visage dans son ensemble est l'ACP. Les algorithmes globaux s'appuient sur des propriétés statistiques bien connues et utilisent l'algèbre linéaire. Ils sont relativement rapides à mettre en œuvre, mais sont sensibles aux variations d'illumination, de pose et d'expression faciale. [2]

Parmi les approches les plus importantes réunies au sein de cette classe on trouve :

A. Techniques linéaires :

Les techniques linéaires réalisent une projection linéaire des visages (espace dont la dimension est égale à la dimension des images, donc grande) sur un espace de plus faible dimension.

Cependant, ces techniques linéaires sont sensibles aux conditions de luminosité notamment, et plus généralement aux variations non convexes. Ainsi, l'utilisation de distances classiques dans l'espace projeté ne permet pas toujours de réaliser une bonne classification entre les classes « visages » et « non visages ».

Et parmi les approches les plus importantes réunies au sein de cette méthode, citons :

a. L'Analyse Discriminante Linéaire (LDA ou Fisherfaces) :

LDA est une méthode d'analyse numérique qui permet de rechercher un ensemble linéaire de variables qui représente le mieux les données, et elle est largement utilisée dans le domaine de la reconnaissance de formes, c'est-à-dire la reconnaissance faciale introduite par Belhumeur et al en 1997.

LDA (souvent appelé Fisherfaces) consiste à diviser les visages en classes selon le critère de Fisher, puis à analyser les vecteurs propres de dispersion des données, pour maximiser les différences entre classes (images de différences individuelles différentes) (images d'un même individu), cette technique est une variante de l'ACP, par opposition à cette méthode où la meilleure représentation (qui augmente la variance) est recherchée, et le but ici est une meilleure séparation des classes.

D'autres techniques linéaires ont également été utilisées pour le calcul de vecteurs caractéristiques :

- l'analyse en composantes indépendantes **(ICA)**
- la factorisation de matrices non négatives **(NMF)**
- l'analyse discriminante bilinéaire **(BDA).**
- la technique dite de « Vecteurs communs discriminants » **(DCV).**

Bien que ces méthodes linéaires soient assez efficaces, elles manquent de précision dès que les images de visages subissent des transformations non linéaires. Une simple modification de la luminosité transforme celui–ci de façon non linéaire étant donné la complexité de la forme.

B. Techniques non linéaires :

Des techniques universelles non linéaires ont été développées, souvent à partir de techniques linéaires. Ainsi l'analyse en composantes de base (ou "kernel-PCA") et l'analyse discriminante linéaire du noyau (ou "kernel-LDA") utilisent le concept mathématique de noyau pour étendre les technologies linéaires que sont l'ACP et l'ADL.

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

- le MultiDimensional Scaling **(MDS)**
- les approches neuronales
- l'Isomap
- la diffusion maps

L'utilisation de ces méthodes de projection de l'espace des images sur l'espace de caractéristiques est non linéaire et permet ainsi dans une certaine mesure de réduire la dimension des images de meilleure façon.

6.2. Les Méthodes Locales :

Elles sont également appelées méthodes de caractéristiques, géométriques, localisées ou analytiques. Ce type consiste à appliquer des transformations à des endroits précis de l'image, souvent autour de points distincts (coins des yeux, bouche, nez, ...), le pouvoir sera donné aux petits détails locaux pour éviter le bruit des cheveux, lunettes, chapeaux, barbes, etc.

Mais la difficulté surgit lorsqu'il s'agit de prendre en compte plusieurs points de vue du visage ainsi que l'imprécision dans l'étape "d'extraction" des points qui sont le principal inconvénient. Plus précisément, ces méthodes extraient les caractéristiques faciales locales telles que les yeux, le nez et la bouche, puis utilisent leur géométrie et/ou leur apparence comme entrée du classificateur.

Deux pratiques différentes peuvent être distinguées :

- La première repose sur l'extraction de régions entières du visage, elle est souvent implémentée avec une approche globale de reconnaissance de visage.
- La deuxième pratique extrait des points particuliers des différentes régions caractéristiques du visage, tels que les coins des yeux, de la bouche et du nez.

Parmi ces approches on peut citer :

- Modèles de Markov Cachés (Hidden Markov Models (HMM)),
- L'Algorithme Elastic Bunch Graph Matching (EBGM),
- Eigen Object (EO),
- L'appariement de gabarits.

Parmi les approches de cette méthode, citons :

A. Les ondelettes (wavelet) :

La transformée en ondelettes a été introduite par Morlet au début des années 80, utilisées pour l'évaluation des données sismiques. Sous l'impulsion de personnalités scientifiques telles que le physicien A. Grossman ou le mathématicien Y. Meyer, les ondes se sont révélées être des outils essentiels pour l'analyse harmonique moderne et sont largement appliquées dans les domaines de l'ingénierie tels que le traitement du signal et de l'image où elles ont obtenu un grand succès dans des problèmes tels que l'estimation de mouvement, la reconnaissance de formes, la recherche de bases de données et la transmission progressive d'informations.

Domaine temporel temps et espace-fréquence utile dans le traitement numérique du signal et la compression d'images dans le traitement du signal, les ondelettes sont utiles pour récupérer les signaux faibles du bruit.

B. Machines à Vecteurs de Support (SVM) :

C'est une technique qui a été proposée par V.Vapnik en 1995, elle est utilisée dans plusieurs domaines statistiques (classement, régression, fusion,... etc.).

Depuis son introduction dans le domaine d'efficacité et principalement dans le traitement d'images. L'idée essentielle de cette approche consiste à projeter les données de l'espace d'entrée (appartenant à différentes classes) non linéairement séparables, dans un espace de plus grande dimension appelé espace de caractéristiques, de façon à ce que les données deviennent linéairement séparables

Dans cet espace, la technique de construction de l'hyperplan optimal est utilisée pour calculer la de classement séparant les classes tels que : Les vecteurs appartenant aux différentes classes se trouvent de différents côtés de l'hyper plan, et la plus petite distance entre les vecteurs et l'hyperplan (la marge) soit maximale.

6.3. Méthodes hybrides :

Les méthodes hybrides combinent les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométriques (ou structurelles) et l'extraction de caractéristiques d'apparence locales.

Elles permettent d'augmenter la stabilité des performances de reconnaissance lors des changements de position, d'éclairage et d'expressions faciales. Les méthodes les plus connues sont basées sur des modèles statistiques dont le modèle d'apparence active.

Parmi les approches de cette méthode, citons :

- LogGabor PCA présenté par Perlibakas.

Une convolution par des ondelettes de Gabor orientées s'effectue autour de certains points caractéristiques du visage. Les vecteurs ainsi créés contiennent à la fois la localisation ainsi que les amplitudes des énergies locales. Une analyse en composantes principales est ensuite réalisée afin de réduire la dimension de ces vecteurs.

A. Les Modèles Actifs d'Apparence (Active Appareance Models ou AAM) :

Une méthode proposée par Cootes et ses collègues qui modélisent indépendamment la forme et la texture du visage en appliquant une analyse en composantes principales. Les vecteurs de forme et de texture obtenus sont ensuite utilisés pour les identifier. Le nouveau visage à sélectionner est superposé au modèle par un processus d'optimisation itératif. Ensuite, les paramètres de forme et de texture obtenus sont comparés à ceux de la base.

Le tableau si dessous récapitule qualitativement la différence entre les deux types de caractéristiques locale et globale.

Tableau 8 . **Comparaison entre les caractéristiques locales et globales**

Facteurs de variations	Caractéristiques locales	Caractéristiques globales
• Illuminations	Très sensible	Sensible
• Pose	Sensible	Très sensible
• Expressions	Pas sensible	Sensible
• Bruit	Très sensible	Sensible
• Occlusion	Pas sensible	Très sensible

7. Conclusion

Dans ce chapitre, nous avons présenté la technologie de pointe dans l'exploitation d'un système de reconnaissance automatique des visages, les difficultés telles que la capture d'illumination, la pose, l'orientation du visage et les expressions faciales. Etc., puis nous avons vu les principales méthodes utilisées dans la littérature pour la reconnaissance (méthodes globales, locales et hybrides).

Dans le chapitre suivant nous verrons le schéma, la méthode que nous avons proposés et l'outil utilisé.

Chapitre 3

Contribution

Introduction

Dans ce chapitre nous présentons le schéma du système proposé ainsi que les expériences que nous avons menées au cours de notre étude et la comparaison entre les résultats expérimentaux sur l'ILLuminance et la réflectance et la fusion entre eux pour la reconnaissance faciale des individus.

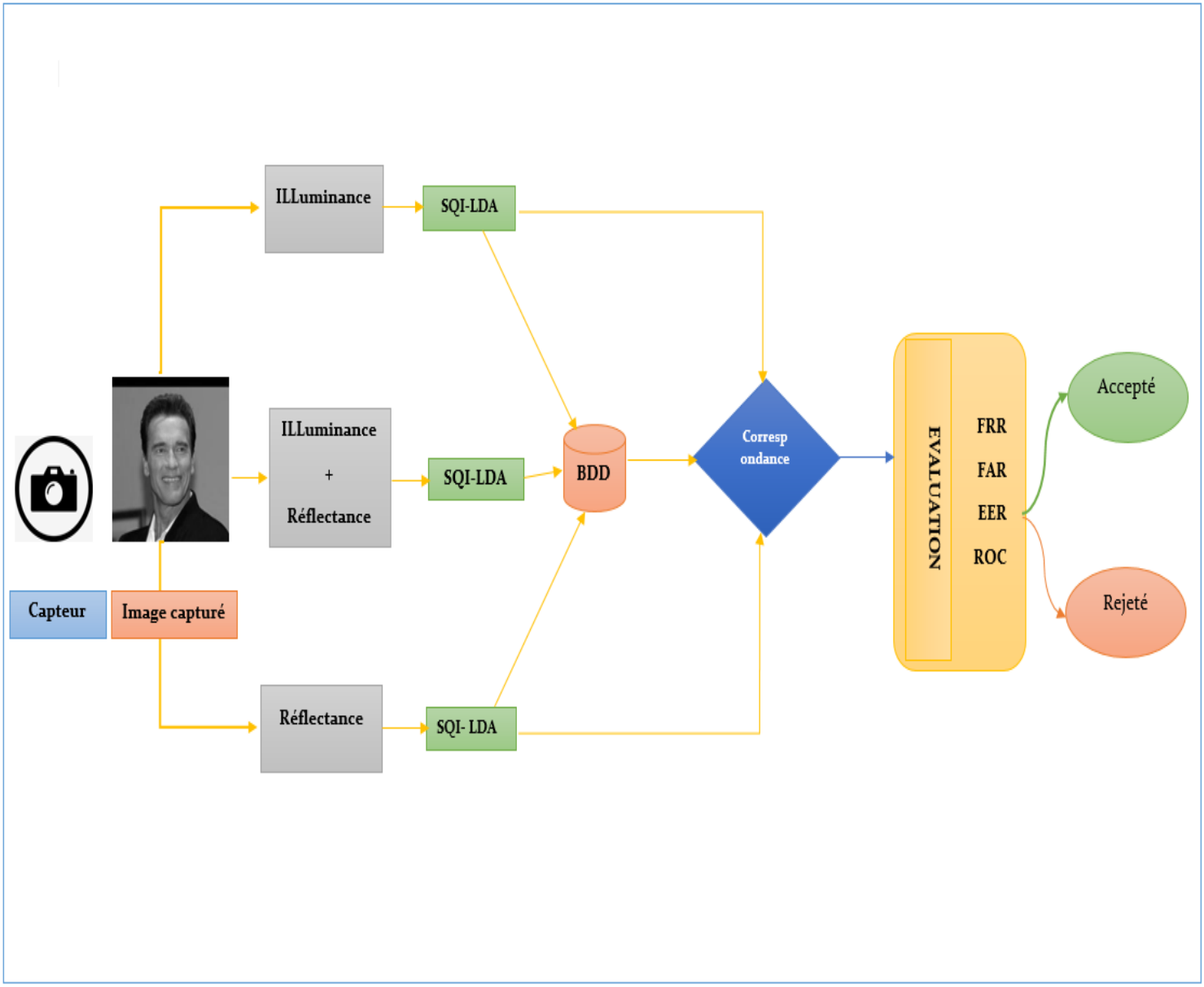

FIGURE 26 . SCHEMA FONCTIONNELLE PROPOSE DU SYSTEME DE RECONNAISSANCE UTILISANT LE VISAGE AVEC UNE FUSION AU NIVEAU D'ILLUMINANCE ET DE REFLECTANCE.

PARTIE 01

1. Méthode proposé l'algorithme SQI :

Image auto-quotient (SQI), pour une reconnaissance faciale robuste dans diverses conditions d'éclairage. Les propriétés invariantes et variantes d'illumination de l'algorithme d'auto-quotient sont analysées selon le modèle lambertien. Bien que SQI ait une forme similaire à QI, il n'a besoin que d'une seule image de visage pour la mise en œuvre et aucun alignement dans la procédure SQI n'est nécessaire.

Cet algorithme a une capacité spéciale de désombrage. Les résultats de l'expérience montrent que la méthode SQI peut améliorer considérablement le taux de reconnaissance des images de visage dans différentes conditions d'éclairage (ILLuminance et réflectance)

Le système proposé comprend une étape avant l'extraction des caractéristiques. C'est l'étape de traitement sur l'image capturée afin de modifie L'illumination et la réflectance.

DESCRIPTION GÉNÉRALE

La fonction effectue une normalisation photométrique de l'image X en utilisant la technique d'image à quotient propre. Même si dans l'article original la technique est proposée pour être implémentée avec plusieurs échelles (similaire à la technique des rétines multi-échelles), cette implémentation ne supporte qu'une seule échelle. L'image de quotient propre à plusieurs échelles est implémentée dans une fonction distincte. La fonction est destinée à être utilisée dans des expériences de reconnaissance faciale et les paramètres par défaut sont définis de manière à obtenir une "bonne" normalisation pour les images de taille 128 x 128 pixels. Bien sûr, le terme "bon" est relatif.

1.1. La Technique LDA

LDA est utilisé pour réduire les dimensions de ces vecteurs de caractéristiques

1.2. Enrôlement

L'enrôlement est l'enregistrement de données biométriques déjà extraites dans une base de données, c'est-à-dire la phase de création de références afin qu'elles puissent ensuite être utilisées pour l'identification et l'authentification.

1.3. Correspondance et évaluation

C'est une comparaison entre toutes les caractéristiques extraites avec le modèle enregistré dans la base de données du système afin de déterminer le degré de similitude ou de divergence entre les deux

1.4. Décision

En fonction de la phase d'appariement et d'évaluation, le système prend la décision d'accepter ou de rejeter l'individu

1.5. Base de données

Pour l'évaluation de notre système proposé nous avons 3 bases de données d'images accessibles au public ces bases de données AR, JAFFE et 15YALE contiennes respectivement 2600, 210 et 165 images avec de différents extension.

1.6. Architecture de système proposé

Le système de reconnaissance personnelle utilisant le visage au niveau de l'extraction des caractéristiques est illustré par la figure 38 qui représente le schéma fonctionnel de la reconnaissance faciale proposé.

PARTIE 02

Outil de développement

Lors de développement de notre système nous avons eu recours à Matlab 9.9.0 (R2020b) que nous présenterons ci-dessous.

1. MATLAB 9.9.0 (R2020b)

Matlab et son environnement interactif est un langage de haut niveau qui permet la mise en œuvre des tâches nécessitant une puissance de calcul importante et qui sera beaucoup plus simple et rapide à mettre en œuvre que les langages de programmation traditionnels tels que C et C++.

Il dispose de nombreuses boîtes à outils et bibliothèques, notamment celles de « Image Processing ToolBox » qui propose un ensemble d'algorithmes et d'outils de dessin de référence pour le traitement, l'analyse, la visualisation et le développement d'algorithmes de traitement d'images.

La boîte à outils de reconnaissance faciale PhD (Pretty Helpful Development functions for) est un ensemble de fonctions et de scripts Matlab destinés à aider les chercheurs travaillant dans le domaine de la reconnaissance faciale.

La boîte à outils PhD propose des implémentations de plusieurs techniques de reconnaissance faciale populaires, telles que l'analyse en composantes principales, l'analyse discriminante linéaire, l'analyse en composantes principales du noyau ou l'analyse du pêcheur du noyau. En plus de ces techniques. Une partie importante de la boîte à outils sont également les outils d'évaluation qui permettent la construction des courbes de performance les plus courantes (par exemple, ROC, CMC) utilisées pour évaluer les systèmes de reconnaissance faciale.

2. Résultat et discussion :

Cette partie d'expérience détermine les résultats obtenus par l'application du block Overlap ratios sur les différentes bases de données AR, JAFFE et 15 Yale respectivement afin de bien définir les meilleurs scores de reconnaissance faciale.

Résultat BDD AR :

TABLEAU 9 . RESULTAT DE LA BASE DE DONNEES AR

	REFLECTANCE				ILLUMINANCE				REFLECTANCE + ILLUMINANCE			
Block Overlap Ratio (RA)%	Identification RANK-1%	EER%	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%	Identification RANK-1%	EER %	Vérification VR@1 % FAR%	Vérification VR@0,1 % FAR%	Identification RANK-1%	EER%	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%
0.5	98,60	0,66	99,40	99,00	**98,80**	**0,66**	**99,40**	**99,00**	**96.20**	**0.80**	**99.40**	**96.00**
0.75	**99,00**	**0,44**	**99,40**	**99,00**	**98,80**	**0,66**	**99,40**	**99,00**	96.00	0.80	99.20	95.80
1	99,00	0,60	99,40	99,00	86.80	2.22	95.40	81.20	95.80	0.80	99.20	96.40
1.25	98,80	0,66	99,40	99,00	87.20	2.75	94.40	82.20	95.80	0.80	99.20	96.20

Le tableau présente la comparaison entre les quatre valeurs du block Overlap ratio (RA)% appliqué sur la base de données AR pour définir les meilleurs scores d'ILLuminance, de la réflectance et d'ILLuminance & réflectance ensemble proposées au niveau de la modalité visage

Le tableau ci-dessus montre que les meilleurs résultats obtenus sont ceux des valeurs 0,5 et 0.75.

Réflectance : RANK=99.00%, EER=0.44.

ILLuminance : RANK=98.00%, EER=0.66.

Réflectance + ILLuminance : RANK=96.00%, EER=0.80, VR@1% FAR%=99.00.

Les Courbe CMC et ROC de la BDD AR :

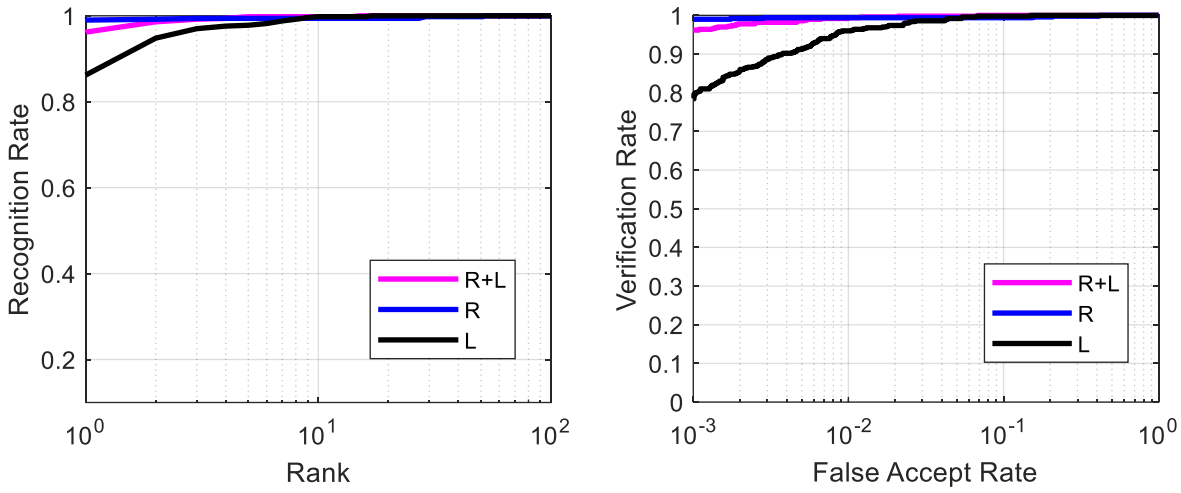

FIGURE 27 . PLOT BDD AR (CMC ET ROC 0.5)

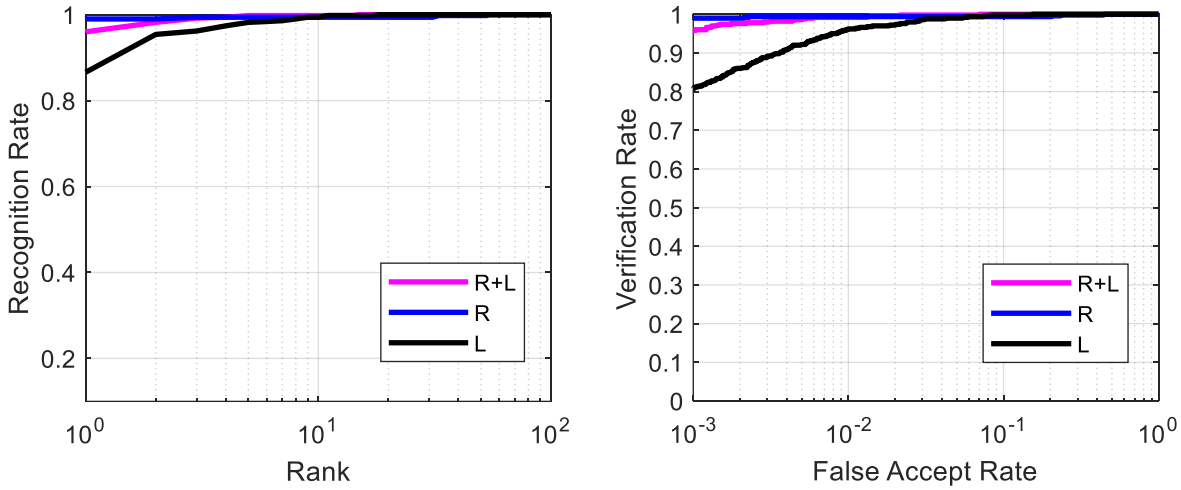

FIGURE 28 . PLOT BDD AR (CMC & ROC 0.75)

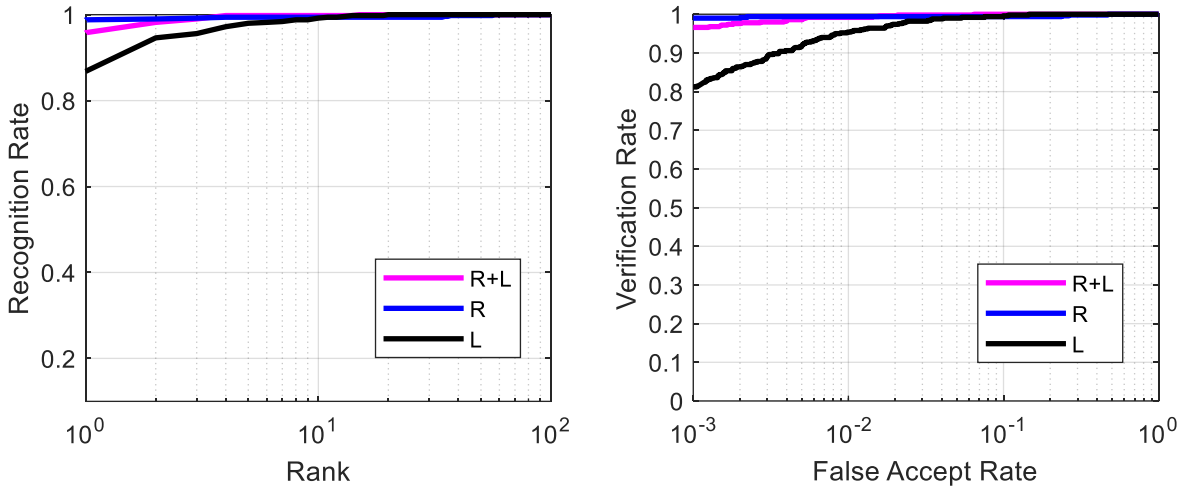

FIGURE 29 . PLOT BDD AR (CMC & ROC 01)

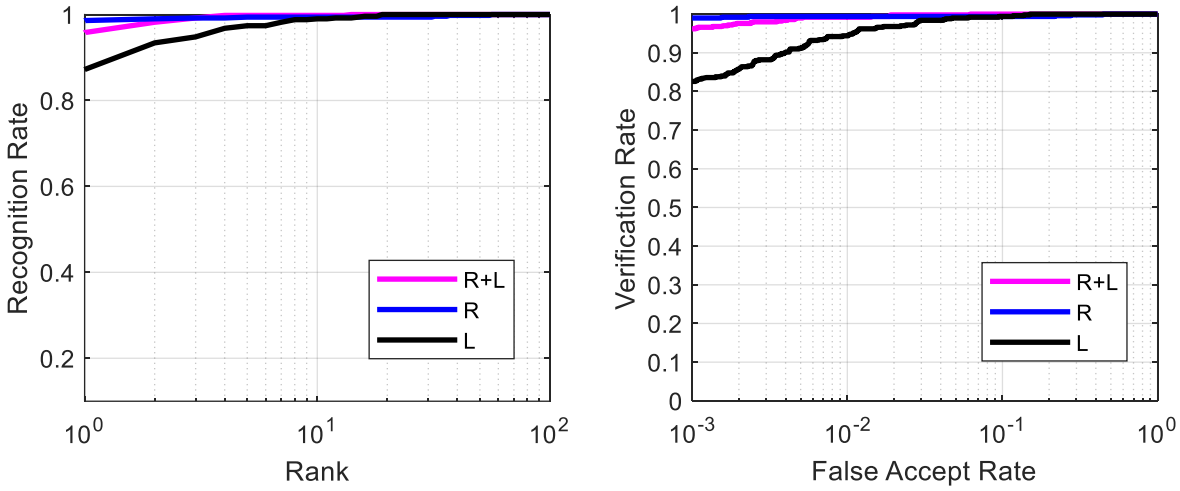

FIGURE 30 . PLOT BDD AR (CMC & ROC 1.25)

Résultat de la BDD JAFFE

TABLEAU 10 . RESULTAT DE LA BASE DE DONNEES JAFFE

	REFLECTANCE				ILLUMINANCE				REFLECTANCE + ILLUMINANCE			
Block Overlap Ratio (RA)%	Identification RANK-1%	EER %	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%	Identification RANK-1%	EER %	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%	Identification RANK-1%	EER %	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%
0.5	**84.00**	**6.33**	**80.00**	**2.00**	94.00	2.00	92.00	2.00	**86.00**	**6.00**	**72.00**	**2.00**
0.75	84.00	7.56	80.00	2.00	94.00	2.00	92.00	2.00	**86.00**	**6.00**	**72.00**	**2.00**
1	84.00	7.78	80.00	2.00	94.00	2.00	92.00	2.00	**86.00**	**6.00**	**72.00**	**2.00**
1.25	84.00	7.78	80.00	2.00	**94.00**	**2.00**	**96.00**	**2.00**	**86.00**	**6.00**	**72.00**	**2.00**

Le tableau présente la comparaison entre les quatre valeurs du block Overlap ratio (RA)% appliqué sur la base de données JAFFE pour définir les meilleurs scores d'ILLuminance, de la réflectance et d'ILLuminance & réflectance ensemble proposées au niveau de la modalité visage

Le tableau ci-dessus montre que les meilleurs résultats

Pour la réflectance sont ceux de 0.5, ILLuminance de 1.25 contrairement à l'ensemble réflectance et ILLuminance les résultats sont les mêmes pour les différentes valeurs d'Overlap.

LES courbes CMC et ROC de la BDD JAFFE

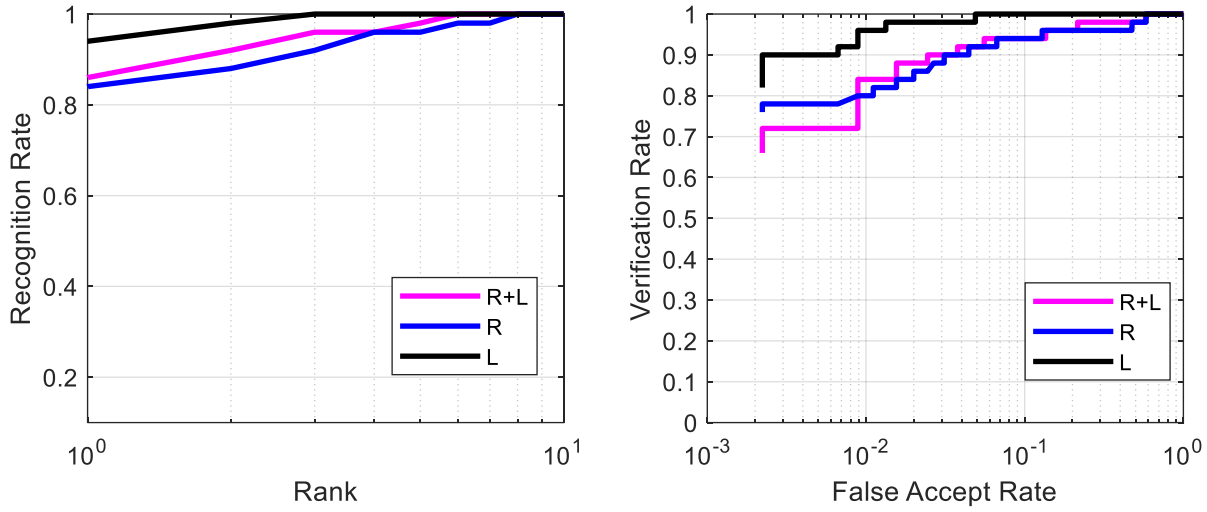

FIGURE 31 . PLOT BDD JAFFE (CMC & ROC 0.5)

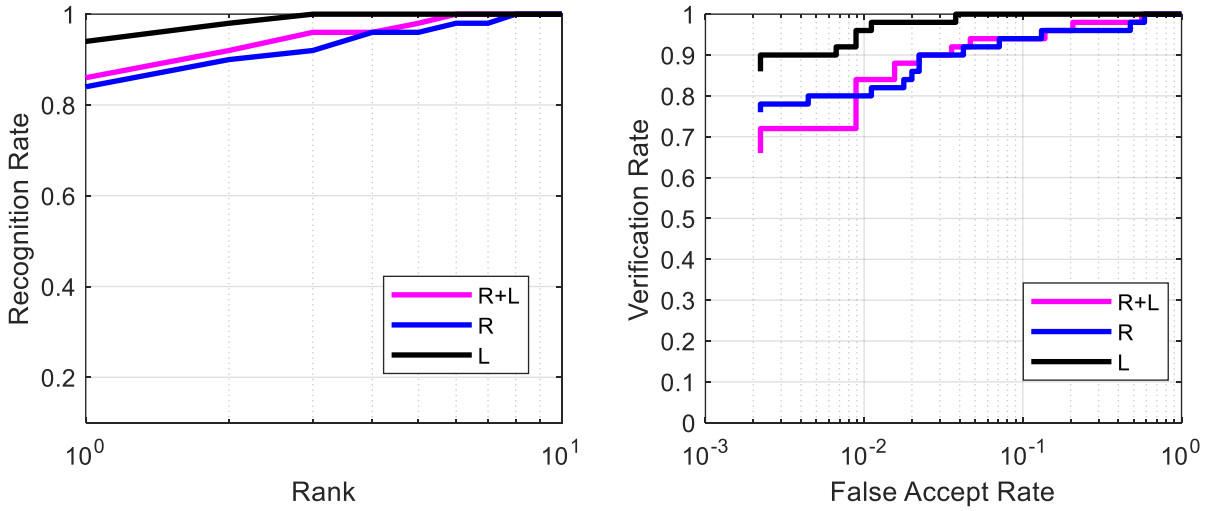

FIGURE 32 . PLOT BDD JAFFE (CMC & ROC 0.75)

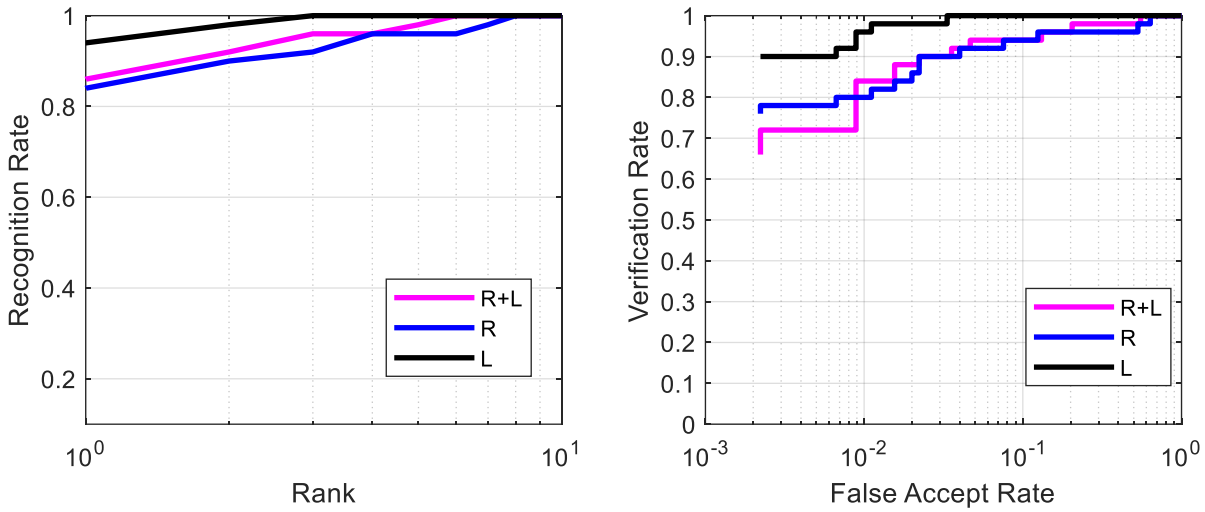

FIGURE 33 . PLOT BDD JAFFE (CMC & ROC 01)

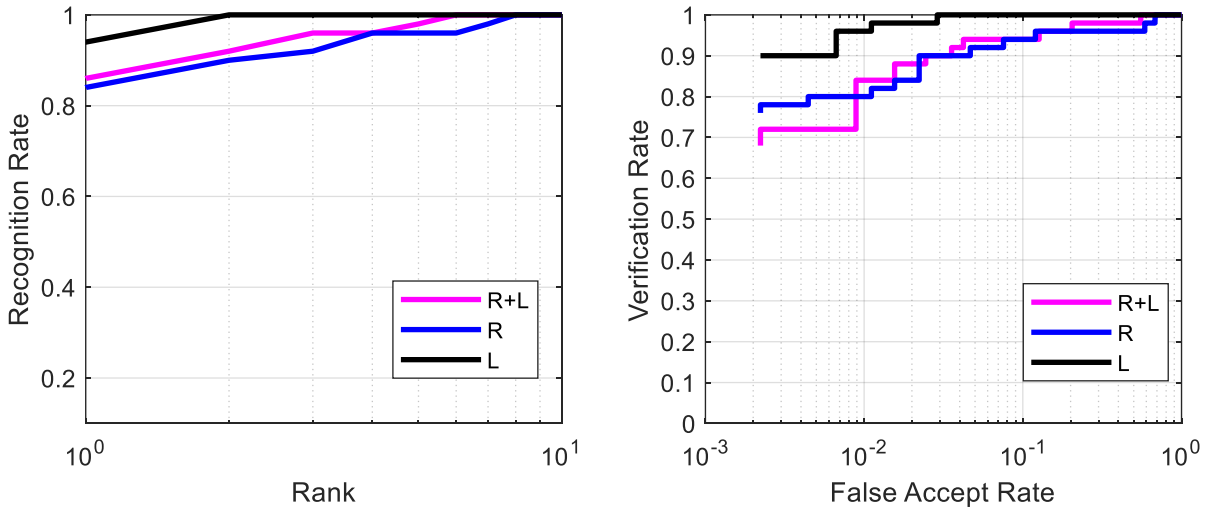

FIGURE 34 . PLOT BDD JAFFE (CMC & ROC 1.25)

Résultat de la BDD15 YALE :

TABLEAU 11 . RESULTAT DE LA BASE DE DONNEES 15 YALE

	REFLECTANCE				ILLUMINANCE				REFLECTANCE + ILLUMINANCE			
Block Overlap Ratio (RA)%	Identification RANK-1%	EER %	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%	Identification RANK-1%	EER %	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%	Identification RANK-1%	EER %	Vérification VR@1% FAR%	Vérification VR@0,1% FAR%
0.5	98.67	1.19	98.67	96.00	93.33	1.33	96.00	76.00	97.33	0.24	100	90.67
0.75	98.67	1.19	98.67	96.00	93.33	1.33	96.00	76.00	97.33	0.19	100	92.00
1	98.67	1.14	98.67	96.00	93.33	1.33	96.00	78.67	97.33	0.19	100	94.67
1.25	**98.67**	**1.10**	**100**	**96.00**	**93.33**	**1.33**	**97.33**	**78.67**	**97.33**	**0.19**	**100**	**94.67**

Pour la base de données 15 YALE les résultats obtenus démontrent que les meilleurs scores sont de 1.25 d'Overlap.

Les Courbes ROC et CMC de la base de données 15YALE :

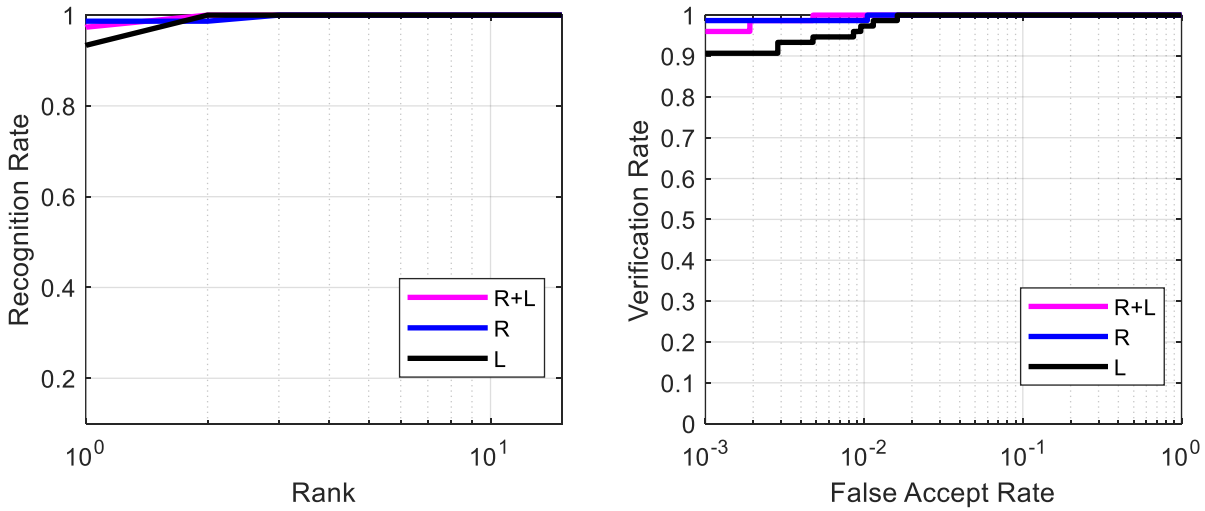

FIGURE 35 . PLOT BDD 15YALE (CMC & ROC 0.5)

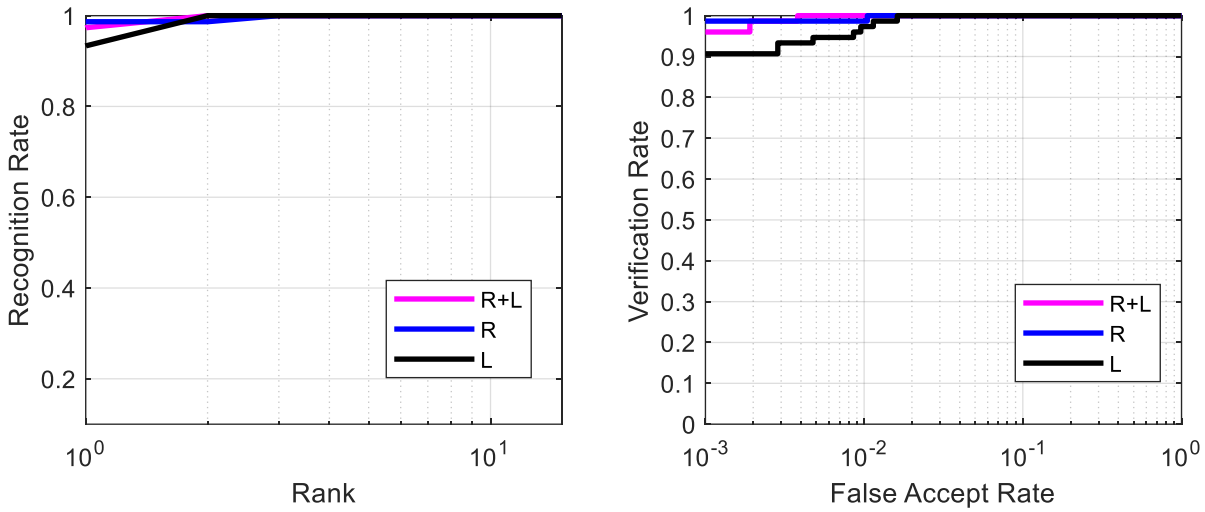

FIGURE 36 . PLOT BDD 15YALE (CMC & ROC 0.75)

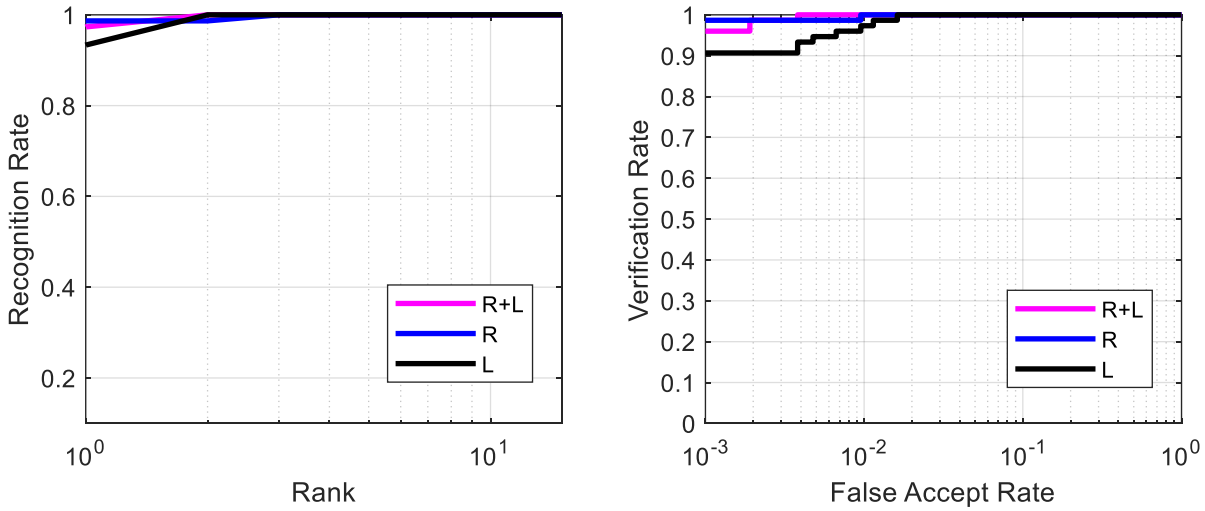

FIGURE 37 . PLOT BDD 15YALE (CMC & ROC 01)

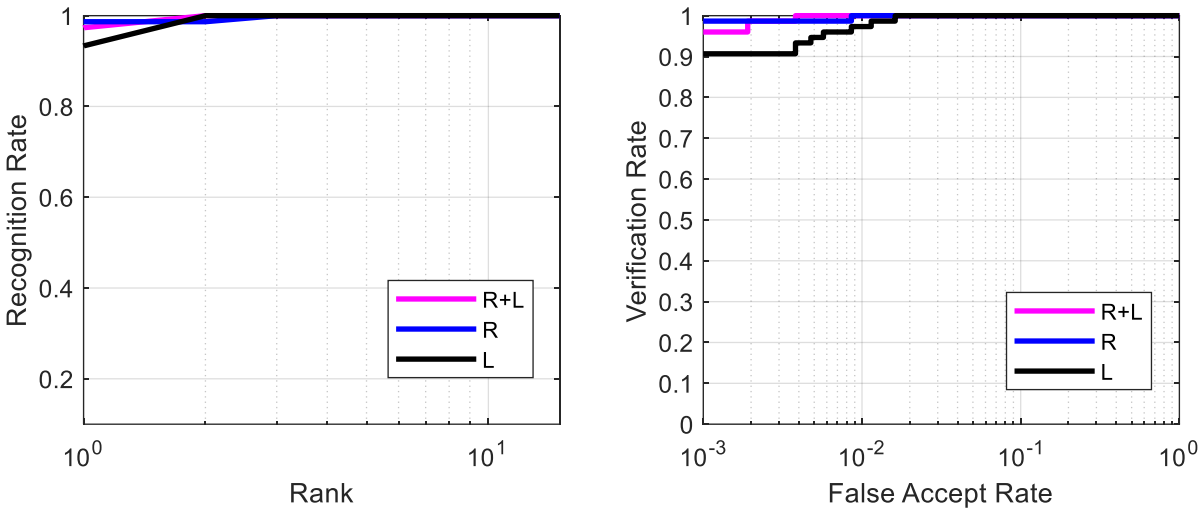

FIGURE 38 . PLOT BDD 15YALE (CMC & ROC 1.25)

3. Conclusion :

Dans ce chapitre nous concluons que notre système d'identification biométrique des personnes est fiable vu les résultats obtenus comme satisfaisants il permet une bonne séparabilité. Nous avons étudié l'influence d'illumination et la réflectance qui nous a donné de bons résultats.

L'ensemble des tests effectues a permis de conclure qu'avec l'utilisation de la fusion d'ILLuminance et réflectance nous a apporté une amélioration considérable du RANK1 et du EER et des deux erreurs FAR 1% et FAR 0.1%.

Conclusion Générale

La biométrie est une science à la fois passionnante et rigoureuse qui étudie les méthodes d'authentification des individus, ou encore de chiffrement basé sur la reconnaissance automatique des caractéristiques physiologiques et comportementales d'un individu.

La reconnaissance faciale est une technologie biométrique très populaire, qui est importante pour authentifier un individu. Elle est largement utilisée dans les applications de contrôle d'accès. Dans la littérature, il existe plusieurs méthodes globales, locales et hybrides de reconnaissance faciale.

Les essais ont montré aussi que l'algorithme de SQI ne nécessite pas une très longue période d'entraînement. Ces tests ont été réalisés sur les bases de données AR, JAFFE et 15 YALE en respectant la condition suivante : la prise de différentes poses pour chaque personne pendant la phase d'apprentissage. La discrimination représente la dernière étape de la reconnaissance. Les résultats que nous avons obtenus sont très encourageants.

Dans notre système de reconnaissance faciale, nous avons effectué nous tests dans le but d'améliorer et d'évoluer les performances de notre système dans ces deux modes (identification et vérification) en concluant la, FAR. FRR et RATIO Overlap , les tests expérimentaux effectués sur les bases de données les plus pertinente pour le système de reconnaissance de visages, ces tests nous ont permis de constater que la FUSION entre ILLuminance et la réflectance donne de meilleurs résultats. Et que l'algorithme de SQI ne nécessite pas une très longue période d'entraînement. Ces tests ont été réalisés sur les bases de données AR, JAFFE et 15 YALE en respectant la condition suivante : la prise de différentes poses pour chaque personne pendant la phase d'apprentissage. La discrimination représente la dernière étape de la reconnaissance. Les résultats que nous avons obtenus sont très encourageants.

A travers ce projet nous avons assimilé plusieurs informations concernant l'architecture des systèmes de reconnaissance biométrique et leur fonctionnement, on a également élargi nos connaissances relatives à l'outil Matlab.

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

- ♣ De faire plusieurs tests en utilisant d'autres bases de données virtuelles ou réelles.
- ♣ Utiliser d'autres prétraitements dans le but d'améliorer les qualités des images.
- ♣ Tester les fusions a d'autres niveaux que le score.
- ♣ Utiliser plusieurs méthodes de normalisation.
- ♣ Faire varier les seuils pour essayer d'obtenir de résultats.

Bibliographie

Les sites web

[W, 1] https://datascientest.com/convolutional-neural-network 25 juin 2020, consulté le 14 avril 2022, 21:38

[W, 2] https://www.kdnuggets.com/2018/05/general-approaches-machine learningprocess.html mai 2015, consulté le 14 avril 2022, 14:03

[W, 3] http://yann.lecun.com/exdb/lenet/ (consulté le19 avril 2022 a 10 :58)

[W, 4] https://datascientest.com/convolutional-neural-network 25 juin 2022 (consulté le 7 mai 2022 a 19 :38)

https://abgi-france.com/methodes-biometriques-d-identification-reconnaissance-faciale-et-digitale/ (consulté le 7 mai 2022 à 19 :50)

https://www.electronicid.eu/fr/blog/post/reconnaissance-faciale/fr Reconnaissance faciale : les 7 tendances de 2021 | Thales (consulté le 7 mai 2022 à 20 :12)

[1]H. Bredin "Vérification biométrique d'identité basée sur les visages parlants. Apport de la mesure de synchronie audiovisuelle face aux tentatives d'imposture élaborées." Juin 2007

[2]Gonzalez, Rafael C « Digital image Processing » volume 2 1987. [A. BETTAHAR, F. SABER, mémoire fin d'étude, thème Extraction des caractéristiques pour l'analyse biométrique d'un visage, OUARGLA 2014

[3]Ahonen, A. Hadid, and M. Pietikainen. Face recognition with local binary patterns. In ECCV, pages 469_481, 2004.

[4]M. LEMMOUCHI, mémoire fin d'étude, thème Identification des Visages Humains par Réseaux de Neurones, Université de Batna, Juin 2013.

[5]R. Beveridge, M. Kirby, Biometrics and Face Recognition, IS&T Colloquium, p.25, 2005.

[6] M. A. Turk and A. P. Pentland, "Face recognition using Eigenfaces", IEEE Conference on Computer Vision and Pattern Recognition, p. 586-590, Hawai, 1992.

[7]I. Buciu, I. Pitas, "Application of non-negative and local non negative matrix factorization to facial expression recognition", International Conference on Pattern Recognition, p. 288-291, 2004.

[8]Y. Wang, Y. Jia, C. Hu, M. Turk, "Non-negative matrix factorization framework for face recognition",

Internation Journal of Pattern Recognition and Artificial Intelligence, vol.19, no. 4, p. 495-511, 2005.

[9]M. Visani, C. Garcia, J. M. Jolion, "Normalized radial basis function networks and bilinear discriminant analysis for face recognition", IEEE Conference on Advanced Video and Signal Based Surveillance, p. 342-347, 2005.

[10]H. Cevikalp, M. Neamtu, M. Wilkes, A. Barkana, "Discriminative common vectors for face recognition", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, n1 , p. 4-13, 2005

[11] Ngoc_ Son _VU _thèse _ Contributions à la reconnaissance de visages à partir d'une seule image et dans un contexte non-contrôlé_ 2010