REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOHAMED BOUDIAF - M'SILA
FACULTE DES MATHEMATIQUES ET DE L'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Informatique Décisionnelle et Optimisation

Par : GASMI Lynda

SUJET

Deep Learning for face Recognition

Soutenu publiquement le : / /2020 devant le jury composé de :

Nom et prénom Enseignant		
……	**Université de M'sila**	**Président**
Dr. AKHROUF Samir	**Université de M'sila**	**Rapporteur**
……	**Université de M'sila**	**Examinateur**

Promotion : 2019/2020

Remerciements

Remercier est d'autant plus facile que l'on est conscient de ne pas être arrivé là tout seul. Derrière le succès de tout étudiant se pressent une foule de gens qui ont contribué à sa réussite. Je tiens tout d'abord à remercier en premier lieu Dieu le tout-puissant pour nous avoir donné la santé, le courage et la bonne volonté pour réaliser ce modeste travail.

En second lieu, je voudrais adresser toute ma reconnaissance à mon encadreur ***Docteur AKHROUF Samir****, pour sa patience, sa disponibilité et ses judicieux conseils, qui ont contribué à alimenter ma réflexion.*

Je souhaiterais exprimer ma gratitude et reconnaissance au ***Docteur ATTIA Abdelouahed****, pour avoir suivi de près mon travail, ses précieux conseils et orientations m'ont été très bénéfiques. Je le remercie sincèrement de m'avoir permis d'évoluer dans le monde de la biométrie et du Deep Learning pour le traitement d'images appliquée à la biométrie. Je le remercie également pour sa patience et ses qualités scientifiques.*

Je tiens également à exprimer toute ma reconnaissance envers les membres du jury de ma soutenance de master 2. Merci à docteur ...d'avoir accepté le rôle du jury de ce travail. Je remercie également docteur ...accepté d'être examinateur.

Mes plus profonds remerciements vont à mes parents pour leurs présences et leur accompagnement pendant tout mon parcours et dans les moments de doute. Tout au long de mon cursus, ils m'ont toujours soutenue et encouragé dans la poursuite de mes études. Ils ont su me donner toutes les chances pour réussir. Ils m'ont donné le goût de la connaissance. Qu'ils trouvent, dans la réalisation de ce travail, l'aboutissement de leurs efforts ainsi que l'expression de ma plus affectueuse gratitude. Je leur exprime ici toute ma gratitude de m'avoir toujours écoutée et même souvent relue avec la plus grande attention et m'apporter chaque jour tant et plus. Un grand merci à mon mari Nasreddine sur lequel j'ai toujours pu compter et grâce à sa solidarité j'ai pu poursuivre de longues études. Son courage et endurance pour réussir dans la vie m'ont beaucoup inspiré.

Je remercie sincèrement tous les enseignants qui ont contribué de loin ou de près à ma formation du primaire au supérieur.

Je terminerai en dédiant ce mémoire à tous mes amis aux caractères merveilleux, plein de joie et dont les sourires sont aussi agréables que communicatifs.

Dédicaces

À mes chers parents,

À mes frères,

À ma sœur,

À mon mari,

À mon fils et ma fille,

À ma belle -famille,

À tous mes amis et camarades,

À tous les étudiants de la promotion 2019/ 2020,

À tous ceux qui, par un mot, m'ont donné la force de continuer….

Table des matières

Chapitre 3 : Le Deep learning

Chapitre 4 : Résultats expérimentaux

Liste des Figures

Liste des tableaux

Abréviation

2D : Deux **D**imensions

3D : Trois **D**imensions

ACP : **A**nalyse en **C**omposantes **P**rincipales

ADN : Acide **D**ésoxyribo **N**ucléique

AE: **A**uto **E**ncoders

CNN: **C**onvolutional **N**eural **N**etworks

DL: **D**eep **L**earning

DNN: **D**eep **N**eural **N**etworks

ERR: Equal **E**rror **R**ate

FAR: False **A**cceptance Rate

FERET: Fac e Recognition **T**echnology

FRR: False **R**ejection **R**ate

GAN: **G**enerative **A**dversarial **N**etworks

GPU *:* **G**raphics **P**rocessing **U**nit)

IA : **I**ntelligence **A**rtificielle

IBG: International **B**iometric **G**roup

LDA: **A**nalyse **D**iscriminante **L**inéaire

ML: **M**achine **L**earning

ORL: Olivetti **R**esearch **L**aboratory

PhD: Pretty **H**elpful **D**evelopment

PIN: Personal **I**dentification **N**umber

ROC : Receiver **O**perating **C**haracteristic

RN : **R**éseaux de **N**eurones

RNA : **R**éseaux de **N**eurones **A**rtificiels

RNN : **R**ecurrent **N**eural **N**etworks

SAE-DNN: **S**tacked **A**uto**E**ncoder - **D**eep **N**eural **N**etwork

SVM : Machine à **V**ecteurs de **S**upport

INTRODUCTION GENERALE

De nos jours on parle de plus en plus de l'insécurité dans divers secteurs, de l'augmentation du taux de criminalité, du piratage …etc. Par ailleurs, le développement des communications tant en volume qu'en diversité (déplacements des individus, transactions financières, accès aux services...) nécessite un besoin pressant pour s'assurer de l'identité des individus.

Les systèmes traditionnels de sécurité sont basés sur une connaissance a priori "knowledgebased" (code PIN, mot de passe...) ou sur une possession d'un objet "token-based" (clef, pièce d'identité, badge...). Cependant, ces systèmes sont moins fiables pour beaucoup d'environnement, à cause de leur inhabilité commune à distinguer un individu réellement autorisé d'un fraudeur. Plusieurs méthodes de reconnaissance biométriques ont été proposées, c'est ce qui a permis à la biométrie de s'étendre vite à de nombreuses applications destinées à gérer l'accès à des ressources physiques (aéroports, casinos...etc.) et logiques (ordinateurs, comptes bancaires...etc.).

Dans ce contexte, un de ces systèmes a été choisi d'être étudié dans ce mémoire, c'est le système de reconnaissance de visage par le Deep learning (Apprentissage profond), ou plus exactement, un système qui utilise le visage comme caractéristique biométrique d'identification des individus, car elle possède beaucoup d'avantage tels que, la facilité d'utilisation, l'acceptation par l'utilisateur (non intrusive), et le faible coût. C'est pour cela que la reconnaissance du visage a été déjà intégrée dans plusieurs systèmes de sécurités biométriques.

Dans ce travail, nous allons nous focaliser sur la réalisation d'un système complet d'authentification de personnes par le visage. Notre but est donc de développer une extraction robuste du modèle (Template) biométrique par l'apprentissage profond pour obtenir une représentation comprimée qui sera utilisée comme entrée pour minimiser les erreurs de reconstruction et améliorer les performances .

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

Le premier chapitre intitulé << La Biométrie >> définit la biométrie et les différentes techniques utilisées.

Le deuxième chapitre intitulé << Le système de reconnaissance de visage >> où nous présentons le processus de reconnaissance de visage et étudions les principales techniques

proposées, ainsi que les différentes difficultés inhérentes à la reconnaissance automatique des visages.

Le troisième chapitre intitulé << Le Deep Learning >>, où nous détaillons les fondements théoriques des méthodes d'apprentissage déjà évoquées. Nous rappelons aussi la notion des réseaux des Neurones (RN) artificiels et leur fonctionnement. En autre, nous abordons une nouvelle technique dérivée des RN qui s'appelle l'apprentissage en profondeur (En Anglais : Deep Learning DL) et nous discutons leurs différents types.

Le quatrième chapitre intitulé << Résultats Expérimentaux >> où l'on présente l'implémentation réalisée et les résultats obtenus. Ce dernier va représenter les résultats expérimentaux finaux de la reconnaissance des visages effectués avec l'algorithme d'apprentissage profond (l'autoencodeur), sur deux bases de données de test qui regroupe plusieurs images de plusieurs personnes (ORL/BBA Faces).

A la fin de ce travail nous concluons par une conclusion **générale** qui résume nos contributions et proposera quelques perspectives sur les travaux futurs.

CHAPITRE 1

LA BIOMETRIE

Introduction

La croissance des communications, tant en taille qu'en diversité, implique la nécessité de sécuriser l'identité des individus. L'importance des paris incite les fraudeurs à contourner les systèmes existants : le premier repose sur la connaissance d'une personne utilisant un mot de passe ou un code PIN. Le second est basé sur ce que possède la personne comme un badge ou une carte à puce. Dans le premier cas, le mot de passe peut être oublié par son utilisateur ou bien deviné par une autre personne. Dans le second cas, le badge (ou la pièce d'identité ou clef) peut être perdu ou volé. Pour contourner cette limitation ou cette faiblesse, un autre moyen de sécurité a été développé pour l'identification des individus en l'occurrence la biométrie.

1. Biométrie

La **biométrie** vise à identifier les personnes à partir de leurs caractéristiques physiques, elle peut être définie comme étant << la reconnaissance automatique d'une personne en utilisant des traits distinctifs>> basée sur les attributs **morphologiques** (empreinte digitale, visage…etc.) ou **comportementales (**la démarche, la dynamique de frappe au clavier, la voix...etc.) ou **biologiques** (salive, ADN...etc.) liés à un individu [1].

1.1 Caractéristique biométriques

Les caractéristiques biométriques par lesquelles il est possible de vérifier l'identité d'un individu sont appelées modalités biométriques. Ces modalités sont basées sur l'analyse des données liées à l'individu et sont généralement classées en trois catégories : biométrie biologique, comportementale et morphologique. Pratiquement, n'importe quelle caractéristique morphologique ou comportement peut être considérée comme une caractéristique biométrique, dans la mesure où elle satisfait les propriétés suivantes :

- **Universalité :** toutes les personnes à identifier doivent la posséder
- **Unicité :** l'information doit être aussi dissimilaire que possible entre les déférentes personnes.
- **Collectabilité :** l'information doit être collectable et mesurable afin d'être utilisé pour les comparaisons.
- **Permanence :** l'information collectée doit être présente pendant toute la vie d'un individu.

- **Acceptabilité :** le système doit respecter certains critères (facilité d'acquisition, rapidité...etc.) afin d'être employés.

1.2 Modalités biométriques

Aucune biométrie unique ne pouvant répondre efficacement aux besoins de toutes les applications d'identifications. Un certain nombre de techniques biométriques ont été proposées, analysées, et évaluées, chaque biométrie à ses forces et ses limites et ses conséquences, chaque biométrie est utilisé dans une application particulière. La biométrie biologique se base sur l'analyse des données biologiques liées à l'individu (salive, ADN, etc.) La biométrie comportementale se base sur l'analyse des comportements d'un individu (manière de marcher, dynamique de frappe au clavier, etc.) [2]. La biométrie morphologique se base sur les traits physiques particuliers qui est pour toute les personnes, sont permanents et uniques (empreinte digitale, visage, etc.).

1.2.1 Biométrie physique

✓ **Empreintes digitales** : La reconnaissance des empreintes digitales est la technique biométrique la plus ancienne et c'est l'une des plus matures. Elle se base sur le fait que chaque personne a des empreintes uniques. Après la capture de l'image de l'empreinte, on fait un rehaussement de l'image. Ensuite on identifier et on extrait les minuties, qui vont être comparées avec l'ensemble des minuties sauvegardées des autres utilisateurs. C'est l'une des technologies biométriques les plus étudiées et les plus utilisées, surtout dans le contrôle d'accès [3].

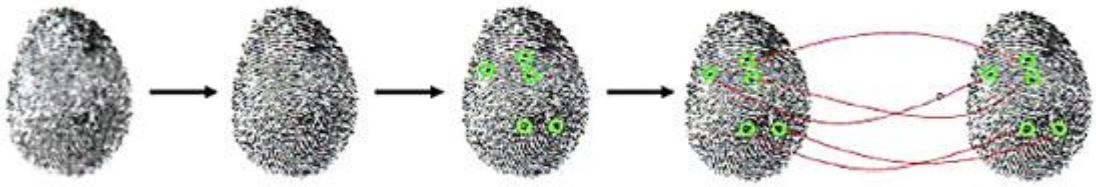


Figure 1.1: le processus de reconnaissance par empreinte digitale

Avantages

-Prix faible.

-Taille du lecteur biométrique n'est pas volumineuse.

-Système reste très simple à mettre en place.

-Utilisation facile.

Inconvénients

-L'inscription est par toutes les parties concernées ce qui peut poser un problème dans le cas où la maladie est physique.

✓ **Visage :** Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s'identifier entre eux, ce qui peut expliquer pourquoi elle est en général très bien acceptée par les utilisateurs. Le système d'acquisition est soit un appareil photo, soit une caméra numérique [3].

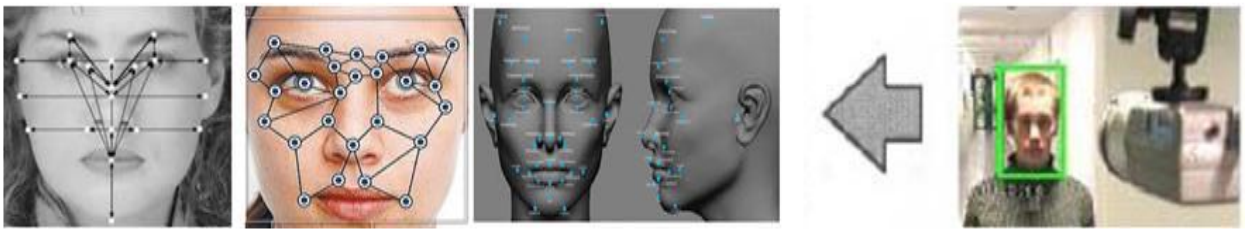


Figure 1.2: Trait biométrique Visage

Avantages

-Technique acceptable par le public.

-Fonctionnement simple.

-Les technique peu couteuse et peut s'appuyer sur l'équipement d'acquisition des images actuel.

Inconvénients

- Les vrais jumeaux ne sont pas différenciés.
- Les changements physiques peuvent tromper le système.
- La technique est trop sensible au changement d'éclairage ou l'angle de l'appareil-photos...etc.

✓ **L'iris :** La reconnaissance de l'iris est une technologie plus récente puisqu'elle s'est véritablement développée que dans les années 80. L'iris est la région annulaire située entre la pupille et le blanc de l'œil. Après l'avoir localisé, on prend des photos en noir et blanc, on utilise ensuite des coordonnées polaires et on cherche les transformées en ondelettes, pour avoir finalement un code représentatif de l'iris. Et on utilise la distance de hamming comme mesure de similarité [3].

Figure 1.3: Trait biométrique Iris

Avantages

-Les structures de l'iris restent stables durant toute la vie

-Grande quantité d'information contenue dans l'iris.

Inconvénients

-L'acquisition des images exige une certaine formation et de la pratique.

-La fiabilité diminue proportionnellement à la distance entre l'œil et la caméra.

-Les gens ont du mal à accepter cette biométrie.

1.2.2 Biométrie comportementale

✓ **Voix :** la voix **humaine** varie d'une personne à l'autre et peut se constituer des composantes physiologiques et comportementales. L'identification par la voix basée sur la forme et la taille des appendices (bouches, cavités nasales et les lèvres) utilisées dans la synthèse du son [4].

Figure 1.4: Signal de voix

Avantages

-Très bien acceptée parce que la voix est un signal naturel à produire.

-Dynamique des ondes produites sont unique.

Inconvénients

-Caractéristiques comportementales changent avec le temps.

-Possibilité de fraude par enregistrement.

-Sensibilité aux bruits lors d'acquisitions.

✓ **Signature manuscrite :** C'est une écriture personnelle d'un individu, la vérification de la signature est basés deux modes :

Mode statique : la vérification de la signature statique met l'accent sur les formes géométriques de la signature, dans ce mode en générale la signature est normalisée à une taille connue ensuite décomposer en élément simple.

Mode dynamique : il utilise les caractéristiques dynamiques telles que l'accélération, la vitesse et les profils de trajectoire de la signature [5].

Figure 1.5: Signature manuscrite

Avantages

- Très acceptable par l'utilisateur.
- Peut protéger l'ensemble de vos fichiers personnels.

Inconvénients

- Grande variante durant le temps (vous ne pouvez pas maintenir la même forme de la signature pour toute la vie).
-Grande possibilité de fraude.

✓ **Frappe dynamique sur le clavier :**

C'est le système de reconnaissance d'un individu basé sur la manière de ses écritures par un dispositif logicielle qui calcule la vitesse de frappe, la suite des lettres, le temps de frappe et la pause entre chaque mot [5].

Figure 1.6: Frappe dynamique sur le clavier

Avantages

- Acceptation forte par l'utilisateur.
- Sécurité bien précise.

Inconvénients

- N'est pas pratique.
- N'est pas permanente durant toute la vie (âge, émotion, fatigue).

1.2.3 Biométrie biologique

✓ **Veines de la main :** les veines de la main sont des réseaux qui varient d'une personne à l'autre. L'analyse de cette différence permet de maintenir des points pour différencier une personne de l'autre.

Figure 1.7: Veines de la main

Avantages

- Ne Nécessite pas de Contact.
- Difficile à falsifier.

Inconvénients

-Très chère.

✓ **Analyse de l'ADN :** la façon la plus précise pour déterminer l'identité de la personne. Il est impossible de trouver deux personnes qui ont le même ADN. Cette modalité possède l'avantage d'être unique et permanente durant toute la durée de vie [5].

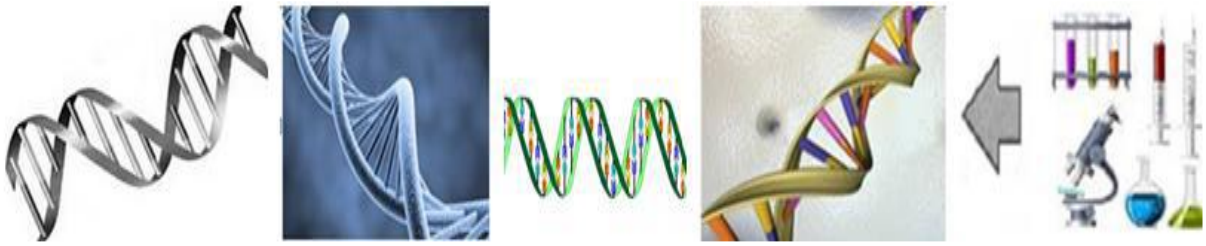


Figure 1.8: Analyse de l'ADN

Avantages

-Distinguer les individus avec une grande précision.

-Facilite la détection des délinquants.

Inconvénients

-Lente pour obtenir les résultats.

-Avoir un coût élève.

2. Architecture d'un système biométrique

Les systèmes biométriques sont de plus en plus utilisés. En général, un système de reconnaissance des personnes basées sur leurs descripteurs biométriques peut se décomposer en deux phases, phase d'enrôlement (création de la base de données) et la phase de reconnaissance [5]. (Voir **Figure 1.9)**.

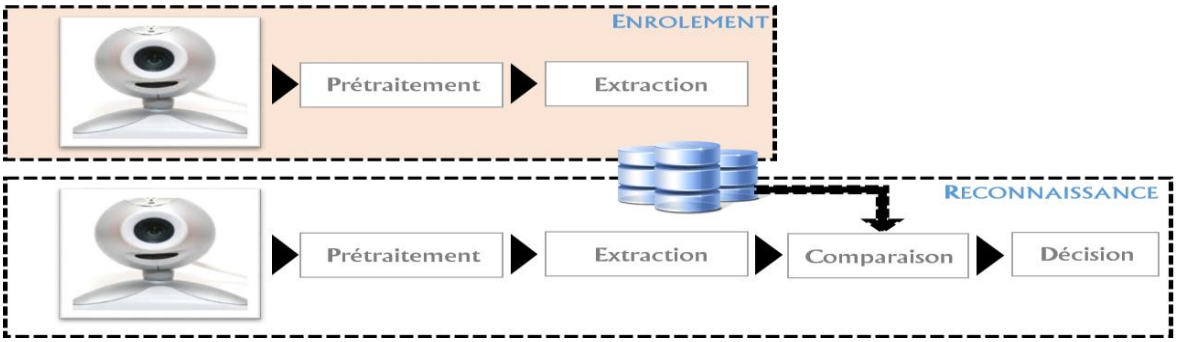


Figure 1.9: Système biométrique

2.1 Fonctionnement

Chaque système biométrique comprend deux phases distinctes :

2.1.1 Phase d'enrôlement : La phase d'enrôlement est définie par le procédé de la collection de traits biométriques d'un individu et le convertir en référence biométrique (Template, vecteur de caractéristique), et à la stocker dans une base de données pour une comparaison ultérieure.

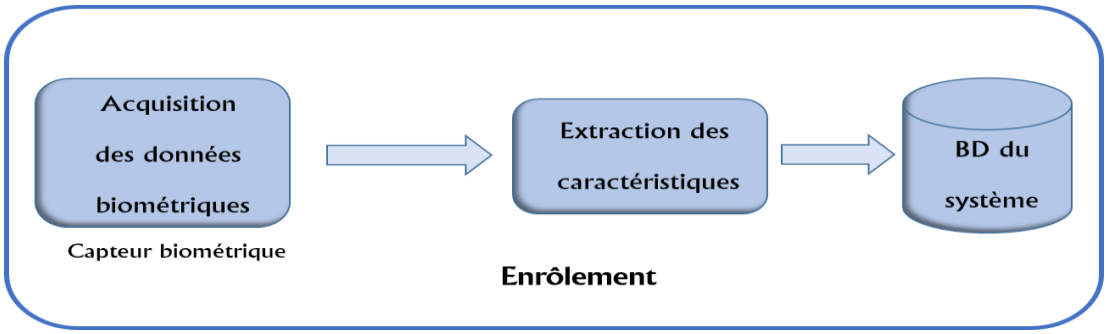


Figure 1.10: Mode d'enrôlement

2.1.2 Phase de reconnaissance : Au cours de la reconnaissance, la modalité biométrique est mesurée et un ensemble des caractéristiques distinctives (Template) est extrait comme lors de l'enrôlement [6]. Cette phase peut être décomposée en deux modes :

2.1.2.1 Mode vérification : le système doit répondre à une question de type :<< Suis-je bien la personne que je prétends être ? >>. L'utilisateur propose une identité au système et le système doit vérifier que l'identité de l'individu est bien celle proposées. Il suffit donc de comparer le signal avec un seul des modèles présents dans la base de données (type 1 :1).

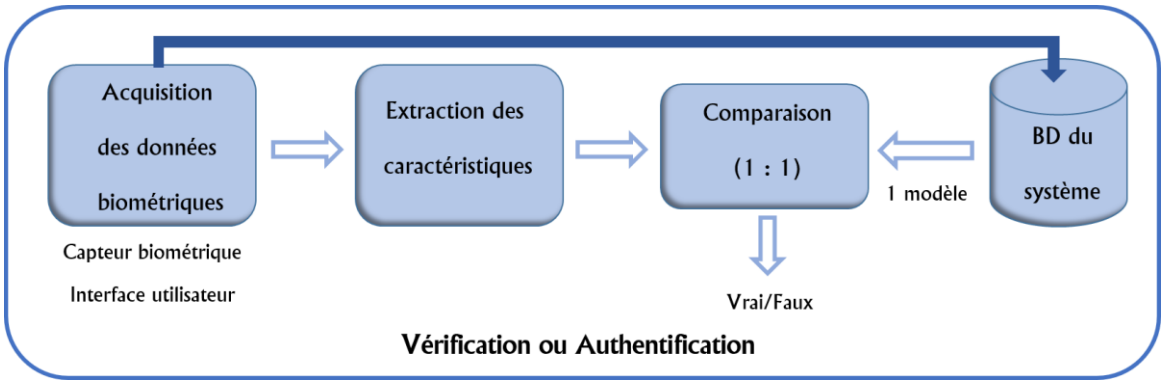


Figure 1.11: Mode vérification

2.1.2.2 Mode identification : Le système doit deviner l'identité de la personne. Il répond donc à une question de type :<< Qui suis-je ? >>. Dans ce mode, le système compare le signal mesuré avec les différents modèles contenus dans la base de données **(type 1 : N)**. En général, lorsque l'on parle d'identification, on suppose que le problème soit fermé, c'est -à-dire que toute personne qui utilise le système possède un modèle dans la base de données [6].

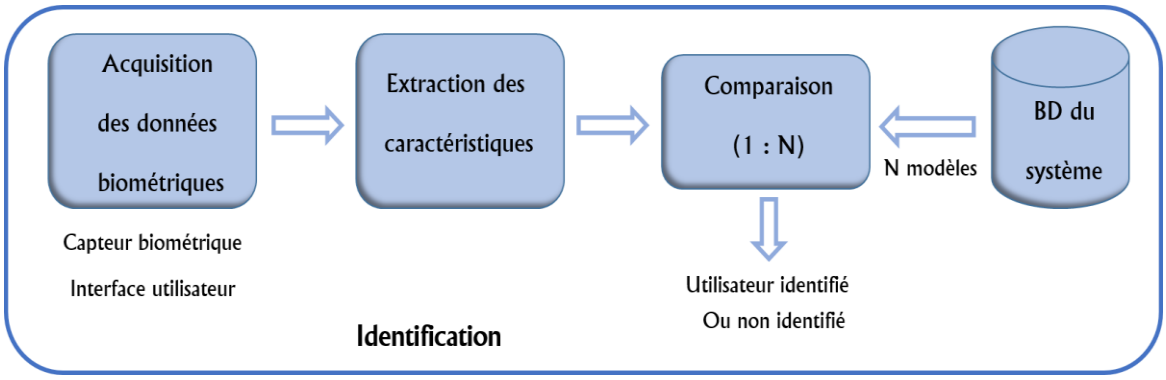


Figure 1.12 : Mode Identification

2.2 Principaux Modules

Un système biométrique typique peut être représenté par quatre modules principaux : **Module de capture :** responsable de l'acquisition des données biométriques d'un individu (cela peut être un appareil photo, un lecteur d'empreintes digitales, une caméra de sécurité...).

Module d'extraction de caractéristiques : Qui prend en entrée les données biométriques acquises par le module de capture et extrait seulement l'information pertinente afin de former une nouvelle représentation des données. Idéalement, cette nouvelle représentation est censée être unique pour chaque personne et relativement invariante aux variations intra-classe.

Module de correspondance : Il compare l'ensemble des caractéristiques extraites avec le modèle enregistré dans la base de données du système et détermine le degré de similitude (ou de divergence) entre les deux.

Module de décision : vérifie l'identité affirmée par un utilisateur ou détermine l'identité d'une personne basée sur le degré de similitude entre les caractéristiques extraites et le(s) modèle(s) stocké(s). [7]

3. Evaluation d'une performance

La performance d'un système d'identification biométrique peut se mesurer principalement à l'aide de trois critères : sa précision, son efficacité (vitesse d'exécution) et le volume de données qui doit être stocké pour chaque personne. Nous nous concentrerons dans cette section sur le premier aspect. Comme nous l'avons vu précédemment, identification et vérification sont des modes opératoires différents.

Elles nécessitent donc des mesures de précision différentes que nous étudierons dans les deux sous -sections suivantes.

3.1 Evaluation de la vérification

3.1.1 Taux d'erreurs : lorsqu'un système en mode de vérification ou identification ensemble ouvert, il existe deux types d'erreur qui peuvent être utilisés pour évaluer leur performance. La première erreur mesure le taux de faux rejet (False Rejection Rate ou FRR) et la deuxième erreur mesure le taux d'acceptation des imposteurs, on parle alors à la fausse acceptation (False Acceptante Rate ou FAR). [2]

Figure 1.13: Distribution des scores et le taux d'erreurs pour un seuil données [2].

FAR : c'est le pourcentage d'individus reconnus par le système biométrique, ce système classe alors deux caractéristiques provenant de deux personnes différentes, comme appartenant à la même personne.

$$FAR = \frac{\text{Nombre des imposteurs acceptés}}{\text{Nombre total d'accès imposteurs}} \quad (1.1)$$

FRR : ce taux représente le pourcentage d'individus censés être reconnus par le système mais qui sont rejetés, le système indique la probabilité qu'un utilisateur connu soit rejeté.

$$FRR = \frac{\text{Nombre de clients rejetés}}{\text{Nombre total d'accès clients}} \quad (1.2)$$

Le taux le plus simple pour mesurer la performance d'un algorithme dans le contexte de la vérification est de calculer le point d'équivalence des erreurs (Equal Error Rate ou EER).

ERR : ce taux est calculé à partir du FAR et du FRR et constitue un point de mesure de performance courant, c'est - à-dire **ERR= FRR= FAR**

$$ERR = \frac{\text{Nombre de fausses acceptations} + \text{Nombre de faux rejets}}{\text{Nombre total d'accès}} \quad (1.3)$$

3.1.2 Les courbes des caractéristiques : Les performances d'un système biométrique peuvent être présentées graphiquement à l'aide de la courbe ROC (Receiver Operating Characteristic) [3].

Cette courbe représente les valeurs de FRR en termes de FAR. Ceci est obtenu en calculant le couple (FAR, FRR) ou chaque valeur du seuil de décision. Celui-ci diffère de la plus petite valeur obtenue à une valeur obtenue à une valeur supérieure. Cette courbe peut être décomposée en trois zones: zone de haute sécurité, zone de compromis et zone de basse sécurité [4].

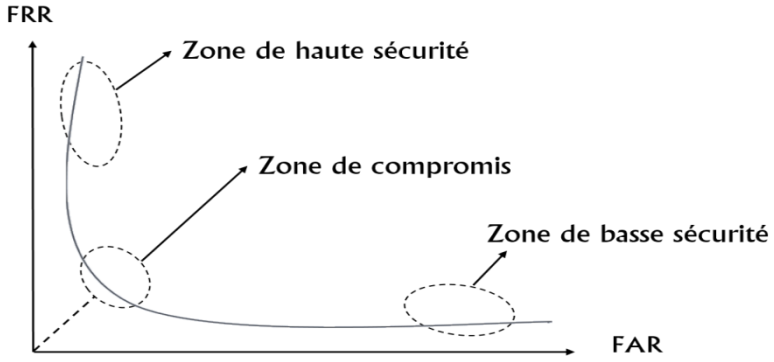
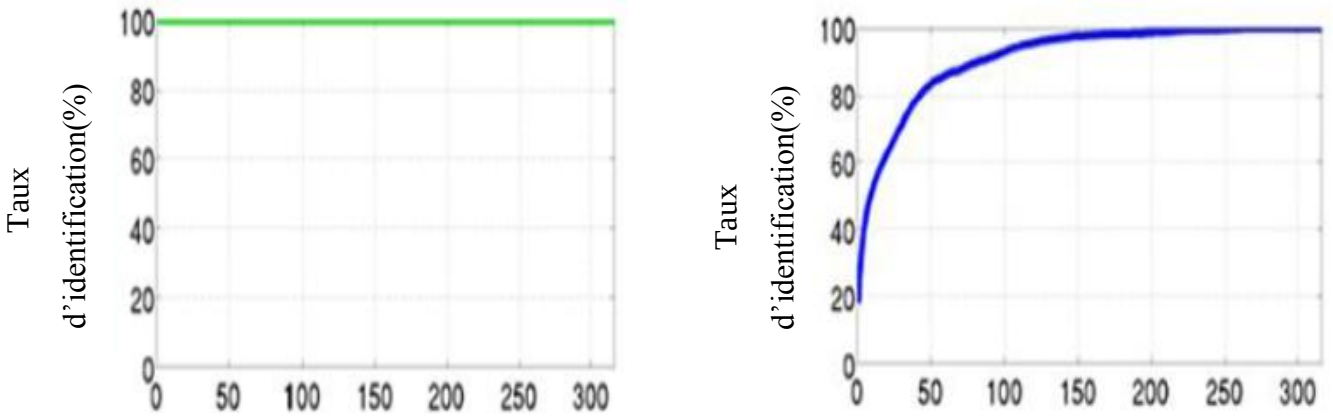


Figure 1.14: Courbe des caractéristiques ROC.

3.2 Evaluation de l'identification

Le taux d'identification (ensemble fermé) est la mesure la plus couramment utilisée mais il n'est pas toujours suffisant. En effet, en cas d'erreur, il peut être utile de savoir si le bon choix se trouve dans les premiers. On trace alors le score cumulé (cumulative match score) qui représente la probabilité que le bon choix se trouve parmi les N [3]. Dans la base de données, les mesures classiques des systèmes de recherche dans une base de données peuvent être utilisées.



(a) Cas idéal (b) Performances usuelles

Figure. 1.15 : Différentes courbes CMC.

(a) 100% des paires sont correctement associées au premier essai

(b) 16% au rang 1 et il faut attendre le rang 270 (sur 316) pour atteindre 100%.

4. Domaines d'applications

La biométrie répond aux exigences de sécurité par les secteurs particuliers et les entreprises dans tous les pays. La sécurité biométrique couvre presque tous les domaines.

Aujourd'hui, La sécurité biométrique est utilisée dans l'accès aux réseaux et aux systèmes d'informatique, paiement électronique et cryptage des données. Généralement, les applications de la sécurité biométrique peuvent être classées en quatre sections principales [4].

4.1 Service public

✓ Le contrôle et la sécurité des bâtiments gouvernementaux frontière.

✓ Contrôle les immigrants qui entrent et sortant pays.

✓ Utilisés dans les aéroports et la santé.

✓ Aidant à passer de la carte d'assurance sociale.

4.2 Pouvoir judiciaire

✓ L'utilisation des empreintes digitales pour prouver certains faits concernant les infractions pénales.

✓ L'utilisation de l'ADN extrait du sang ou des cheveux dans la scène du crime pour obtenir le criminel

4.3 Secteur des banques

✓ Les transactions bancaires (retraits en espèces, les cartes bancaires, paiement par le téléphone et internet).
✓ La réduction de la proportion de la fraude grâce à l'intégration des cartes à puce avec reconnaissance des empreintes digitales

4.4 Accès physique et logique

Ceci se rapporte au contrôle d'accès physique comme la sécurisation des lieux (bâtiment ou une pièce) ou le contrôle d'accès logique comme la sécurisation d'une session informatique (ordinateur ou base de données).

5. Marché de la biométrie

Périodiquement, un rapport sur le marché de la biométrie est publié par l'IBG (International Biometrics Group). Cette étude est une analyse complète des chiffres d'affaires, des tendances de croissance et des développements de l'industrie du marché actuel et futur de la biométrie.

La lecture de ce rapport est essentielle pour les organisations déployant la technologie biométrique, les investissements dans les entreprises biométriques ou les développeurs de solutions biométriques. L'ampleur du chiffre d'affaires de l'industrie de la biométrie, y compris les applications médico-légales et du secteur public, évolue rapidement

Une grande partie de la croissance proviendra du contrôle d'accès aux systèmes d'information (ordinateurs / réseau) et du commerce électronique, bien que les applications du secteur public restent un élément vital de l'industrie. On prévoit que le chiffre d'affaire de marches émergentes (accès aux systèmes d'information, commerce électronique et téléphonie, accès physique et surveillance) dépasse le chiffre d'affaires des secteurs plus matures (identification criminelle et identification des citoyens. [4]

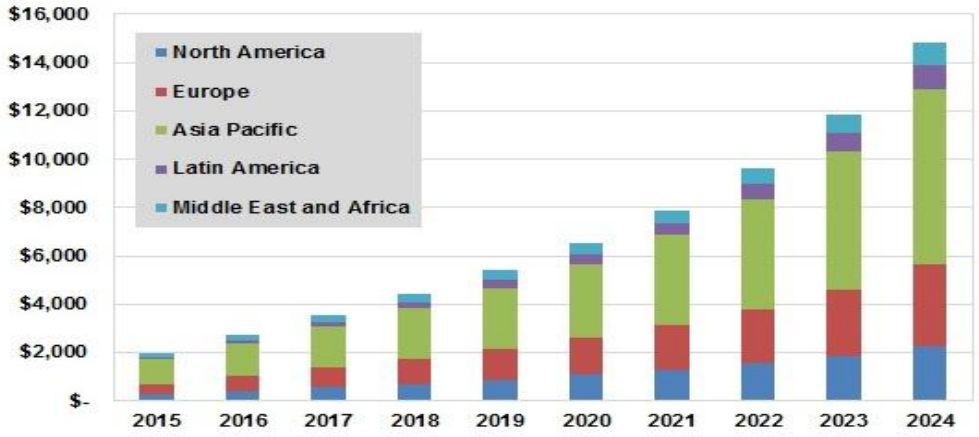


Figure 1.16 : Revenus annuels de la biométrie par région, marchés mondiaux : 2015-2024 [18]

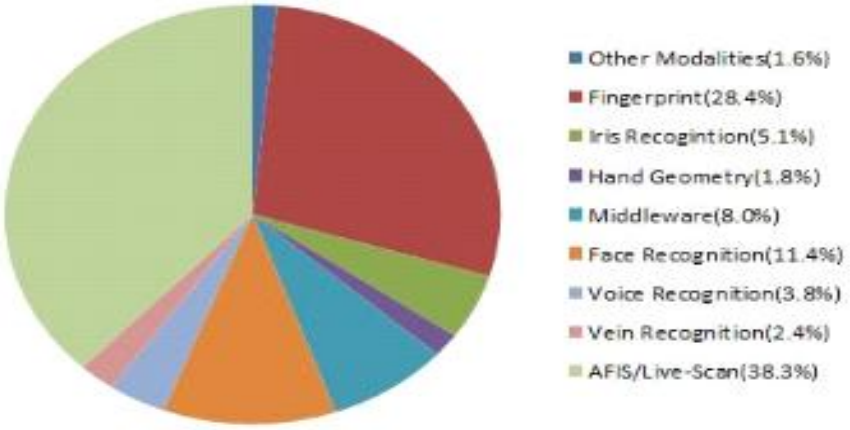


Figure 1.17 : Parts de marché des différentes méthodes biométriques [19]

Conclusion

Dans ce chapitre, nous avons présenté un état de l'art sur les technologies biométriques et mis l'accent sur le grand nombre de ces technologies. Nous avons aussi indiqué quelques points fort et faible de chaque technologie qui met en évidence le fait qu'elles ne sont pas toutes de la même efficacité. Nous avons aussi pris connaissance de l'architecture d'un système biométrique et de l'évaluation de sa performance. Nous avons introduit la notion de vérification et d'identification des personnes, les applications analytiques sur l'utilisation du système de la biométrique.

Les différentes étapes de la reconnaissance de visage sont détaillées dans le chapitre suivant.

CHAPITRE 2

LE SYSTEME DE RECONNAISSANCE DE VISAGE

Introduction

La reconnaissance de visage a été abordée par plusieurs chercheurs et chaque année des avancements dans ce domaine ont vu le jour. L'utilisation de plusieurs notions de base a abouti à de meilleurs résultats pour l'identification du visage.

Au cours des vingt dernières années, la reconnaissance automatique des visages est devenue un enjeu primordial, notamment dans les domaines de l'indexation de documents multimédias et surtout dans la sécurité, ceci est dû aux besoins du monde actuel et aussi à ses caractéristiques avantageuses, Cependant beaucoup de chercheurs essayent d'automatiser le processus de reconnaissance des visages. Pour cela, différentes théories mathématiques et statistiques trouvent leurs applications dans le domaine de la reconnaissance des visages. Il faut adapter ces méthodes à ce problème, en essayant de lui trouver un modèle représentatif.

1. Pourquoi la reconnaissance de visage ?

La reconnaissance de visages est la technique la plus commune et populaire. Elle reste la plus acceptable puisqu'elle correspond à ce que les humains utilisent dans l'interaction visuelle; et par rapport aux autres méthodes, la reconnaissance du visage s'avère plus avantageuse, d'une part c'est une méthode non intrusive, c'est-à-dire elle n'exige pas la coopération du sujet (en observant les individus à distance), et d'autre autre part les capteurs utilisés sont peu coûteux (une simple caméra) contrairement à l'empreinte digitale et l'iris où le sujet devra être très proche du capteur et devra coopérer pour l'acquisition de l'image sans oublier le coût de l'équipement nécessaire pour l'acquisition (équipement spécial coûteux).

Bien que certains disent que la reconnaissance faciale est une biométrie relativement peu sûre. En effet, le fait que le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques, comme la variation de l'éclairage, le changement de la position du visage, la présence ou l'absence de lunettes et autres; mais, au cours de ces dernières années plusieurs techniques de traitements d'images sont apparues, telle que la détection du visage, la normalisation de l'éclairage, etc., sans oublier le développement considérable des technologies des caméras numériques, ce qui néglige l'effet de ces problèmes.

2. Les étapes de la reconnaissance de visage

La reconnaissance faciale est un système permettant d'identifier et de confirmer les personnes en contrôlant si celles-ci appartiennent à la base de données du système. L'image suit un processus de reconnaissance faciale spécifique contenant plusieurs étapes qui peuvent être illustrées dans le diagramme de la figure 2.1 ci-dessous :

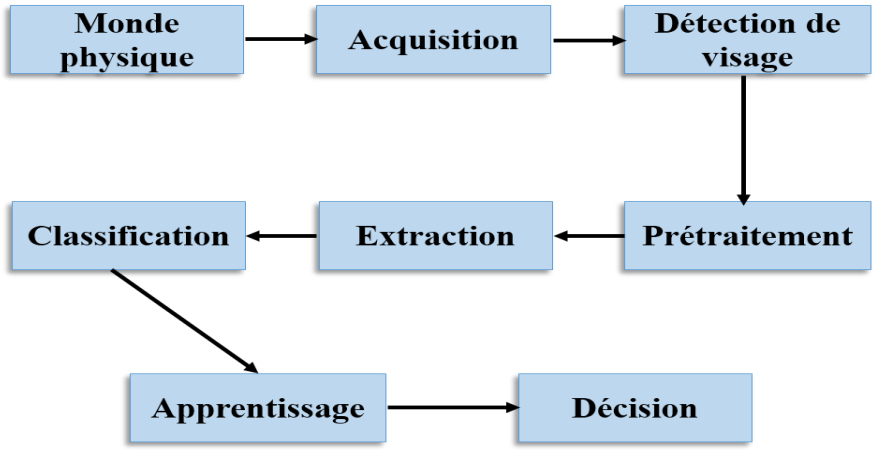


Figure 2.1: Processus d'un système de reconnaissance de visage.

2.1 Le monde physique

C'est le monde réel en dehors du système avant l'acquisition de l'image. Dans cette étape, on tient compte généralement de trois paramètres essentiels : L'éclairage, la variation de posture et l'échelle. La variation de l'un de ces trois paramètres peut conduire à une distance entre deux images du même individu, supérieure à celle séparant deux images de deux individus différents, et par conséquence une fausse identification [8].

2.2 Acquisition

Le système d'acquisition est généralement équipé d'un capteur qui permet aux utilisateurs d'obtenir une fonction spécifique (par exemple, un microphone pour enregistrer le son et une caméra pour capter une photo, etc.). Un appareil photo nous permet d'avoir une image 2D du visage à partir d'une scène 3D comme indiqué dans la figure 2.2

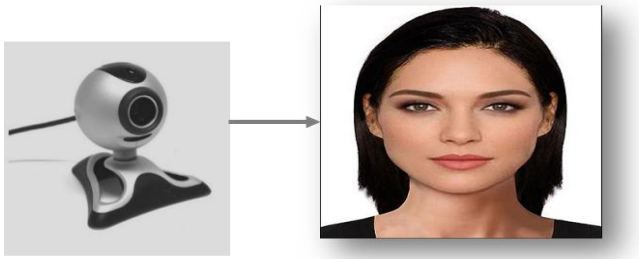


Figure 2.2: Exemple d'acquisition d'une image

2.3 Détection de visage

La détection de visage est une étape très intéressante dans le domaine de reconnaissances de visage. Plusieurs travaux de recherches ont été effectués dans ce domaine. Ils ont donné lieu au développement d'une multitude de techniques allant de la simple détection du visage, à la localisation précise des régions caractéristiques du visage, tels que les yeux, le nez, les sourcils, la bouche, les lèvres, les oreilles, etc. [10].

Un visage est considéré correctement détecté si la taille d'image extraite ne dépasse pas 20% de la taille réelle de la région faciale. Cette étape peut faire la détection de la couleur, de peau, la forme de la tête, il existe plusieurs méthodes détectant les différentes caractéristiques du visage [11].

Les solutions proposées jusqu'à présent ne sont pas suffisamment satisfaites, car elles fonctionnent sous certaines conditions et ne fonctionnent pas dans des acquisitions normales, notamment en présence ou en absence d'aspects structurels du visage, tels que barbe, moustache, lunettes, etc.

Figure 2.3: Détection de visage.

2.4 Le prétraitement

Les données délivrées par les capteurs primaires ne sont qu'une représentation initiale de celles-ci d'où la nécessité d'un traitement antérieur. L'image brute peut être affectée par divers facteurs provoquant sa dégradation, pouvant être bruyante, c'est-à-dire contenir de

fausses informations dues à des dispositifs optiques ou électroniques. Le rôle de cette étape est d'éliminer les parasites accompagnants l'image, provoqués par la qualité de ces dispositifs.

Ceci est nécessaire car l'image ne peut jamais être sans bruit, car le fond et la lumière sont généralement inconnus. Il existe plusieurs types de traitement et d'optimisation de la qualité d'image, tels que la normalisation, les graphiques, le filtrage, la correction gamma ou des méthodes plus complexes telles que le lissage anisotrope [9].

2.5 Extraction des caractéristiques

L'extraction des caractéristiques est le cœur du système de reconnaissance qui extrait les informations d'image qui seront stockées dans la mémoire pour une utilisation ultérieure dans l'étape de décision. Le choix de cette information utile réside dans la création d'un modèle de visage, qui doit être discriminatoire. Cette analyse est appelée propriétés d'indexation, de représentation, de modélisation ou d'extraction. L'efficacité de cette étape a un impact direct sur la performance du système de reconnaissance faciale [8].

2.6 Classification

Lorsque les formulaires sont stockés dans la base de données, le système se compose d'échantillons similaires de nombreuses personnes sélectionnées ainsi que d'une liste limitée de candidats. Cette étape consiste à modéliser les paramètres extraits de la ou les faces de chaque individu en fonction de leurs caractéristiques communes. Un modèle est une collection d'informations utiles, uniques et non récurrentes qui identifie une ou plusieurs personnes ayant des similitudes.

2.7 Apprentissage

L'apprentissage consiste à retenir les modèles calculés pendant la phase d'analyse des personnes connues. Ce modèle est une représentation intégrée d'images pour faciliter l'identification, mais aussi la quantité de données stockées sous une forme ou une autre. Cette étape correspond aux références interactives réelles qui seront enregistrées dans la base de données.

2.8 Décision

La décision fait partie du système dans lequel nous décidons si l'individu appartient à tous les visages ou non. Dans cette phase, le système d'identification consiste à trouver le modèle correspondant au visage pris à partir de ceux stockés dans la base de données, dans ce cas quelle est son identité. Par conséquent, la résolution est l'aboutissement de ce processus, il peut être évalué au taux de reconnaissance (fiabilité), déterminé par le taux de résolution de la décision.

3. Les Méthodes de reconnaissance de visage

Les méthodes de reconnaissance de visages peuvent être classées en trois grandes approches. Une approche globale dans laquelle on analyse le visage (l'image pixellisée du visage) dans son entier, une approche locale basée sur un modèle, dans laquelle le système essaie de détecter, regrouper et reconnaitre les différents éléments constitutifs du visage tel que le nez, les yeux et la bouche. Enfin, il existe des méthodes hybrides qui combinent les deux approches précédentes

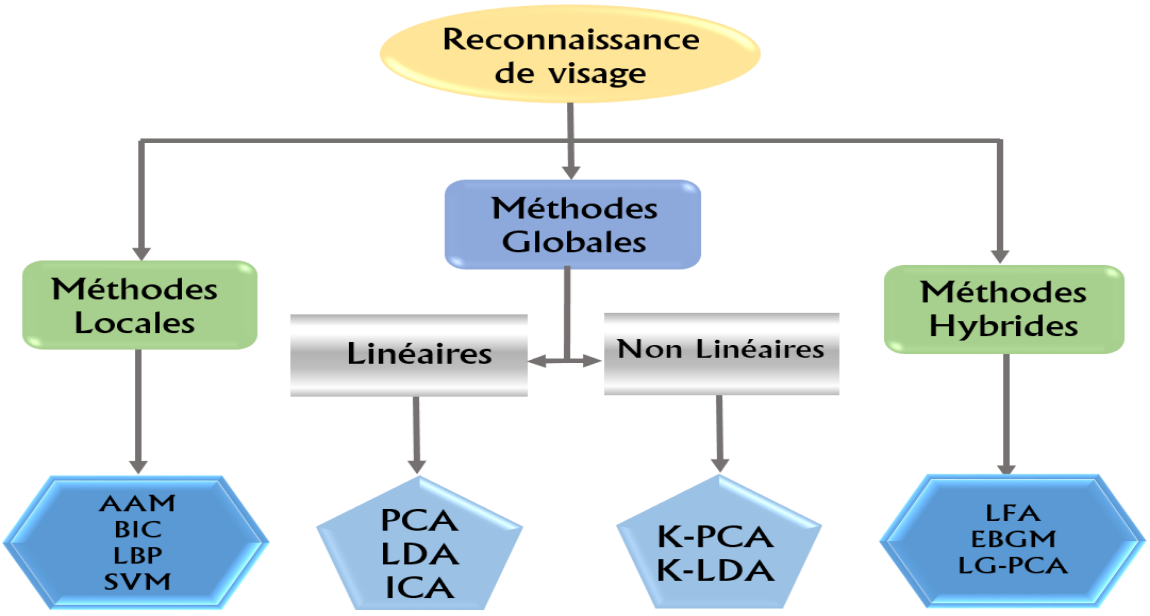


Figure 2.4: Les Méthodes de reconnaissance de visage.

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

✓ L'**A**nalyse en **C**omposantes **P**rincipales (**PCA** ou **Eigen Faces**).
✓ L'**A**nalyse **D**iscriminante **L**inéaire (**LDA**).
✓ **M**achine à **V**ecteurs de **S**upport (**SVM**).
✓ Les **R**éseaux de **N**eurones (**RNA**).

3.2 Méthodes Locales

On les appelle aussi les méthodes à traits, à caractéristiques locales, ou analytiques. Le visage humain est analysé à travers la description individuelle de ses parties et de leurs relations. Ce modèle correspond à la façon dont une personne perçoit le visage, c'est-à-dire à nos notions de traits et de parties du visage comme les yeux, le nez, la bouche, etc. La plus part des travaux réalisés se sont concentrés sur l'extraction des traits à partir d'une image du visage et sur la définition d'un modèle adéquat pour représenter ce visage. Un certain nombre de stratégies ont modélisé et classé les faces en fonction des distances et des angles naturels entre des points distincts. Cette étape d'extraction des traits distinctifs du visage est la première étape du processus, car les performances de l'ensemble du système en dépendent. L'avantage de ces méthodes est qu'elles prennent en compte la particularité du visage en tant que forme naturelle, elle doit être reconnue et le nombre de paramètres minimisé en exploitant les résultats de la recherche en neuropsychologie et en psychologie cognitive sur le système visuel humain. La difficulté éprouvée quand il s'agit de prendre en considération plusieurs vues du visage ainsi que le manque de précision dans la phase "extraction" des points constituent leur inconvénient majeur. [12]

3.3 Méthodes Hybrides

Les méthodes hybrides permettent d'associer les avantages des méthodes globales et locales en combinant la détection de caractéristiques géométrique avec l'extraction de caractéristique

d’apparence locales. Elles permettent d’augmenter la stabilité de la performance de reconnaissance lors de changements de pose, d’éclairement et d’expressions faciales. [4]

4. Principales difficultés de la reconnaissance de visage

Pour le cerveau humain, la reconnaissance faciale est une mission visuelle de haut niveau. Bien que les gens puissent détecter des objets et les reconnaître dans une scène sans trop de problèmes, la création d'un système automatique qui effectue ces tâches est un défi sérieux. Ce défi est beaucoup plus grand que les conditions pour obtenir des images très différentes. La différence entre les sujets est limitée par la similitude physique entre les individus. D'un autre côté, la différence dans ce sujet est plus grande. Cela peut être attribué à plusieurs facteurs que nous analysons ci-dessous.

4.1 Changement d’illumination

Certains facteurs tels que l'éclairage (répartition de la source de lumière, intensité, spectre) et les caractéristiques de la caméra affectent l'apparence d'un visage dans l'image acquise.

Figure 2.5: Exemples de changement d’illumination. [20]

4.2 Variation de pose

C'est une variation de la rotation et c'est un gros problème avec les systèmes de reconnaissance faciale. En effet, de nombreux tests ont montré que la restauration de la tête n'entraîne pas de réduction significative des taux de détection à ± 25 °. Mais si cette rotation dépasse ce seuil, cela réduira les performances.

Figure 2.6: Exemples de variation de pose. [20]

4.3 Expressions faciales

La déformation faciale due aux expressions faciales affecte principalement la partie inférieure du visage. L'information faciale trouvée en haut du visage reste presque constante, ce qui est habituellement suffisant pour mener à bien le processus d'identification. Cependant, puisque l'expression faciale modifie l'apparence du visage, elle entraîne nécessairement une diminution du taux de reconnaissance. L'identification faciale avec l'expression faciale est un problème difficile qui est toujours pertinent et reste non résolu [4].

Figure 2.7: Exemples de variation d'expressions. [20]

4.4 Présence ou absence des composants structurels

Des aspects particuliers tels que la barbe, la moustache et les lunettes, provoquent des changements importants dans les composants structuraux du visage, notamment la forme, la couleur, la taille, etc.

Figure 2.8: Exemples de composants structurels. [20]

4.5 Les occultations

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

5. Les bases de visages utilisées

Plusieurs bases de visages ont été développées pour l'évaluation des algorithmes de reconnaissance faciale. Chacune comporte des conditions de prises de vues différentes. Les bases les plus anciennes (ORL et YALE) ont été le plus utilisées et permettent de comparer plus facilement de nouvelles méthodes à celles de l'état de l'art. Les plus récentes (Color FERET, FRGC, CVL, AR et IV²) contiennent plus de personnes et sont donc utiles pour des évaluations à plus grande échelle. D'autres bases de visages sont disponibles et destinées à des évaluations adaptées à certaines variabilités du visage telles que les bases UMIST, BANCA, PF01, Yale et PIE. Ces trois dernières bases par exemple (PF01, Yale et PIE) disposent d'un nombre important de poses différentes mais renferment seulement quelques dizaines de personnes acquises lors d'une seule session.

Différents facteurs sont appliqués sur les visages à savoir des changements d'éclairage, de poses, d'expressions faciales et des occultations. Les variations dans le temps des visages sont étudiées à travers l'acquisition de plusieurs sessions avec un intervalle de durée défini [31].

Conclusion

Dans ce chapitre, nous avons présenté la technologie de reconnaissance faciale pour identifier les personnes. Nous avons également fourni un aperçu des étapes et des techniques de reconnaissance faciale (PCA, ICA, etc.). Cette étude nous a permis de savoir que la reconnaissance faciale attire davantage l'attention de la communauté scientifique car elle présente de nombreux défis et obstacles technologiques.

Enfin, nous avons mis en évidence les différentes difficultés inhérentes à la reconnaissance automatique des visages, ce qui nous a permis d'identifier les problèmes qui pourraient être résolus.

CHAPITRE 3

LE DEEP LEARNING

Introduction

L'intelligence artificielle est une discipline scientifique recherchant des méthodes de solution de problèmes à forte complexité logique ou algorithmique. L'apprentissage automatique est un champ d'étude de l'intelligence artificielle. Par conséquent, L'apprentissage profond (en anglais deep Learning, deep structured Learning, hierarchical Learning) est un ensemble de méthodes d'apprentissage automatique tentant de modéliser avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires. Dans ce chapitre nous allons présenter tout d'abord les notions en relation avec l'apprentissage profond.

1. Réseaux de neurones

1.1 Définition

Un réseau de neurones artificiels est un système dont la conception est à l'origine inspirée du fonctionnement des neurones biologiques, et qui par la suite s'est rapproché des méthodes statistiques [23]. Les réseaux de neurones artificiels sont des réseaux fortement connectés par des processeurs élémentaires fonctionnant en parallèle. Chaque processeur élémentaire (neurone artificiel) calcule une sortie unique sur la base des informations qu'ils reçoivent.

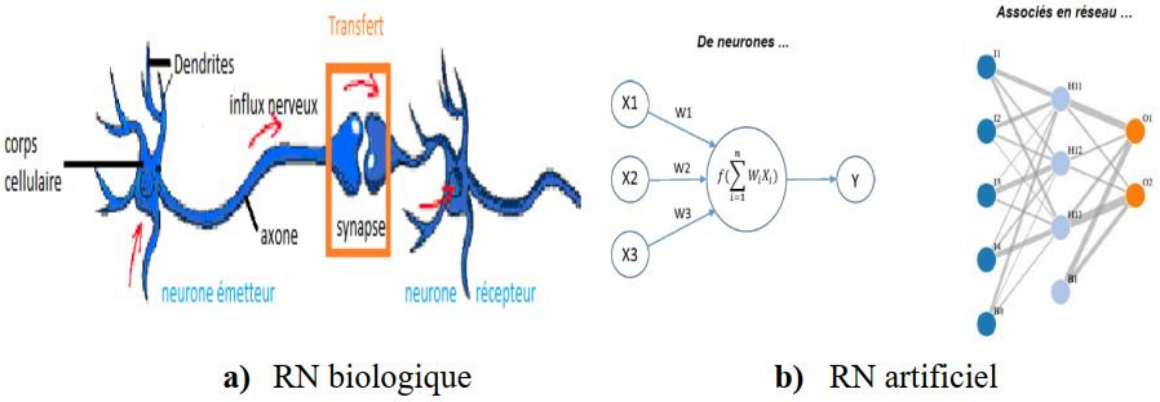


Figure 3.1 : Définition d'un réseau de neurones [22]

1.2 L'évolution de l'intelligence artificielle

L'intelligence artificielle a connu une longue histoire puisqu'elle a été conceptualisée dès l'antiquité. Bien sûr ce n'est que suite à la création des premiers ordinateurs qu'elle a pu être mise en œuvre de façon concrète. Différents courants se sont alors développés. L'un de ces consistait à s'inspirer du cerveau humain afin de tenter de créer des neurones artificiels. Un neurone artificiel n'est rien d'autre qu'une opération mathématique relativement simple. La complexité repose avant tout dans l'interconnexion de plusieurs neurones. Le premier réseau de neurones artificiels a été mis au point en 1951 par Marvin Minsky et Dean Edmonds de l'Université de Harvard. Peu de temps après, en 1956, Frank Rosenblatt a mis au point le Perceptron qui a suscité un grand engouement. Les scientifiques misaient alors énormément sur les réseaux de neurones mais les résultats ont fini par décevoir. [21]

2. L'apprentissage en profondeur (deep Learning)

2.1 Introduction sur deep Learning

Le Deep Learning est un nouveau domaine de recherche de la machine Learning (ML), qui a été introduit dans le but de rapprocher le ML de son objectif principal à savoir : l'intelligence artificielle. Il concerne les algorithmes inspirés par la structure et du fonctionnement du cerveau. Ils peuvent apprendre plusieurs niveaux de représentation dans le but de modéliser des relations complexes entre les données.

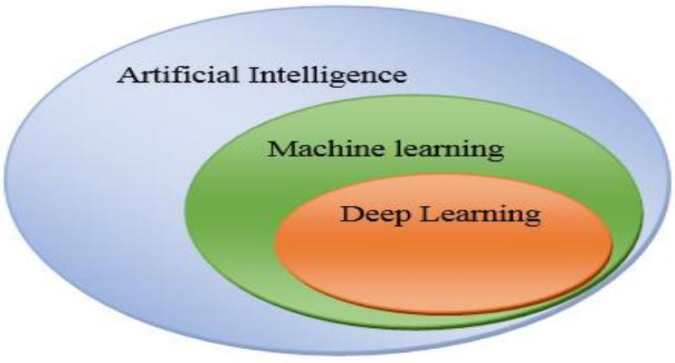


Figure 3.2 : La relation entre l'intelligence artificielle, le ML et le deep Learning

2.2 Définition

L'apprentissage en profondeur est un ensemble d'algorithmes d'apprentissage automatique qui tentent d'apprendre à plusieurs niveaux, correspondant à différents niveaux d'abstraction.

Il a la capacité d'extraire des caractéristiques à partir des données brutes grâce aux multiples couches de traitement composé de multiples transformations linéaires et non linéaires et apprendre sur ces caractéristiques petites à petit à travers chaque couche avec une intervention humaine minime [16].

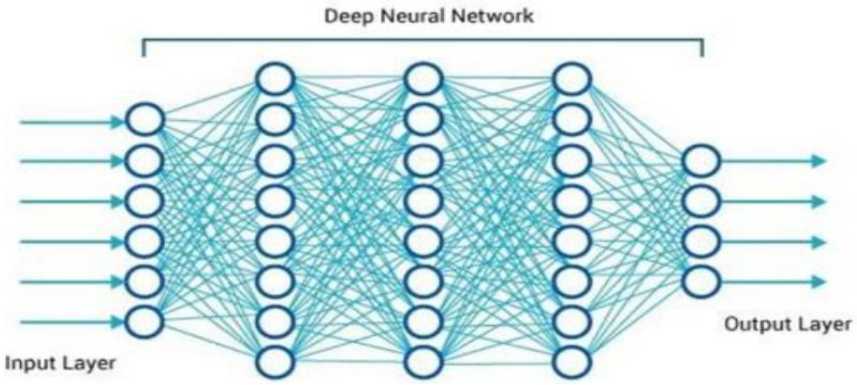


Figure 3.3 : Schéma illustratif de DL avec plusieurs couches [16]

2.3 L'avènement du Deep Learning

Ce n'est que récemment, grâce à l'avancée des performances de calcul des ordinateurs que s'est développé le concept de Deep Learning. Il s'agit de réseaux de neurones disposant de nombreuses couches cachées (c'est à dire de nombreuses couches de neurones situées entre les couches d'entrées, acceptant des données à traiter, et les couches de sortie, destinées à délivrer le résultat du calcul). A la grande surprise des spécialistes, l'ajout de ces couches de neurones a eu un impact extrêmement bénéfique sur la qualité des résultats obtenus. C'est ce qui permet à l'intelligence artificielle de revenir sur le devant de la scène depuis quelques années. La plupart des acteurs du domaine **ne** jurent aujourd'hui plus que par le Deep Learning. Google, Facebook, Apple et Microsoft mettent d'ailleurs tous leur propre librairie de Deep Learning à la disposition des développeurs.

Année	Contributeur	Contribution
2006	Geoffrey Hinton	Introduction des deep Belief network
2009	Salakhutdinov and Hinton	Introduction des deep Boltzmann machines
2012	Alex Krizhevsky	Introduction de AlexNet qui remporta le challenge Image Net

Tableau 3.1 : Les étapes majeures du Deep Learning [16].

2.4 Pour quoi le deep Learning ?

Les algorithmes de ML décrits dans la première partie fonctionnent bien pour une grande variété de problèmes. Cependant ils ont échoué à résoudre quelques problèmes majeurs de l'IA telle que la reconnaissance vocale et la reconnaissance d'objets. Le développement du deep Learning fut motivé en partie par l'échec des algorithmes traditionnels dans de telle tâche de l'IA. Mais ce n'est qu'après que de plus grandes quantités de données ne soit disponibles grâce notamment au Big Data et aux objets connectés et que les machines de calcul soient devenues plus puissantes qu'on a pu comprendre le potentiel réel du Deep Learning. Une des grandes différences entre le Deep Learning et les algorithmes de ML traditionnelles c'est qu'il s'adapte bien, plus la quantité de données fournie est grande plus les performances d'un algorithme de Deep Learning sont meilleures. Contrairement à plusieurs algorithmes de ML classiques qui possèdent une borne supérieure à la quantité de données qu' ils peuvent recevoir des fois appelée "plateau de performance", les modèles de Deep Learning n'ont pas de telles limitations (théoriquement) et ils sont même allés jusqu'à dépasser la performance humaine dans des domaines comme l'image processing .Autre différence entre les algorithmes de ML traditionnelles et les algorithmes de Deep Learning c'est l'étape de l'extraction de caractéristiques. Dans les algorithmes de ML traditionnelles l'extraction de caractéristiques est faite manuellement, c'est une étape difficile et coûteuse en temps et requiert un spécialiste en la matière alors qu'en Deep Learning cette étape est exécutée automatiquement par l'algorithme.

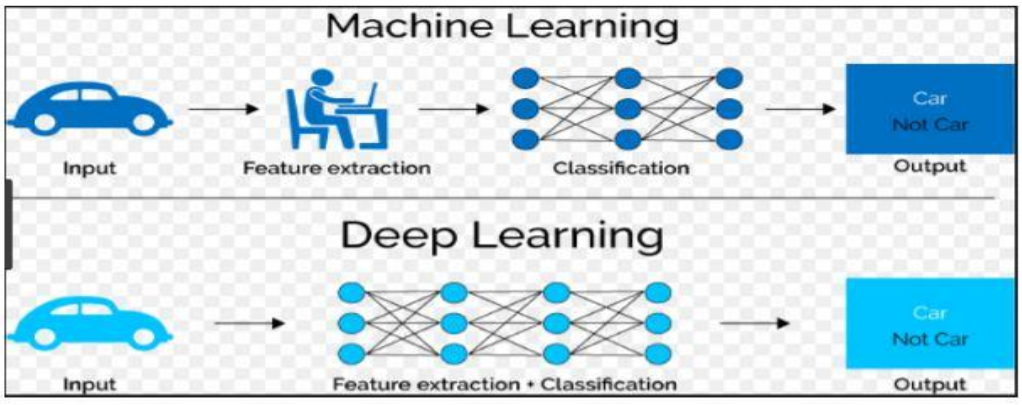


Figure 3.4 : La différence entre machine Learning et deep Learning [24].

2.5 Les différentes architectures du Deep Learning

Nous examinons les tops cinq architectures d'apprentissage en profondeur les plus populaires et les plus utilisées que nous devons connaître :

2.5.1 Convolutional Neural Networks

Les réseaux de neurones convolutifs, ou CNN, sont le choix populaire des réseaux de neurones pour différentes tâches de vision par ordinateur telles que la reconnaissance d'image. Le nom « convolution » est dérivé d'une opération mathématique impliquant la convolution de différentes fonctions. La conception d'un CNN comporte 4 étapes principales :

- **Convolution :** le signal d'entrée est reçu à ce stade
- **Sous-échantillonnage :** les entrées reçues de la couche de convolution sont lissées pour réduire la sensibilité des filtres au bruit ou à toute autre variation.
- **Activation :** cette couche contrôle la façon dont le signal circule d'une couche à l'autre, semblable aux neurones de notre cerveau.
- **Entièrement connecté :** dans cette étape, toutes les couches du réseau sont connectées avec chaque neurone d'une couche précédente aux neurones de la couche suivante

Voici un aperçu approfondi de l'architecture CNN et de son fonctionnement, comme l'explique le célèbre chercheur en IA Giancarlo Zaccone. [17]

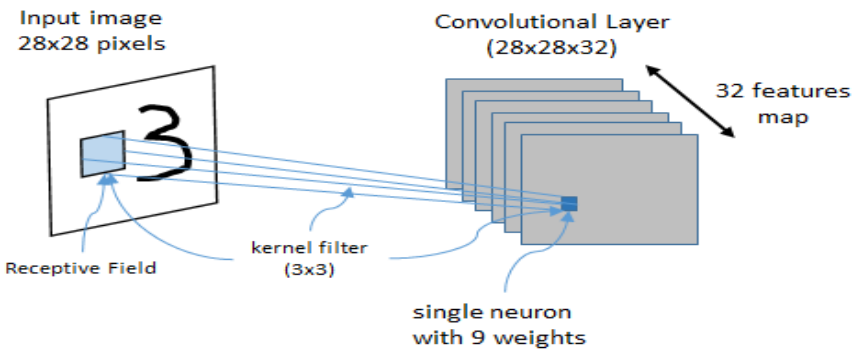


Figure 3.5: Un échantillon de CNN en action

2.5.2 Recurrent Neural Networks

Les réseaux neuronaux récurrents (RNN) ont été très populaires dans les domaines où la séquence dans laquelle les informations sont présentées est cruciale. En conséquence, ils

trouvent de nombreuses applications dans des domaines du monde réel tels que le traitement du langage naturel, la synthèse vocale et la traduction automatique.

Les RNN sont appelés « récurrents » principalement parce qu'une tâche uniforme est exécutée pour chaque élément unique d'une séquence, la sortie dépendant également des calculs précédents. Considérez ces réseaux comme ayant une mémoire, où chaque information calculée est capturée, stockée et utilisée pour calculer le résultat final

Au fil des ans, plusieurs variétés de RNN ont été recherchées et développées :

- **RNN bidirectionnel :** La sortie de ce type de RNN dépend non seulement du passé mais aussi des résultats futurs
- **RNN profond :** Dans ce type de RNN, il y a plusieurs couches présentes par étape, permettant un plus grand taux d'apprentissage et plus de précision. [17]

2.5.3 **Generative Adversarial Networks**

La prémisse de base des réseaux adverses génératifs (GAN) est la formation simultanée de deux modèles d'apprentissage profond. Ces réseaux d'apprentissage en profondeur se font essentiellement concurrence un modèle qui essaie de générer de nouvelles instances ou de nouveaux exemples est appelé générateur. L'autre modèle qui essaie de classer si une instance particulière provient des données d'apprentissage ou du générateur est appelé discriminateur [17]

2.5.4 ResNets

Depuis qu'ils ont gagné en popularité en 2015, les réseaux ResNets ou Deep Residual Networks ont été largement adoptés et utilisés par de nombreux scientifiques des données et chercheurs en IA. Comme vous le savez déjà, les CNN sont très utiles pour résoudre les problèmes de classification d'images et de reconnaissance visuelle. À mesure que ces tâches deviennent plus complexes, la formation du réseau neuronal commence à devenir beaucoup plus difficile, car des couches profondes supplémentaires sont nécessaires pour calculer et améliorer la précision du modèle. L'apprentissage résiduel est un concept conçu pour s'attaquer à ce problème, et l'architecture résultante est communément connue sous le nom de ResNet. [17]

.

2.5.5 Auto-encoders

L'autoencodeur est un modèle permettant de faire une compression de l'entrée (encodeur) et une décompression de celle-ci (décodeur)

Les auto-encodeurs (AE) sont des réseaux de neurones qui ont pour objectif de copier leurs entrées dans leurs sorties. Ils travaillent en comprimant l'entrée dans une représentation spatiale latente, puis en reconstruisant la sortie de cette représentation. Ce type de réseau est composé de trois parties :

Encodeur : C'est la partie du réseau qui compresse l'entrée en une représentation en espace latent. Il peut être représenté par une fonction de codage ***h = f (x).***

Milieu : C'est l'espace latent où l'on trouve la partie compressée des données d'entrée.
Décodeur : Cette partie a pour objectif de reconstruire l'entrée de la représentation de l'espace latent. Il peut être représenté par une fonction de décodage ***y = g (h)***. [25]

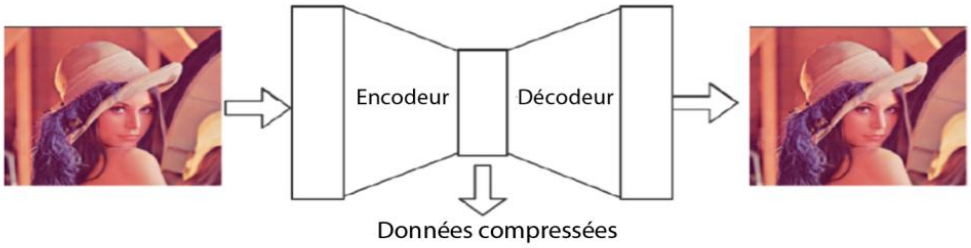


Figure 3.6 : Schéma de principe de l'autoencodeur [26].

2.5.5.1 Architecture d'autoencodeur

L'Autoencodeur est un type spécial du DNN (Deep Neural Networks) sans classe étiquetée, dont les vecteurs de sortie ont la même dimensionnalité que les vecteurs d'entrées.

Il est souvent utilisé dans l'encodage de données Un autoencodeur a typiquement une couche d'entrée (couche L1) qui représente les vecteurs de données ou de caractéristique, une ou plusieurs couches cachées qui représentent la caractéristique transformée (couche L2) et une couche de sortie qui correspond à la couche d'entrée (couche L3). Lorsque le nombre de couches cachées est supérieur à un, l'auto encoder est considéré comme profond. La dimension des couches peut être soit plus petite (lorsque l'objectif est la compression) ou grande (lorsque l'objectif est d'augmenter la dimension d'espace) (voir La Figure 3.7) [15]

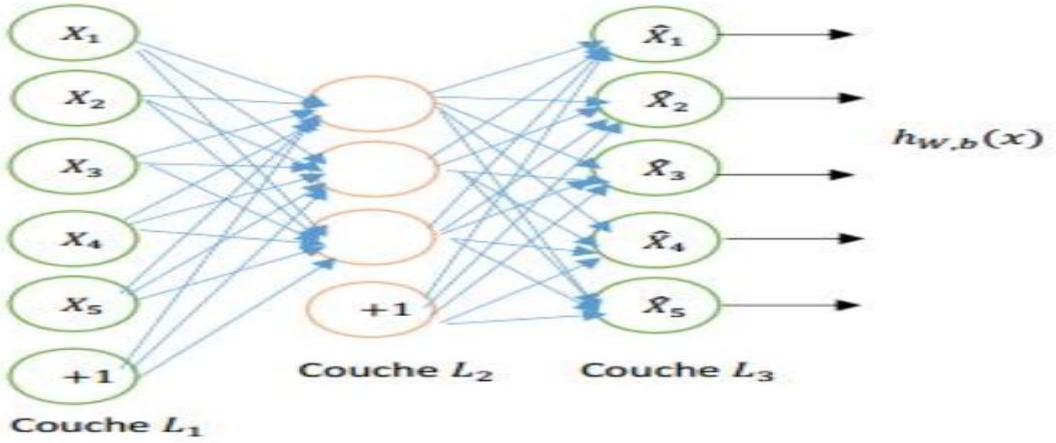


Figure 3.7 : L'architecture des autoencodeurs [27]

2.5.5.2 Le prétraitement de l'image avec l'autoencodeur

Fondamentalement, un autoencodeur est une méthode d'apprentissage non supervisée qui est entrainée pour reconstruire son entrée à sa sortie (encodage). L'auto encodeur est constituée de deux parties essentielles : l'encodeur et le décodeur. Ainsi, trois couches ont été utilisées :

- Une couche d'entrée.
- Une couche de sortie.
- Une couche cachée.

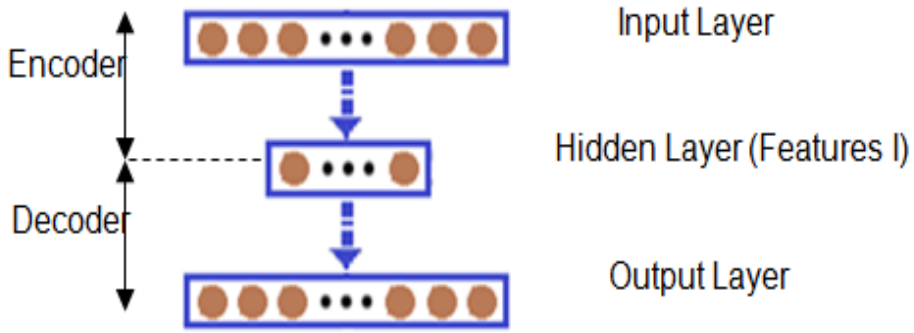


Figure 3.8 : Le prétraitement de l'autoencodeur

Soit V un ensemble de vecteurs de caractéristiques d'entraînement que l'entrée d'une auto encodeur, puis l'encodeur associe ces données à une autre donnée en utilisant les formules suivantes :

$$z^{(1)} = f^{(1)}\left(w^{(1)}x + b^{(1)}\right) \qquad (3.1)$$

Ensuite, le décodeur mappe la représentation du codeur z dans une estimation de la matrice d'entrée originale, x, comme suit :

$$\hat{x} = g^{(2)}\left(w^{(2)}x + b^{(2)}\right) \qquad (3.2)$$

La fonction d'activation sigmoïde Logistic a été utilisée à la fois pour le codeur et le décodeur. Il est calculé par :

$$\log sig(v) = \frac{1}{(1 + \exp(-v))} \qquad (3.3)$$

La fonction de coût mesure l'erreur entre l'entrée x $\in \mathbb{R}^D$ et sa reconstruction à la sortie $\hat{x} \in \mathbb{R}^D$.

L'apprentissage d'un autoencodeur crypté consiste à ajuster la fonction d'erreur quadratique moyenne comme suit :

$$E = \frac{1}{N}\sum_{n=1}^{N}\sum_{m=1}^{M}(x_{mn} - \hat{x}_{mn})^2 + \alpha.\lambda_{weight} + \beta.\lambda_{sparsity} \quad (3.4)$$

Où α et β se réfèrent respectivement aux coefficients du terme de régularisation et du terme de régularisation de la parcimonie

Les $\lambda_{sparsity}$, λ_{weight} sont calculés comme suit :

$$\lambda_{weight} = \frac{1}{2}\sum_{h}^{H}\sum_{j}^{n}\sum_{i}^{m}({w_{ij}}^{(h)})^2 \quad \lambda_{sparsity} = \sum_{i=1}^{D}\xi\log\left(\frac{\xi}{\hat{\xi}_i}\right) + (1-\xi)\log\left(\frac{1-\xi}{1-\hat{\xi}_i}\right) \qquad (3.5)$$

Où H désigne le nombre de couches cachées, n désigne le nombre d'observations et m représente le nombre de données d'apprentissage.

ξ_i représente les mesures d'activation de sortie moyenne d'un neurone i donnée par:

$$\hat{\xi}_i = \frac{1}{n}\sum_{j=1}^{n} h\left({w_i}^{(1)T}x_j + {b_i}^{(1)}\right) \qquad (3.6)$$

Où x_j représente le j échantillon d'apprentissage ${w_i}^{(1)T}$ et ${b_i}^{(1)}$ sont la ligne i de la matrice de poids et l'entrée i du vecteur de polarisation respectivement [32].

2.5.5.3 SAE-DNN (Stacked autoencoder - Deep Neural Network)

Le SAE-DNN consiste à deux types de réseau de neurones profond à savoir le SAE et le DNN.

Le SAE est constitué de plusieurs couches d'autoencodeur dans lesquels les sorties de chaque couche sont reliées aux entrées de la couche suivante. Ces auto encodeurs entrainent les couches cachées de DNN l'un après l'autre. L'apprentissage de DNN comprend deux étapes (figure 3.11). À la première étape, l'« autoencodeur 1»subit un apprentissage non supervisé. Ensuite, la « couche h1 » de DNN est initialisée par les poids d'« autoencodeur 1» après son apprentissage. Par la suite, les poids de « couche h1 » de premier auto-encodeur deviennent les entrées de la seconde (couche h2) et ainsi de suite. À la deuxième étape, l'apprentissage supervisé de DNN s'amorce [24].

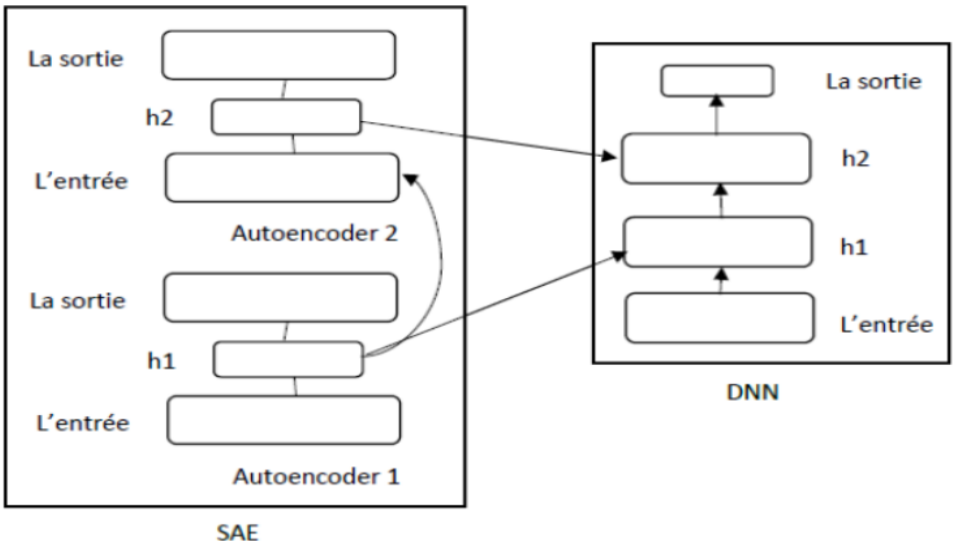


Figure 3.9 : L'architecture de SAE-DNN [27].

Conclusion

Dans ce chapitre nous avons présenté les notions de base de RN notamment son principe de fonctionnement, ses composantes principales et également ses limitations.

Ensuite, nous avons décrit une nouvelle variante de RN qui s'appelle Deep Learning (DL). Cette technique se caractérise par son habilité de résoudre le problème de la complexité de l'entraînement de (RN) ainsi que son pouvoir de représenter les formes (les entrées) d'une manière puissante, automatiques et discriminante.

Finalement, nous avons discuté les différents modèles de Deep Learning à savoir le CNN, RNN, GAN, ResNets et l'Autoencodeur. Ce dernier a été bien détaillé car il va faire l'objet de plusieurs expériences dans le chapitre suivant.

CHAPITRE 4

RESULTATS EXPERIMENTAUX

Introduction

Ce chapitre représente les résultats expérimentaux finals de la reconnaissance de visages, effectués avec l'algorithme d'apprentissage profonds (Auto-encodeurs) et les algorithmes Gabor,LDA sur une base de données de test « ORL », qui regroupe plusieurs images de plusieurs personnes sous Matlab .

1. Environnement du travail

Dans cette section, nous présenterons le matériel et le logiciel utilisés dans notre travail

1.1 Environnement matériel

Le Deep Learning est un domaine avec des exigences en calculs intenses et la disponibilité des ressources (surtout en GPU) dédiés à cette tâche vont fondamentalement influencer sur l'expérience de l'utilisateur car sans ces ressources, il faudra trop de temps pour effectuées sur une machine qui offre des performances acceptables Dont voici les caractéristiques :

Processeur : AMD E1-2500APU with Radeon (TM) HD Graphics 1.40 GHz
RAM : 6GB
Système d'exploitation : Windows 7 Professionnel 64 bits

Tableau 4. 1 Caractéristiques de la machine utilisée

1.2 Logiciel MATLAB :

Entre 1970 et 1990, de nombreux programmes informatiques interactifs sont apparus sur le marché électronique, notamment le programme MATLAB, conçu par « Cleve Moler » à la fin des années 1970.

MATLAB « Matrix Laboratory » est un langage de développement informatique spécialement conçu pour les applications scientifiques, utilisé pour développer des solutions nécessitant une puissance de calcul très élevée, et permettant d'effectuer de multiples simulations basées sur des algorithmes d'analyse numérique [21].

1.3 PhD Tools

La boîte à outils de reconnaissance faciale PhD (Pretty Helpful Development) est une collection de fonctions et de scripts Matlab destinés à aider les chercheurs travaillant dans le domaine de la reconnaissance faciale. La boîte à outils a été produite en tant que sous-produit de mes travaux de recherche et est disponible gratuitement en téléchargement.

La boîte à outils PhD propose des implémentations de plusieurs techniques de reconnaissance faciale populaires, telles que l'analyse des composants principaux, l'analyse discriminante linéaire, l'analyse des composants principaux du noyau ou l'analyse du pêcheur du noyau. En plus de ces techniques, il contient des fonctions pour la construction de filtres Gabor, l'extraction de caractéristiques Gabor, le calcul de congruence de phase et autres. Une partie importante de la boîte à outils est également les outils d'évaluation qui permettent de construire les courbes de performance les plus courantes (par exemple, ROC, DET, CMC, EPC) utilisées pour évaluer les systèmes de reconnaissance faciale.

En plus de ce qui précède, la boîte à outils comprend également un grand nombre de scripts de démonstration qui montrent comment utiliser les fonctions de la boîte à outils dans des expériences de reconnaissance faciale utilisant une vraie base de données. Ces scripts illustrent la procédure complète de création et de test de systèmes de reconnaissance faciale basés sur des filtres de Gabor et des techniques de projection sous-spatiale. [30]

1.4 Description des bases de données utilisées

1.4.1 Base de données ORL

Conçu par AT&T laboratoires de l'université de Cambridge en Angleterre, la base données ORL (Olivetti Research Laboratory) est une base de données de référence pour les systèmes de reconnaissances automatique des visages. En effet tous les systèmes de reconnaissances de visages trouvés dans la littérature ont été testés par rapport à l'ORL, cette popularité est aux nombres de contraintes imposer par cette base car la plus part des changements possibles et prévisibles du visage ont été pris en compte, comme par exemple : le changement de coiffure, la barbe, les lunettes, les changements dans les expressions faciales, *etc*. Ainsi que les conditions d'acquisition telles que : le changement d'illumination et le changement d'échelle dû à la distance entre le dispositif d'acquisition et l'individu. La base de données ORL est constituée de 40 individus, chaque individu possède 10 poses, donc la base contient 400 images. Les poses ont été prises sur des intervalles de temps différents pouvant aller jusqu'à trois mois. L'extraction des visages à partir des images a été

faite manuellement. Nous présenterons dans ce qui suit les figures montré les spécificités de la base de données de référence ORL. [29]

Figure.4.1 : Exemples d'images de visages de la base ORL

1.4.2 Base de données BBA Faces

Conçu par SEHILI Mohamed El-Amine et CHEKHCHOUKH Abdessalem sous la direction de monsieur Akrouf Samir de l'université de Bordj Bou Arreridj .Le modèle suivi est en grande partie emprunté à celui de l'université deYale. Il néanmoins introduit de nouvelles catégories d'images (i.e. *dark*, *toplight* et *bottomlight*). De l'autre côté ils ont écarté les catégories (*centerlight* et *noglasses*)

La base compte 23 personnes avec 12 images (prises, pour la majorité des individus, dans moments différents) pour chacune. Les images reflètent différentes expressions faciales ainsi que des variations de l'intensité et de la source de lumière. Les séances de photographie ont été organisées entre février et mars 2008. Les visages ont été sélectionnés manuellement pour en faire des images de 124 X 92 pixels converties en niveaux de gris et stockées au format jpg. Cette base possède toutefois quelques lacunes; parmi lesquelles on cite: l'absence de personne de sexe féminin, l'âge des personnes est seulement entre 21 et 33 ans. La figure suivante présente un exemple de la base. [33]

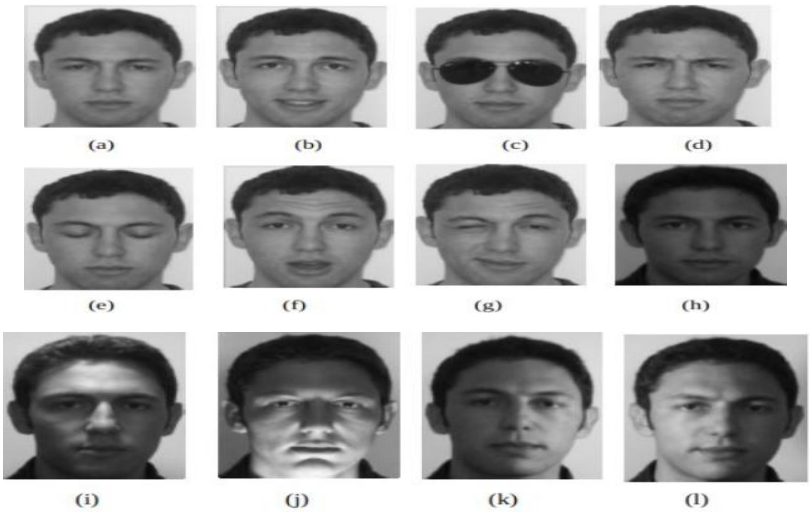


Figure.4.2 : Exemples d'images de visages de la base BBA Faces

(a): normal, (b): happy, (c): glasses, (d): sad, (e): sleepy, (f): surprised, (g): wink, (h): dark, (i): toplight, (j): bottomlight, (k): leftlight, (l): rightlight.

2. Principe d'un système de reconnaissance faciale

Le problème de la reconnaissance faciale est défini tel qu'à partir de l'image du visage, la personne correspondante doit être identifiée. Pour ce faire, il est nécessaire d'obtenir une image de référence (images d'apprentissage) sous la forme d'une base de données de tous les visages connus du système. Chaque image est associée à un vecteur de propriétés qui ne sont pas fixes pour la même personne et varient d'une personne à l'autre. La reconnaissance consiste alors à comparer le vecteur caractéristique du visage à reconnaitre avec chaque vecteur de la base d'apprentissage. Autrement dit, trouver la personne dont le visage est le plus similaire à celui qu'on cherche à identifier.

3. Méthode proposée de reconnaissance faciale

Le système proposé est composé de cinq étapes essentielles la première c'est le prétraitement de l'image ou nous avons utilisés l'autoencodeur. La deuxième étape c'est l'extraction des caractéristiques où nous avons utilisé Gabor, La troisième étape c'est la réduction des caractéristiques avant la classification où nous avons utilisé LDA. La quatrième étape de mise en correspondance (comparaison) nous avons appliqué la distance de Mahalanobis cosins (Mahcos) est utilisée pour l'étape de classification, et la dernière étape c'est l'évaluation des performances.

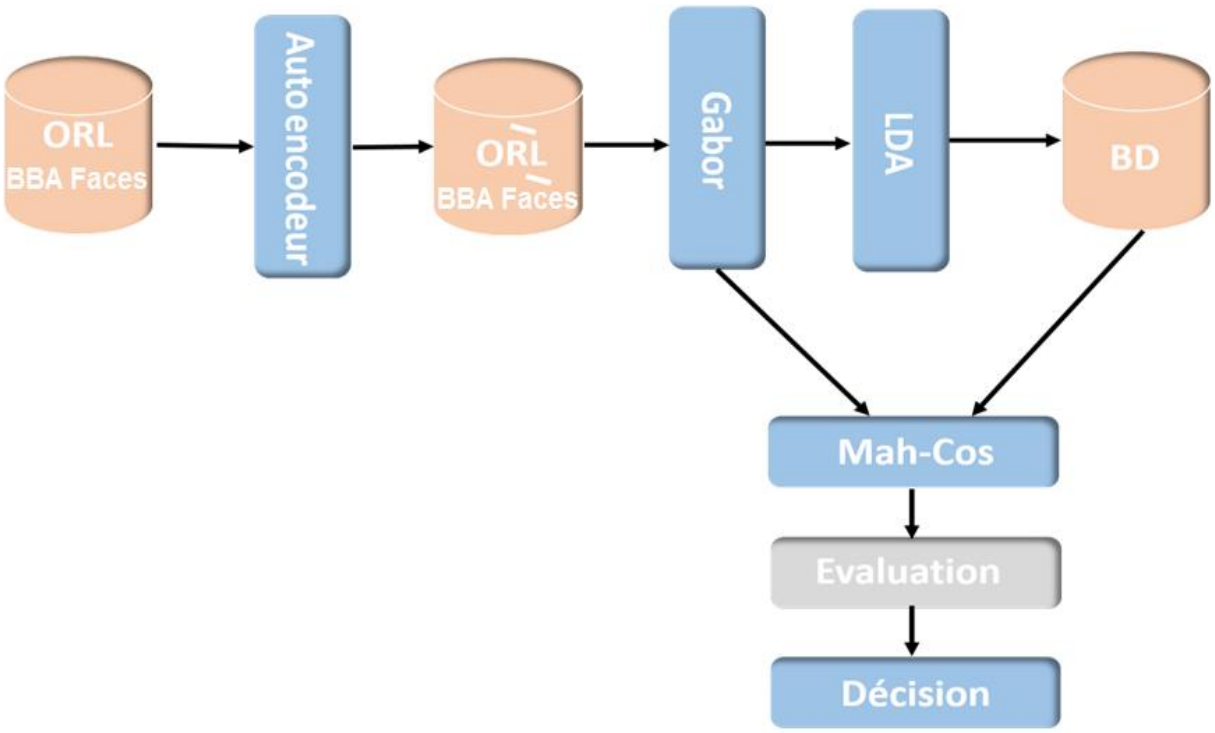


Figure 4.3 : Schéma de réalisation illustre les étapes de travail

4. Partitionnement des images pour l'apprentissage et le test

Dans la série de tests que nous avons effectuée, la base de données était divisée comme suit :

•**Individus :** 40 (ORL) / 23 (BBA Faces).

• Images d'apprentissage :

ORL : cinq images de chaque personne sont utilisées pour la phase d'apprentissage.

BBA Faces : dix images de chaque personne sont utilisées pour la phase d'apprentissage.

• Images de test :

ORL : cinq images de chaque individu ont été utilisées pour la réalisation des différents tests.

BBA Faces : deux images de chaque individu ont été utilisées pour la réalisation des différents tests.

5. Résultats Expérimentaux

5.1 Protocole de test

Dans ces expériences, dans le cas de base ORL, 5 images de la première session, sont utilisées dans la phase d'entrainement. Les autres 5 images de la deuxième session ont été utilisées dans la phase de test. Il y a un total de 200 images d'entrainement et 200 images de test, et dans le cas de base BBA Faces, 10 images de la première session, sont utilisées dans la phase d'entrainement. Les autres 2 images de la deuxième session ont été utilisées dans la phase de test. Il y a un total de 230 images d'entrainement et 46 images de test.

La courbe caractéristique (ROC), qui est un terrain de FRR contre FAR pour tous les seuils possibles, obtenus par l'utilisation de chaque hiddensize et les nombres d'itérations, la courbe des scores cumulés (CMC)).

5.2 Expérimentations

5.2.1 Première expérimentation

Dans un premier temps, nous avons mis en œuvre la méthode Deep Learning grâce à l'autoencodeur pour la phase de prétraitement d'image pour minimiser l'erreur quadratique, en utilisant les formules (3.1), (3.2), (3.3) montré dans le chapitre3.

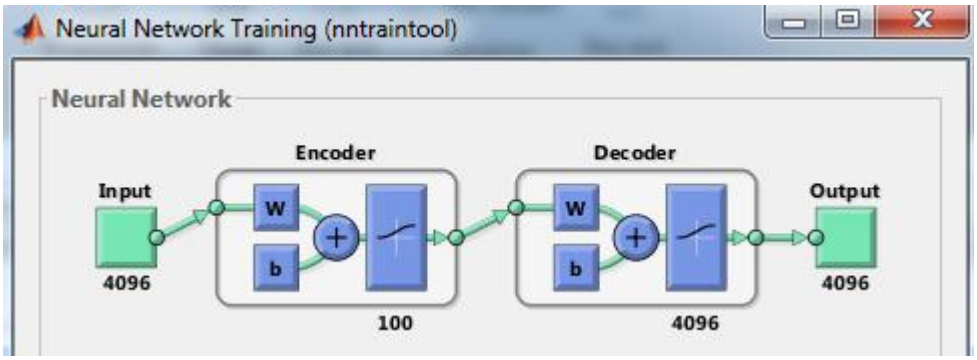


Figure 4.4 : Exemple d'architecture d'un autoencodeur

5.2.2 Deuxième expérimentation

Ensuite, nous continuerons le processus de reconnaissance de visage, on utilisant Gabor,LDA ,Mah Cos, pour faire l'évaluation de performance de système biométrique.

5.3 Les résultats expérimentation obtenus

5.3.1 Première expérimentation

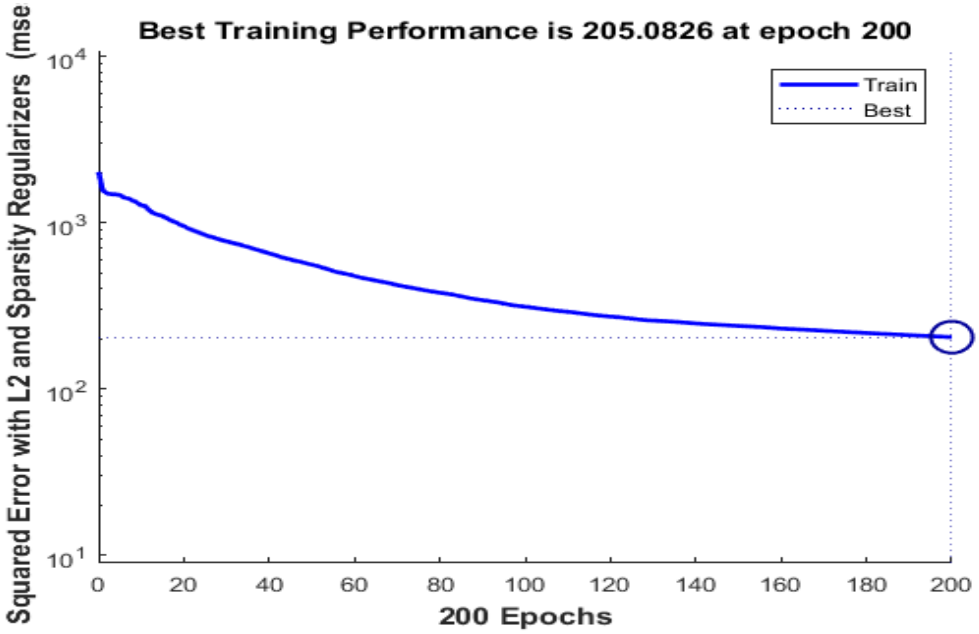


Figure 4.5 : Meilleur performance d'entrainement pour 200 Itérations (Base de données ORL)

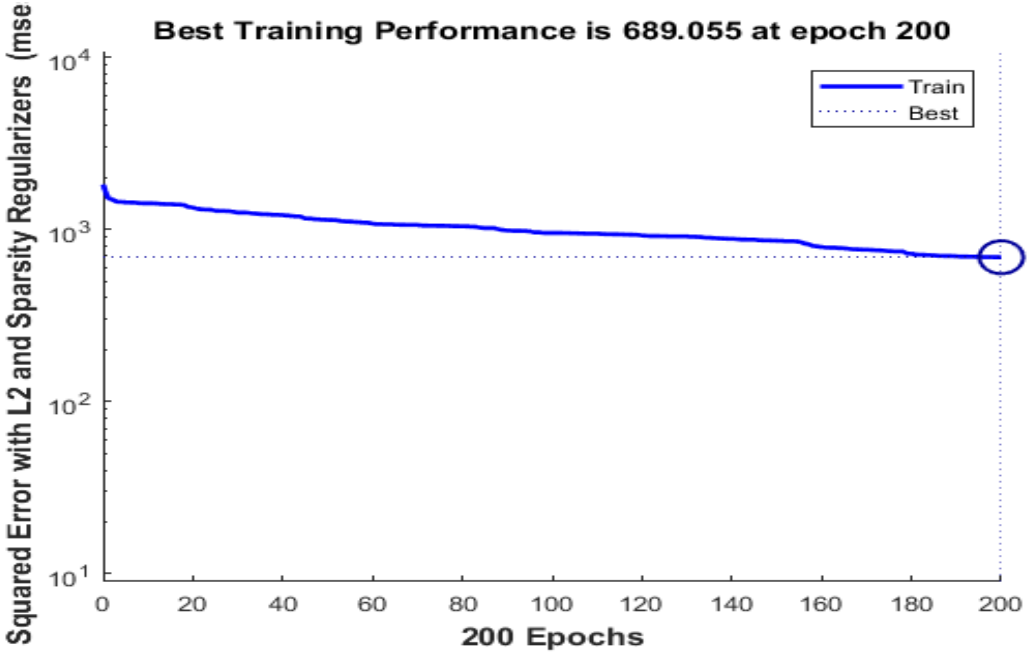


Figure 4.6 : Meilleur performance d'entrainement pour 200 Itérations (Base de données BBA Faces)

D'après les graphes présentés, on obtient un meilleur entrainement de performance égal à 205.0826 dans le cas de base de données ORL dans 200 itérations, et égale à 689.055 dans le cas de base de données BBA Faces dans 200 itérations, qui indique que notre approche atteint une performance presque parfaite.

5.3.2 Deuxième expérimentation

- Sur la base de données ORL

Après les résultats obtenus par les algorithmes autoencodeur, Gabor,LDA avec des itérations différentes 200,300 et 400, les résultats de l'identification et la vérification sont illustrés dans les tableaux ci-dessous.

Hiddensize	Identification	Vérification			
	Rang (%)	EER (%)	Far1%	Far 0.1%	Far 0.01%
200	96.00%	1.28%	98.00%	95.50%	91.50%
250	97.00%	1.28%	97.50%	96.50%	93.00%
270	94.50%	1.01%	99.00%	93.50%	91.00%
300	95.00%	1.00%	99.00%	94.50%	89.00%

Tableau 4.2 : Résultats obtenus par 200 itérations

Hiddensize	Identification	Vérification			
	Rang (%)	EER (%)	Far1%	Far 0.1%	Far 0.01%
200	96.00%	0.96%	99.50%	94.50%	93.50%
250	98.00%	1.50%	98.50%	97.50%	95.00%
270	96.50%	0.94%	99.50%	95.00%	94.00%
300	95.00%	1.00%	99.00%	94.00%	92.50%

Tableau 4.3: Résultats obtenus par 300 itérations

Hiddensize	Identification	Vérification			
	Rang (%)	EER (%)	Far1%	Far 0.1%	Far 0.01%
200	96.00%	1.50%	98.50%	95.00%	92.00%
250	97.50%	1.50%	98.50%	97.00%	94.50%
270	96.50%	1.00%	99.00%	95.50%	93.00%
300	96.00%	1.50%	98.50%	94.50%	91.00%

Tableau 4.4: Résultats obtenus par 400 itérations

Dans ces tableaux il est clair que les caractéristiques obtenues à partir de l'image améliorent considérablement la précision du système.

Deuxièmement, une minimale erreur EER égal à 0.94%,0.96%,1.00%,1.28% ,1.50% ,1.95% vus dans différents itérations ,et un taux de reconnaissance RANG maximal égal à 98.00%,

97.50%,97.00%,96.50%,96.00%,95.50%,95.00% et 93.50%.

- Sur la base de données BBA Faces

Après les résultats obtenus par les algorithmes autoencodeur, Gabor,LDA avec des itérations différentes 200,150 et 100, les résultats de l'identification et la vérification sont illustrés dans les tableaux ci-dessous.

Hiddensize	Identification	Vérification			
	Rang (%)	EER (%)	Far1%	Far 0.1%	Far 0.01%
20	100.00%	0.00%	100.00%	100.00%	0.83%
50	97.50%	0.88%	97.50%	70.83%	0.83%
80	85.00%	6.67%	75.83%	2.50%	0.83%
100	85.00%	4.86%	77.50%	40.83%	0.83%

Tableau 4.5: Résultats obtenus par 200 itérations

Hiddensize	Identification	Vérification			
	Rang (%)	EER (%)	Far1%	Far 0.1%	Far 0.01%
20	100.00%	0.00%	100.00%	100.00%	0.83%
50	99.17%	0.65%	100.00%	97.50%	0.83%
80	92.50%	3.33%	88.33%	13.33%	0.83%
100	90.00%	4.17%	89.15%	55.00%	0.83%

Tableau 4.6: Résultats obtenus par 150 itérations

Hiddensize	Identification	Vérification			
	Rang (%)	EER (%)	Far1%	Far 0.1%	Far 0.01%
20	100.00%	0.00%	100.00%	100.00%	0.83%
50	100.00%	0.00%	100.00%	100.00%	0.83%
80	93.33%	1.67%	95.83%	54.17%	0.83%
100	94.17%	2.64%	95.83%	65.00%	0.83%

Tableau 4.7: Résultats obtenus par 100 itérations.

Dans ces tableaux il est clair que les caractéristiques obtenues à partir de l'image améliorent considérablement la précision du système.

Deuxièmement, une minimale erreur EER égal à 0.00%,0.65%,0.88%,1.67%,2.64%,3.33% 4.17%,4.86% et 6.67% vus dans différents itérations ,et un taux de reconnaissance RANG maximal égal à 100.00%,99.17%,97.50%,94.17%,93.33%,92.50%,90.00% et 85.00%.

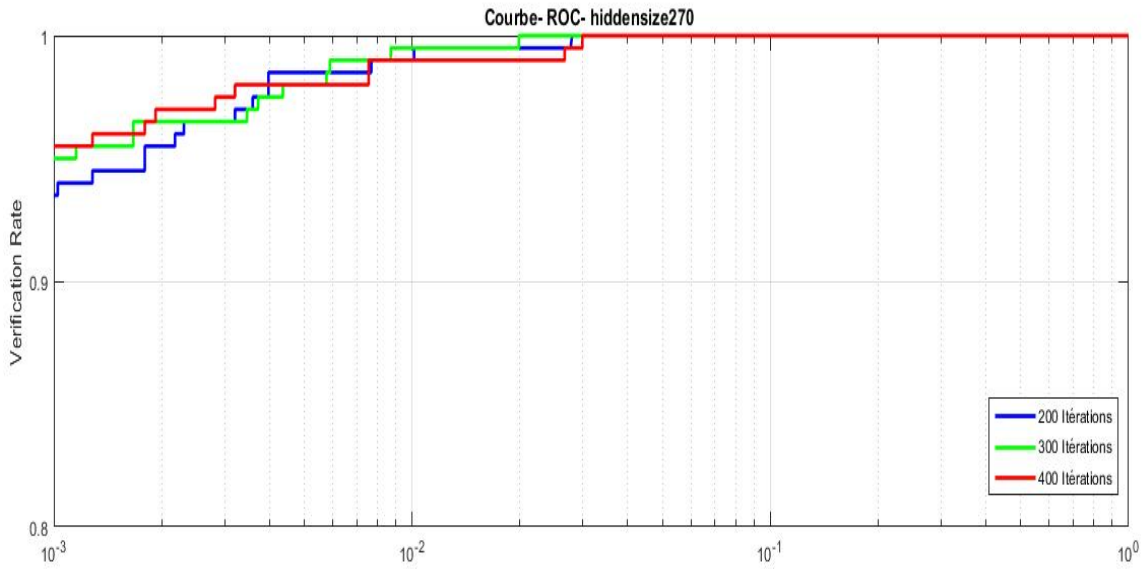


Figure 4.7: Courbe ROC avec hiddensize270 (Base de données ORL)

- Dans le cas de base de données ORL, les courbes ROC pour les différentes itérations montrent que le système donne une haute précision à l'itération 300 avec un hiddensize égal à 270 par rapport aux autres itérations (200,400). Ainsi que, dans ce cas, un FAR (1%) égal à 99.50% avec minimale erreur EER égal à 0.94%.

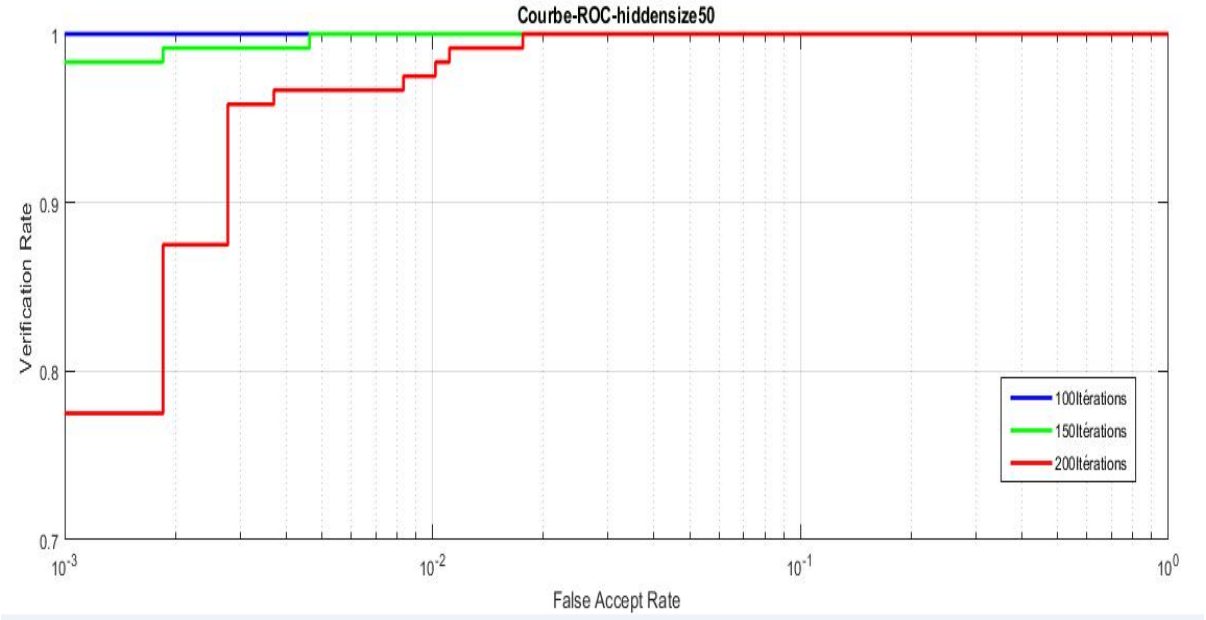


Figure 4.8 : Courbe ROC avec hiddensize50 (Base de données BBA Faces)

- Dans le cas de base de données BBA Faces, les courbes ROC pour les différentes itérations montrent que le système donne une haute précision à l'itération 200 par rapport aux autres

itérations (100,150). Ainsi que, dans ce cas, un FAR (1%) égal à 100% avec minimale erreur EER égal à 0.00%.

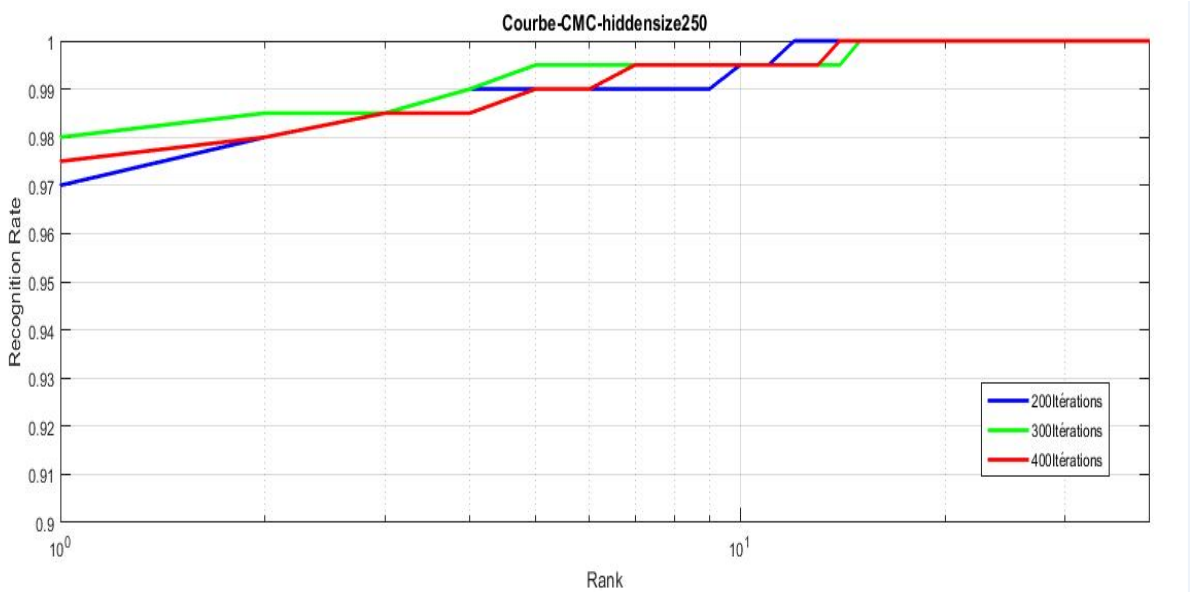


Figure 4.9 : Courbe CMC avec hiddensize250 (Base de données ORL)

- Dans le cas de base de données ORL, les courbes CMC pour les différentes itérations montrent que le système donne une haute précision à l'itération 300 avec un hiddensize égal à 250 par rapport aux autres itérations (200,400). Ainsi que, dans ce cas, le taux de reconnaissance de RANG égale à 98.00%.

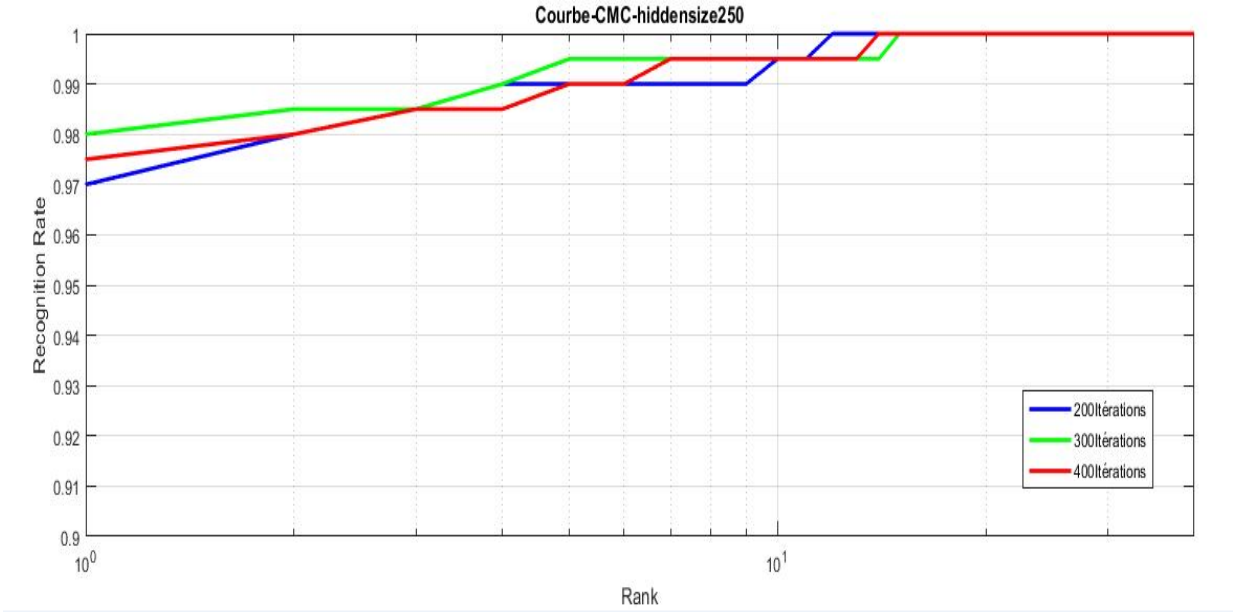


Figure 4.10 : Courbe CMC avec hiddensize50 (Base de données BBA Faces)

- Dans le cas de base de données BBA Faces, les courbes CMC pour les différentes itérations montrent que le système donne une haute précision dans toutes les itérations avec un hiddensize égal à 20 et dans l'itération100 avec un hiddensize égal à 50. Ainsi que, dans ces cas, le taux de reconnaissance de RANG égale à 100.00%.

Conclusion

Dans ce chapitre, nous concluons que notre système d'identification biométrique des personnes est fiable vu que les résultats obtenus sont satisfaisants, il permet une bonne séparabilité des classes clients et imposteurs. Nous avons étudié l'ensemble des tests effectués ce qui a permis de conclure, qu'avec l'utilisation du Deep Learning nous avons apporté une amélioration considérable du RANG et du EER et des deux taux d'erreurs FAR et FRR.

CONCLUSION GENERALE

Ce travail s'inscrit dans le domaine de la reconnaissance biométrique. Celle-ci consiste à vérifier l'identité d'une personne à partir de son image. Utilisés principalement pour des raisons de sécurité et/ou de confidentialité, le système de reconnaissance de visage qui est de plus en plus présente pour accéder à un certain endroit privé.

L'objectif de ce travail était de réaliser un système d'identification biométrique des personnes par reconnaissance de visage basé sur le deep Learning. Après avoir dressé un état de l'art en biométrie et la sécurité d'information et les différentes technologies biométriques, nous avons présenté le système de reconnaissance de visage ou nous avons détaillé les étapes de la reconnaissance de visage et les méthodes de reconnaissance de visage avec les principales difficultés de la reconnaissance de visage, par la suite nous avons fait des rappels sur les réseaux de neurones et l'intelligence artificielle, nous avons défini le deep Learning et les différentes architectures. Pour réaliser notre travail de reconnaissance de visage on a utilisé l'auto encodeur, la méthode d`apprentissages profonds qui a montré ses performances ces dernières années et nous avons choisi Gabor comme méthode d'extraction des caractéristique et LDA pour la réduction des dimensions.

Les résultats obtenus montrent l'efficacité de l'autoencodeur pour l'identification des personnes avec un taux d'erreur EER minimal de 0.00% dans la vérification et un RANG maximal égal à 100% dans identification pour les images.

D'après l'étude effectuée, on peut conclure que le Deep Learning a donné une performance remarquable dans les deux applications traitées identification et vérification par la reconnaissance de visage. Comme perspectives nous pouvons citer :

- Implémentation des techniques qui font le succès des modèles qui participent au challenge Imagenet (ResNet.)
- Tester sur de nouvelles bases de données.
- Combiner avec d'autres modalités tel que : iris, oreille, la voix, etc.

BIBLIOGRAPHIES

[1] Nait-Ali,Régis fournier.A, «Traitement du signal et de l'image pour biométrie»,Livre, Lavoisier, 2012.

[2]. Moulay. M, Arbaoui. M, « Authentification des personnes par l'articulation du doigt », Thèse de Master en génie électrique, Université Kasdi Merbah de Ouargla, 2015.

[3] John. D, Woodward. Jr, Christopher Horn, Julius Gatune, and Aryn Thomas,«Biometrics A Look at Facial Recognition», Livre, RAND Corporation , 2003.

[4] BOUDJELIAL.S, « Détection et identification d'individu par méthode biométrique » Thèse de Magister en Electronique, Université Mouloud Mammeri de Tizi-Ouzou, 2014

[5] Meraoumia. A, « Modèle de Markov caché applique à la multi biométrie », Thèse de Doctorat en électronique,Université des sciences et de la technologie Houari Boumediene 2014

[6] F.Perronnin ,J.Dugelay, «An Introduction to Biometrics Audio and Video-Based Person Authentification», Livre, Crans montana,1997

[7] Belahcen. M « Système de reconnaissance de visage », Thèse de Master en informatique, Université de Biskra, juin 2013.

[8] Ghali. A « Amélioration de la reconnaissance par le visage », Thèse de Magister en informatique, Université Mohamed Boudiaf Oran, 2015.

[9] Ghoulia. B, Kouidri. Y « Etude comparative d'ensemble des descripteurs de texture pour la reconnaissance de visages », Thèse de master en génie électrique, Université Kasdi Merbah Ouargla, 2017.

[10] Djedi. S, « Etude comparative de PCA et KPCA associées au SVM en biométrie », Thèse de Doctorat en informatique, Université Mohamed Khider Biskra, 2012.

[11] Boudjellal. S, « Détection et identification de personne par méthode biométrique », Thèse de Magister, Université Mouloud Mammeri, 2017.

[12] Moad. B, Benmohamed.M, « Méthodes d'identification et de reconnaissance de visages en temps réel basées sur AdaBoost, Article, page 2-3,2005

[13] A. Sofiane, « Détection et identification de personne par méthode biométrique », Thèse de Magister en Electronique.

[14] Wikipédia, www.fr.wikipedia.org, consultée le : 05 janvier 2019.

[15] Diallo.N « La reconnaissance des expressions faciales », Thèse de Master en informatique, Université 8 Mai 1945 de Guelma, 2019

[16] Moualek Djaloul.Y, « Deep Learning pour la classification des images », Thèse de Master en informatique, Université de Tlemcen, Algérie, 2017.

[17] Hub. packtpub, https.www.hub.packtpub.com/top-5-deep-learning- architectures/ consultée le : 15/12/2019

[18] Biométrie-online, www.biometrie-online.net/biometrie/ le-marche, consulté le 31/05/2020

[19] Mémoireonligne, www.memoireonline.com/03/15/8967/m_Conception-et-mise-en-place-dune-plateforme-de-securisation-par-synthese-et-reconnaissance-biom3.html,consultée le 31/05/2020

[20] Guerroudj. B, BRAHMIN .M « Implémentation d'un système de reconnaissance de visages à base de PCA » Thèse de Master en télécommunications, Université Djilali Bounaama Khemis Miliana ,2018

[21] Ouamane.H, « Identification de reconnaissance faciale avec des expressions, » Thèse de Master en électronique, Université de Mohamed Kheider, Biskra, 2012

[22] Benatia. Y, « Deep Auto-Encodeur pour la Reconnaissance de Visage », Thèse de Master en informatique, Université Mohamed Khider », BISKRA, 2019

[23] Djerioui.M, « Contribution au Développement de Systèmes Multicapteurs Intelligents Dédiés à la Surveillance et au Contrôle de la Qualité des Eaux Propres », Thèse de Doctorat en électronique, Université de M'sila, 2019.

[24] Studytonighit, https://www.studytonight.com/post/machine-learning-versus-deep-learning consultée le 01/06/2020

[25] Germain.M, Made.A, «Masked autoencoder for distribution estimation.
in International Conference on Machine Learning», Article, Actes de la 32e Conférence internationale sur l'apprentissage automatique, JMLR W&CP 37: 881-889, 2015

[26] Y. Zhang, «A Better Autoencoder for Image : Convolutional Autoencoder. », Article, Australian National University ACT 2601,2018.

[27] Labiad.A, « Sélection des mots clés basée sur la classification et l'extraction des règles d'association », Thèse de Master en informatique, Université du Québec à Trois-Rivières, 2017.

[28] Christian.G, « Apprentissage profond », Cours en ligne, Université de LAVAL, 29 novembre 2017.

[29] BouKerrouche. Y, Zerriouh. A, « Mise au point d'une application de reconnaissance faciale », Thèse de Master en informatique, Université Abou Bakr Belkaid – Tlemcen 2013

[30] Mathworks, www.fr.mathworks.com/matlabcentral/fileexchange/35106-the-phd-face-recognition-toolbox?s_tid=srchtitle consultée le 03/03/2020

[31] Anis Chaari. «Nouvelle approche d'identification dans les bases de données biométriques basée sur une classification non supervisée". Thèse de Doctorat, Université d'Evry-Val d'Essonne, 2009.

[32] BELHADJ. S, « Détection automatique des crises d'épilepsie », Thèse de Doctorat, Université des sciences et de la technologie Houari Boumediene ,2019

[33] AKROUF, Samir, SEHILI, Med Amine, CHAKHCHOUKH, Abdesslem, et al. Face recognition using PCA and DCT. In : 2009 Fifth International Conference on MEMS NANO, and Smart Systems. IEEE, 2009. p. 15-19.

الملخص

يعد التعرف التلقائي على الوجوه أحد أهم مجالات القياسات الحيوية، فهو يعتمد على التعرف على الأفراد الذين يستخدمون الوجه باعتباره السمة الرئيسية.هذا المجال نشط للغاية، ويرجع ذلك بلا شك إلى تعدد وتنوع مجالات التطبيق، والتي يمكن للمرء أن يقتبس منها: الشركات الحكومية، وشركات الأمن، والتفاعل بين الإنسان والآلة، والرؤية عن طريق الكمبيوتر.
البحث في هذا المجال متعدد وقد تم اقتراح العديد من الأساليب، مثل: التعلم العميق
في هذا العمل، استخدمنا إحدى بنى التعلم العميق (التشفير التلقائي) لبناء تمثيل جديد لمجموعة البيانات لنمذجة نظام القياسات الحيوية بمستوى عالٍ من تجريد البيانات بفضل البنى المفصلية للتحولات غير الخطية المختلفة. وبالفعل حصلنا على نتائج جيدة وقمنا بإجراء العديد من التحسينات من خلال إجراء العديد من التعديلات للحصول على أفضل النتائج
الكلمات الرئيسية: التعرف التلقائي على الوجوه، التعلم العميق، التشفير التلقائي، نظام القياسات الحيوية

Abstract

Automatic face recognition is one of the most important fields of biometrics, it is based on the recognition of individuals using the face as the main characteristic.This field is very active, this is undoubtedly due to the multiplicity and variety of fields of application, including: government companies, security companies, human-machine interaction and computer vision. Research in this area is numerous and several approaches have been proposed, such as:
Deep Learning
In this work, we used one of the deep Learning architectures (autoencoder) to build a new representation of a dataset to model the biometric system with a high level of data abstraction thanks to articulated architectures of different nonlinear transformations. Indeed, we got good results, and we made several improvements by making several modifications to obtain the best results.
Keywords: Automatic face recognition, Deep Learning, autoencoder, biometric system.

Résumé

La reconnaissance automatique des visages est l'un des plus importants domaines de la biométrie, elle se base sur la reconnaissance des individus en utilisant le visage comme principale caractéristique. Ce domaine est très actif, ceci est sans doute dû à la multiplicité et la variété des champs d'application, dont on peut citer : les compagnies gouvernementales, les sociétés sécuritaires, l'interaction homme-machine et la vision par ordinateur. Les recherches dans cet axe sont nombreuses et plusieurs approches ont été proposées, tel que **:**
DeepLearning (L'apprentissage profond).
Dans ce travail, on a utilisé l'une des architectures du deep Learning (auto encodeur) pour construire une nouvelle représentation d'un jeu de données pour modéliser le système biométrique avec un haut niveau d'abstraction des données grâce à des architectures articulées de différentes transformations non linéaires. En effet, nous avons obtenu de bons résultats, et nous avons apporté plusieurs améliorations en apportant plusieurs modifications pour obtenir les meilleurs résultats.
Mots clés : La reconnaissance automatique des visages, Deep Learning, L'apprentissage profond, autoencodeur, le système biométrique.