



جامعة العربي التبسي - تبسة  
Université Larbi Tébessi - Tébessa

République Algérienne Démocratique et Populaire  
Ministère de l'enseignement supérieur et de la  
recherche scientifique

Université Larbi Tébessi - Tébessa

Faculté des Sciences Exactes et des Sciences de la Nature et de la Vie  
Département : Mathématiques et Informatique



كلية العلوم الدقيقة وعلوم الطبيعة والحياة  
FACULTÉ DES SCIENCES EXACTES  
ET DES SCIENCES DE LA NATURE ET DE LA VIE

Mémoire de fin d'études

En vue de l'obtention du diplôme de **MASTER**

**Domaine** : Mathématiques et Informatique

**Filière** : Informatique

**Option** : Systèmes et Multimédia

Thème

# L'apprentissage profond pour la vérification des signatures

Présenté Par :

**Yousfi Douaâ**

Devant le jury :

Dr. Lakhdar Laimeche	MCB	Université Larbi Tébessi - Tébessa	Président
Dr. Ahmed Zeggari	MCB	Université Larbi Tébessi - Tébessa	Examineur
Mr. Ismail Hadjadj	MAA	Université Larbi Tébessi - Tébessa	Encadreur
Dr. Abdeljalil Gattal	MCA	Université Larbi Tébessi - Tébessa	Co-Encadreur

Date de soutenance : 23 Juin 2019

# Remerciement

*Après avoir remercié énergiquement ALLAH le tout puissant de nous avoir donné la force, la patience et le courage pour la réalisation de notre travail, que nous espérons avoir mené à bonne fin.*

*Je tiens à exprimer mes profonds remerciements à mon encadreur Mr Hadjadj Ismail et Co-Encadreur Mr Gattal Abdeljalil, pour les encadrement, la confiance et pour le soutien qu'ils m'ont apportés durant tout ce travail.*

*Leurs compétences scientifiques ont toujours été sources d'enrichissement qui me permettant de faire à bien ce travail. Merci pour tous vos conseils et votre patience.*

*Un grand merci à tous les membres du Jury qui me font l'honneur d'accepter de juger mon travail.*

*Je remercie tous les enseignants et les étudiants du département d'informatique de l'Université de Tébessa, en particulier la spécialité "Système et Multimédia".*

*Je voudrais aussi présenter mes remerciements à mes parents pour tous leurs sacrifices en faveur de nos éducations, ma famille et mes amis pour leur support qui j'ai été autorisé à de travailler dans les meilleures conditions.*

## *Résumé :*

Le travail présenté de ce mémoire de fin d'étude consiste à proposer un modèle basé sur les réseaux de neurones de convolution (**CNN**) pour la vérification de signature hors ligne indépendante de signataire (**WI-OSV**).

Le modèle proposé constitué de onze (**11**) couches dont 5 couches de convolution en alternatifs avec 5 autres couches de pooling en finissons par un dernier couche de type entièrement connectée. La base de données ICDAR 2011 sigComp est utilisée pour l'ensemble d'expérimentations et pour la validation de modèle.

---

**Mots-clés:** Réseaux de neurone convolutif (CNN), vérification de la signature.

## *Abstract:*

The work presented in this thesis consists in proposing a model based on convolution neural networks (CNN) for the verification of writer independent offline signature verification (**WI-OSV**).

The proposed model consisting of eleven (11) layers including 5 convolution layers in alternating with 5 other pooling layers ending with a last layer of a fully connected type. The ICDAR 2011 sigComp database is used for the set of experiments and for model validation.

---

**Keywords:** convolution neural networks (CNN), signature verification.

## المخلص :

يتكون العمل المقدم في هذه الأطروحة النهائية من اقتراح نموذج يعتمد على شبكات الخلايا العصبية التلافيفية (CNN) للتحقق من التوقيع غير متصل بالانترنت المستقل عن التوقيع (WI-OSV).

يتكون النموذج المقترح من أحد عشر (11) طبقة بما في ذلك خمس طبقات تلافيفية بالخلف مع خمس طبقات أخرى من التجميع وأخيراً طبقة نهائية من النوع المتصل بالكامل . يتم استخدام قاعد بيانات ICDAR 2011 sigComp لمجموعة من التجارب والتحقق من النموذج.

---

الكلمات المفتاحية: شبكات الخلايا العصبية التلافيفية (CNN) ، التحقق من التوقيع.

---

---

# TABLE DES MATIÈRES

---

---

Introduction générale .....	I
Chapitre 01 : Inroduction à la biométrie et la vérification de la signature	
1. Biométrie .....	1
1.1. Définition .....	1
1.2. Modalités biométriques .....	1
1.2.1. Modalités morphologiques (physiologiques) .....	1
1.2.1.1. L’empreinte digitale .....	2
1.2.1.2. La reconnaissance de visage .....	2
1.2.1.3. L’iris .....	3
1.2.1.4. Géométrie de la main .....	3
1.2.2. Modalités comportementale .....	4
1.2.2.1. La signature .....	4
1.2.2.2. La voix (Reconnaissance vocale) .....	5
1.2.2.3. Dynamique de la frappe au clavier .....	5
1.2.2.4. La démarche .....	6
2. La vérification de la signature .....	6
2.1. Type de falsification .....	7
3. Processus d’un système de la vérification de signature .....	8
3.1. L’acquisition des données.....	8
3.2. Prétraitement de l’image.....	10
3.2.1. La binarisation .....	11
3.2.2. Le lissage (Filtrage) .....	11
3.2.3. Amélioration d’image .....	12
3.3. Ségmentation.....	12
3.4. Extraction de caractéristiques .....	13
3.4.1. Caractéristiques globales .....	13
3.4.2. Caractéristiques locales .....	13
3.5. Classification.....	13
4. Présentation de certaines techniques de la classification .....	14
4.1. K-plus proche voisin (KNN) .....	14
4.3. Machine à Vecteur Support (SVM) .....	14
Conclusion .....	14

## Chapitre 02 : L'apprentissage profond (Deep Learning)

1. Réseaux de Neurones Artificiels (RNA) .....	16
1.1. Perceptron .....	16
1.2. Perceptron MultiCouche (PMC) .....	17
2. Définition du l'apprentissage profond (Deep Learning) .....	17
3. L'architecture de l'apprentissage profond.....	17
3.1. Réseaux Neurones Convolutif (RNC) .....	17
3.1.1. Définition de RNC.....	18
3.1.2. L'architecture de RNC.....	18
3.1.2.1. La couche de convolution (CONV) .....	19
3.1.2.2. La couche de pooling (POOL) .....	19
3.1.2.3. La couche correction (Rectified Linear Unit (ReLU)) .....	20
3.1.2.4. La couche entièrement connecté (Fully connected (FC)) .....	20
3.1.2.5. La couche de perte(LOSS) .....	21
3.2. Réseaux de Neurones Récurrents (RNR) .....	21
3.3. Mémoire à long terme à court terme (LSTM) .....	21
3.4. Machine de Boltzmann Profonde (MBP) .....	22
Conclusion : .....	22

## Chapitre 03 : Vérification de signature avec CNN

1. Les travaux ultérieurs .....	23
1.1. CNN et MLP pour la vérification de signature Persan (Khalajzadeh <i>et al.</i> (2012)) .....	23
1.2. CNN basé sur VGG16 pour la vérification de signature hors ligne (Alvarez <i>et al.</i> (2016)).....	24
1.3. CNN pour détecter et réduire la falsification des signatures (Cozzens <i>et al.</i> (2017)).....	24
1.4. Ad hoc models CNN pour La vérification de signature (Multu Yapici <i>et al.</i> (2018)).....	25
1.5. CNN et AE pour de vérification signatures dynamique (Man <i>et al.</i> (2018)) .....	25
1.6. CNN et SVM pour la vérification de signature manuscrite hors ligne (Bhanu Sronothara <i>et al.</i> (2018)) .....	26
2. Comparaison des travaux .....	27
Conclusion .....	27

## Chapitre 04 : Méthode proposé et Résultats expérimentaux

1. Présentation des outils de développement .....	28
1.1. Matériel .....	28
1.2. Python .....	28
1.3. Google Colab .....	28
1.4. TensorFlow .....	29
2. Méthode proposée pour la vérification des signatures .....	29
2.1. Base de données .....	29
2.1.1. Présentation de la base de données .....	29
2.1.2. Acquisition de données .....	30
2.2. Prétraitement .....	31
2.2.1. Conversion d'image en niveaux de gris .....	31
2.2.2. Redimensionnement de l'image .....	31
2.3. L'architecture de CNN .....	32
3. Résultats et comparaison les travaux .....	35
Conclusion.....	35
Conclusion générale .....	36
Référence bibliographie .....	37

---

## LISTE DES ILLUSTRATIONS

---

Figure 1.1: Images de l’empreinte digitale.....	2
Figure 1.2: Image visage. ....	3
Figure 1.3: Image Iris.....	3
Figure 1.4: Image Géométrie de main .....	4
Figure 1.5: Différentes signatures de (ICDAR2011).....	4
Figure 1.6: Image de la Reconnaissance vocale .....	5
Figure 1.7: Image de la frappe au clavier .....	5
Figure 1.8: Images sur la démarche .....	6
Figure 1.9: Les différents types de falsification .....	7
Figure 1.10: Processus d’un système de la vérification de signature .....	8
Figure 1.11: Signature hors ligne (statique) .....	9
Figure 1.12: Signature en ligne (dynamique).....	9
Figure 1.13: Prétraitement de la signature .....	10
Figure 1.14: Image binarisée .....	11
Figure 1.15: Exemple de lissage.....	11
Figure 1.16: Amélioration d’image .....	12
Figure 1.17: Ségmentation d’image.....	12
Figure 2.1: La relation entre IA, ML et DL.....	15
Figure 2.2: Réseaux de neurones artificiels.....	16
Figure 2.3: Modèle du perceptron.....	16
Figure 2.4: Perceptron MultiCouche.....	17
Figure 2.5: L’architecture de CNN L’architecture de CNN.....	18
Figure 2.6: Représentation de la fonctionnalité Convolution.....	19
Figure 2.7: Max pooling avec un filtre $2 \times 2$ et un pas de 2 .....	20
Figure 2.8 :Représentation de la fonctionnalité FC .....	20
Figure 2.9: Réseaux de neurones récurrents.....	21
Figure 4.1: Exemples de signatures de la base de données ICDAR 2011 .....	30
Figure 4.2: Exemple de la signature hors ligne .....	30
Figure 4.3: Proposition de CNN pour la vérification de la signature .....	32

---

## LISTE DES TABLEAUX

---

Table 3.1: Principaux travaux de recherche dans le domaine vérification de la signature .....	27
Table 4.2: Couches du CNN.....	34
Table 4.2: Comparaison de différents travaux .....	35

---

# **Introduction générale**

---

### **Introduction générale :**

L'authentification biométrique est le processus de vérification de l'identité des individus en fonction de leurs caractéristiques biologiques uniques. C'est devenu un standard pour l'accès aux systèmes de haute sécurité. Les méthodes actuelles d'apprentissage profond (Deep Learning (DL)) ont permis d'automatiser de manière fiable bon nombre de ces tâches (reconnaissance de visage, empreinte digitale, reconnaissance de l'iris), parmi les nombreuses tâches utilisées pour l'authentification biométrique est la vérification de signature, qui vise à déterminer si la signature donnée est authentique ou falsifiée.

La vérification de la signature est une caractéristique importante de la biométrie, principalement parce qu'elle est largement utilisée pour vérifier l'identité d'une personne et empêcher la contrefaçon de documents dans de nombreux domaines juridiques, financiers, commerciaux et administratifs.

Un système de vérification contournerait, a priori, toutes ces difficultés. La vérification des signatures serait idéalement rapide et efficace, et réduirait de manière significative les risques de contrefaçon. Plusieurs systèmes ont été développés à ce jour afin d'automatiser la vérification des signatures et on peut diviser ces méthodes en deux classes suivant le mode d'acquisition de l'image des signatures: en-ligne et hors-ligne.

Dans le cas en-ligne (On-Line), la signature est capturée à l'aide d'un périphérique de saisie spécial (un disque numérique connecté à un ordinateur, par exemple). Cette méthode vous permet d'utiliser des informations dynamiques telles que la vitesse, la position, la pression et / ou l'inclinaison du stylet, Ces systèmes ne peuvent pas être utilisés pour vérifier des signatures déjà apposées sur des documents (chèques bancaires par exemple).

Inversement, lors du contrôle de la signature en mode hors-ligne (Off-Line), la signature est obtenue une fois le processus d'écriture terminé, en numérisant un document contenant la signature et en le représentant sous la forme d'une image numérique. Les informations dynamiques sur la création de signature (telles que la position du stylo et la vitesse dans le temps) sont perdues, ce qui rend le problème très difficile.

## INTRODUCTION GENERALE

Dans ce projet, nous visons à établir un système de vérification de signature utilisant un Réseau de Neurones Convolutif (CNN), afin d'améliorer le taux de la vérification. Nous avons discuté des notions fondamentales des réseaux de neurones convolutif. Notre travail a été validé sur la base de données ICDAR2011.

### **Objectifs principaux de mon travail:**

- ❖ Etat de l'art sur différentes méthodes de vérification de la signature.
  
- ❖ L'objectif du travail est l'évaluation des performances du système de vérification de la signature en utilisant le principe d'apprentissage profond. L'évaluation est réalisée sur la base de données de la compétition ICDAR 2011.

### **Organisation du mémoire:**

Pour bien présenter le travail on le divise en quatre chapitres principaux :

Le premier chapitre contient une généralité sur la biométrie et définit ce qu'est la vérification de signature en général, et puis définit le processus d'un système de la vérification de signature et présentation de certaines techniques de la classification (SVM, KNN).

Le deuxième chapitre est consacré à l'apprentissage profond (deep learning), une description plus détaillée et les cinq étapes principales d'opérations sur les réseaux de neurones convolutifs (CNNs) qui est la méthode choisie dans notre projet.

Dans le troisième chapitre, nous présentons les différents travaux pour la vérification de signature avec CNN.

Dans le dernier chapitre, un modèle basé sur les Réseau de neurones convolutifs est présenté, où un ensemble d'expérimentation sont faites sur la base de données ICDAR2011.

Enfin nous terminerons ce mémoire par une conclusion générale et perspective pour les futurs travaux.

# **Chapitre 01**

---

**Introduction à la biométrie**

**et**

**la vérification de la signature**

---

Un système biométrique est un système de reconnaissance de formes qui utilise les données biométriques d'un individu. Les systèmes biométriques sont de plus en plus utilisés depuis quelques années. Nous introduirons dans ce chapitre quelques notions et définitions de base liées à la biométrie. Et nous insisterons surtout sur la vérification de la signature, car elle constitue l'objectif de ce thème.

## **1. Biométrie :**

### **1.1. Définition :**

Le mot « biométrie » venant du grec « *bios* » (vie) et de « *metron* » (mesure) [27]. Il désigne dans un sens très large l'étude quantitative des êtres vivants. [1]

En général un système biométrique est un système automatique de mesure basé sur la reconnaissance de caractéristiques physique propres à un individu (l'empreinte digitale, la géométrie de la main, l'iris, la reconnaissance de visage, la voix, la signature, etc...), diviser en deux modalité principale: Morphologiques et comportementale.

Pour que les caractéristiques, propre à chaque individu, puissent être qualifiées de modalités biométriques, elles doivent être :

- Universelles (existent chez tous les individus).
- Uniques (possibilité de différencier un individu par rapport à un autre).
- Permanentes (doit être invariante dans le temps).
- Enregistrables (possibilité d'enregistrer les caractéristiques d'un individu avec son accord).
- Mesurables (possibilité de comparaisons futures).

### **1.2. Modalités biométriques :**

Il existe plusieurs modalités biométriques utilisées dans divers secteurs, on peut distinguer deux catégories :

#### **1.2.1. Modalités morphologiques (physiologiques):**

Elles sont basées sur l'identification des traits physiques particuliers pour chaque personne.  
On cite :

### 1.2.1.1. L’empreinte digitale :

L’identification à l’aide des empreintes digitales est l’une des première techniques biométriques qui se base sur le fait que chaque personne à des empreintes uniques. Les lecteurs d’empreintes digitales scannent puis relèvent des éléments permettant de différencier les empreintes. Statistiquement il est impossible de trouver douze points identiques chez deux individus.

Ce type de système est utilisé par les institutions financières pour leurs employés et leurs clients. Il se retrouve également dans les hôpitaux, les écoles, les aéroports, les cartes d’identité, les passeports, les permis de conduire et de nombreuses autres applications. [2]

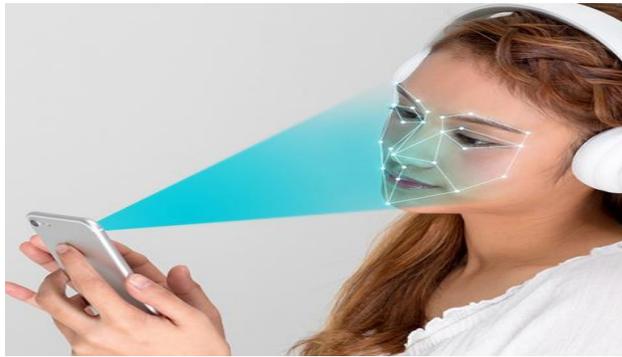


**Figure 1.1:** Images de l’empreinte digitale

### 1.2.1.2. La reconnaissance de visage :

Le visage est certainement la caractéristique biométrique que les humains utilisent le plus naturellement pour s’identifier entre eux. Le système d’acquisition est soit un appareil photo, soit une caméra numérique.

La difficulté de la reconnaissance de visage varie énormément suivant que l’acquisition se fait dans un environnement contrôlé ou non. Dans un environnement contrôlé, des paramètres tels que l’arrière plan, la direction et l’intensité des sources lumineuses, l’angle de la prise de vue, la distance de la caméra au sujet sont des paramètres maîtrisés par le système. Dans un environnement non-contrôlé, une série de prétraitements sont souvent nécessaires avant de faire la reconnaissance à proprement parler. Il faut tout d’abord détecter la présence ou l’absence de visage dans l’image (face détection). Le visage doit ensuite être segmenté (face segmentation).[3]



**Figure 1.2:** Image visage.

### 1.2.1.3. L'iris :

La reconnaissance par l'iris est très utilisée dans les applications d'identification et de vérification suite à stabilité de sa forme, plus distinctive, et unique. Elle est extrêmement fiable mais les équipements d'acquisition sont coûteux. L'acquisition de l'iris est effectuée au moyen d'une caméra pour pallier aux mouvements inévitables de la pupille. Elle est très sensible (précision, reflet...) et relativement désagréable pour l'utilisation car l'œil doit rester grand ouvert et il est éclairé par une source lumineuse pour assurer un contraste correct.



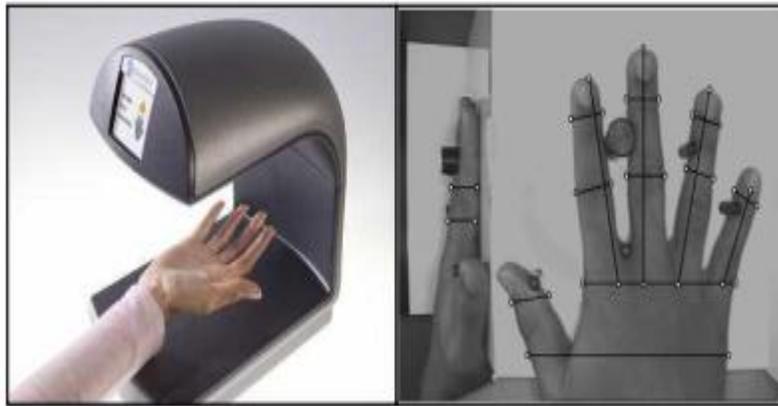
**Figure 1.3:** Image Iris

### 1.2.1.4. Géométrie de la main :

Cette méthode consiste à déterminer les caractéristiques de la main d'un individu : sa forme, la longueur, la largeur, la courbure des doigts,...etc. Les systèmes de reconnaissance de la géométrie de la main sont simples d'usage.

L'utilisateur doit poser la paume de sa main sur une plaque qui possède des guides afin de l'aider à positionner ses doigts.

La géométrie de la main a un faible pouvoir discriminant et les systèmes peuvent être facilement trompés par de vrais jumeaux ou même par des personnes de la même famille. [4]



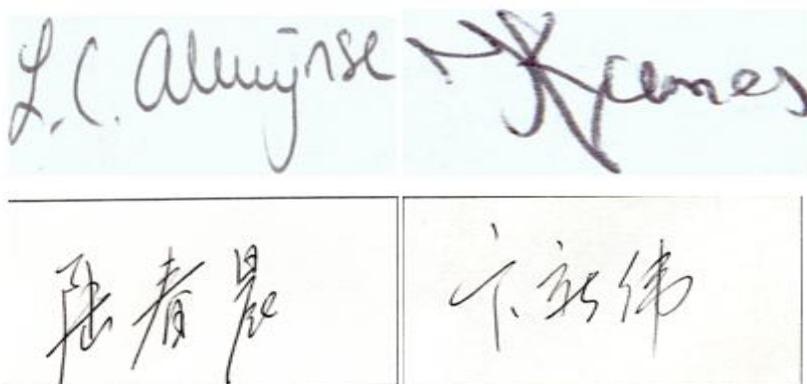
**Figure1. 4:** Image Géométrie de main

## 1.2.2. Modalités comportementale :

Elle est basée sur l'analyse de certains comportements d'une personne.

### 1.2.2.1. La signature :

Signature est une façon dont une personne signe son nom et dont on sait qu'elle est unique. La signature est un comportement biométrique comportemental qui évolue dans le temps et qui est facilement influencé par les conditions physiques et émotionnelles des signataires. Bien que les signatures nécessitent un contact avec l'instrument d'écriture et un effort de la part de l'utilisateur, elles ont été acceptées dans les transactions gouvernementales, juridiques et commerciales en tant que méthode d'authentification, cette technique est considérée parmi les premières utilisées dans le domaine de la biométrie.



**Figure 1.5:** Différentes signatures de (ICDAR2011)

### 1.2.2.2. La voix (Reconnaissance vocale) :

La voix humaine est trait unique de chaque individu. Elle est classée comme caractéristique biométrique comportementale. En effet, une grande partie de cette caractéristique est déterminée par le conduit vocal ainsi que les cavités buccales. La voix n'est pas un attribut permanent. Elle change bien entendu avec l'âge mais peut être aussi affectée temporairement par l'état de santé ou émotionnel du locuteur. [2]

Cette biométrie est en général très bien acceptée car la voix est un signal naturel à produire. De nos jours, tous les ordinateurs sont équipés en standard d'un microphone ce qui explique la popularité de la reconnaissance du locuteur pour les applications de type « desktop ». [4]



**Figure 1.6:** Image de la Reconnaissance vocale

### 1.2.2.3. Dynamique de la frappe au clavier :

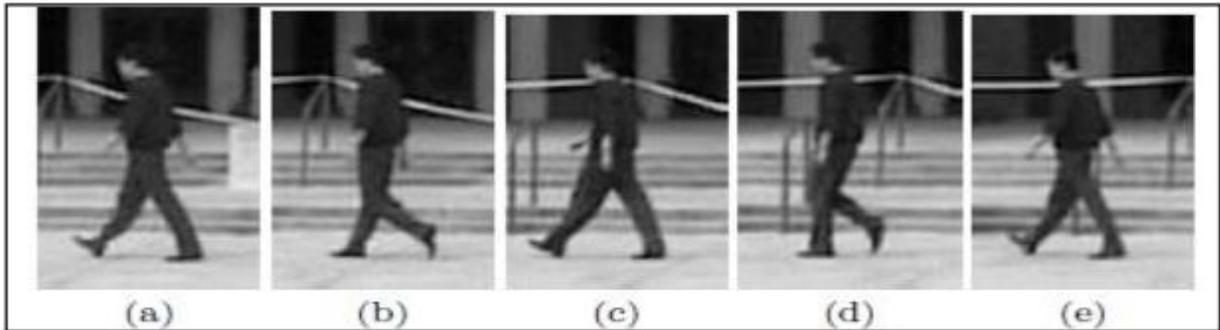
La dynamique de la frappe au clavier est une caractéristique propre de l'individu, c'est la transposition de la graphologie aux moyens électronique. C'est une méthode basée sur la façon d'utiliser ou de taper sur un clavier. Les paramètres pris en compte sont généralement les durées entre frappes. La fréquence des erreurs et la durée de la frappe. En revanche elle dépend de l'état physique et psychique de la personne (âge, maladie....) qui feront varier la qualité de la frappe. [4]



**Figure 1.7:** Image de la frappe au clavier

#### 1.2.2.4. La démarche :

Il s'agit de reconnaître un individu par sa façon de marcher et de bouger (vitesse, accélération, mouvements du corps...), en analysant des séquences d'images. La démarche serait en effet étroitement associée à la musculature naturelle et donc très personnelle. Mais des vêtements amples, par exemple, peuvent compromettre une bonne identification. [1]



**Figure 1.8:** Images sur la démarche

## 2. La vérification de la signature :

La tâche principale de tout système de vérification de signature est de déterminer si la signature est authentique ou falsifiée.

- Signature authentique

On sait que les signatures d'une même personne ne sont jamais les mêmes, qu'elles diffèrent à la fois globalement, localement et qu'elles peuvent également différer en taille et en orientation. Les circonstances dans lesquelles la signature a été écrite ont également un impact comme: la taille de l'espace de signature, les signatures négligentes, les stylos différents, l'état physique et psychologique de la personne, la surface. En outre, la signature d'une personne change souvent au fil du temps, mais ces modifications sont mineurs et peuvent être résolues en mettant à jour les signatures de cette personne dans la base de données.

- Signature falsifiée

Le processus de falsification d'une signature, si l'on veut qu'elle réussisse, implique un double processus exigeant du faussaire non seulement qu'il copie les caractéristiques de l'écriture imitée, mais qu'il masque également les caractéristiques personnelles de l'auteur. En fait, c'est le surmenage de la signature qui en fait surtout de la contrefaçon.

Certains experts en matière de signature notent que si deux signatures d'une même personne écrites sur papier étaient identiques, elles pourraient être considérées comme de la falsification par traçage, et bien sûr il y a les faux qualifiés qui peuvent tromper le système.

## 2.1. Type de falsification:

Les contrefaçons impliquées dans les signatures manuscrites ont été classées en fonction de leurs caractéristiques. Les contrefaçons dans les signatures peuvent être classées dans les types suivants:

- **Falsification aléatoire** : Le signataire utilise le nom de la victime dans son propre style pour créer une falsification connue sous le nom de falsification simple ou falsification aléatoire.
- **Falsification non qualifiée (simple)** : Le signataire imite la signature dans son propre style, sans aucune connaissance de l'orthographe ni expérience préalable.
- **Falsification qualifiée** : des imposteurs professionnels ou des personnes expérimentées dans la copie de la signature constituent sans aucun doute la falsification la plus difficile.



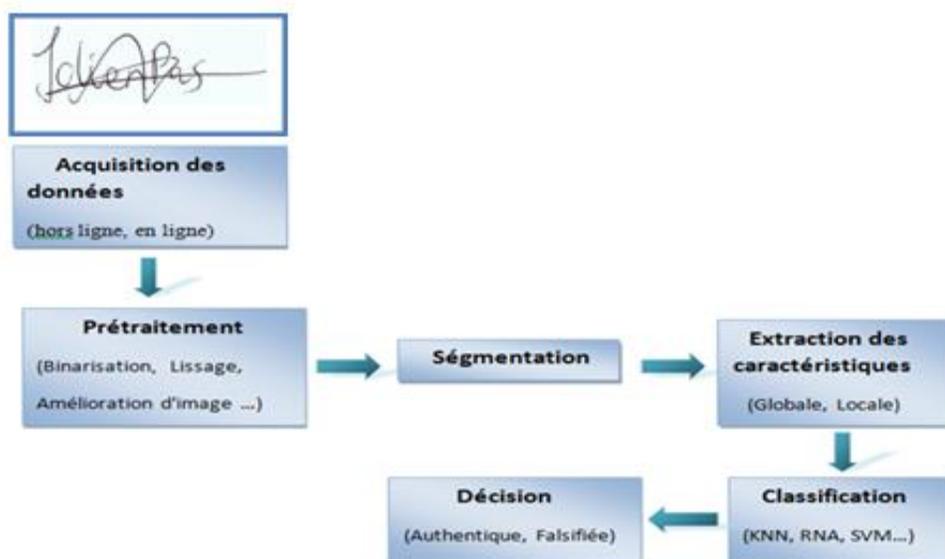
**Figure 1.9:** Les différents types de falsification

- a) Signature authentique b) Falsification aléatoire  
c) Falsification non qualifiée (simple) d) Falsification qualifiée

### 3. Processus d'un système de la vérification de signature :

Un système de la classification de la vérification de signature fait appel généralement aux étapes suivantes : acquisition, prétraitement, segmentation, extraction des caractéristiques, sélection des caractéristiques et leur classification.

Le schéma suivant explique ce processus: (**figure 1.10**)



**Figure 1.10:** Processus d'un système de la vérification de signature

#### 3.1. L'acquisition des données:

Selon la méthode d'acquisition de signature utilisée, les systèmes de vérification de signature peuvent être classés en deux groupes:

- Signature hors ligne (statique).
- Signature en ligne (dynamique).

Dans la vérification de la signature hors ligne (statique), seules les formes géométriques de la signature est utilisée pour authentifier une personne (**Figure 1.11**). Dans cette approche, l'extraction de données dynamiques n'est pas si facile, par ce que l'entrée dans ce système sera une image 2D de la signature et les informations dynamiques ne seront pas disponibles.



**Figure 1.11:** Signature hors ligne (statique)

Pour la deuxième approche (Signature en ligne (dynamique)) de la vérification des signatures, elle utilise, en plus de la forme géométrique, les caractéristiques dynamiques telles que les profils d'accélération, de vitesse et de trajectoire de la signature. La signature évolue avec le temps et est influencée par les conditions physiques et émotionnelles de la personne.



**Figure 1.12:** Signature en ligne (dynamique)

Les deux types de variation trouvés dans les signatures sont: la variabilité interpersonnelle et la variabilité intrapersonnelle. La variation entre les signatures d'une même personne s'appelle Variation intrapersonnelle.

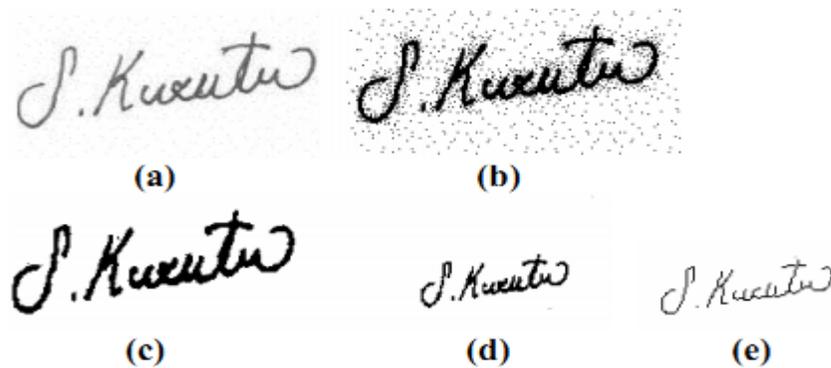
Cette variation peut être due à:

- Âge.
- La maladie.
- Les blessures.
- Les contraintes de temps.
- Drogues.
- Température.

La variation entre les originaux et les contrefaçons s'appelle interpersonnel.

### 3.2. Prétraitement de l'image:

La reconnaissance de signature hors ligne nécessite l'application de plusieurs étapes de prétraitement sur les ensembles d'apprentissage et de test afin de la préparer au processus d'extraction de caractéristiques. En du prétraitement, l'image de la signature passe: numérisation en gris (ou conversion en échelle de gris), puis élimination du bruit de fond, réduction du bruit, normalisation de la taille et dilution. (**Figure1.13**)

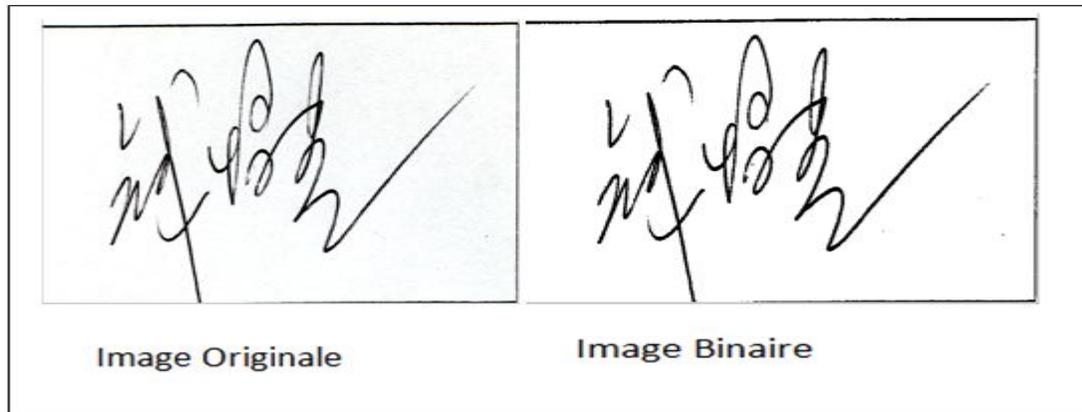


**Figure 1.13:** Prétraitement de la signature

- (a) signature scannée, (b) après binarisation, (c) après réduction du bruit,  
(d) après normalisation de la taille, (e) après dilution

### 3.2.1. La binarisation :

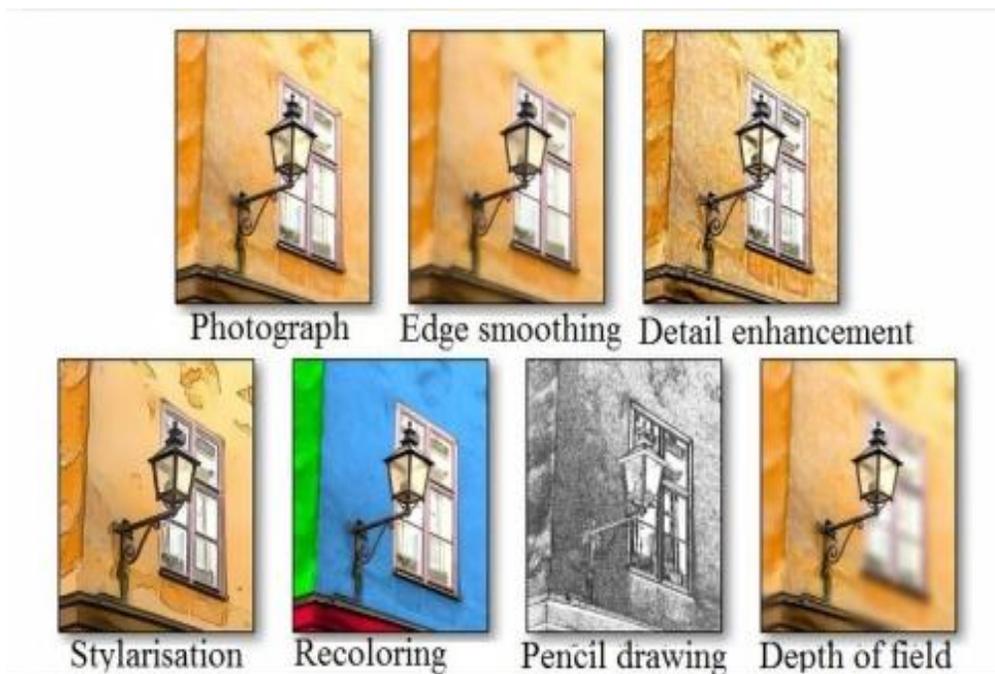
La binarisation qu'il signifie convertit une image jusqu'à 256 niveaux de gris en une image en noir et blanc. (**Figure 1.14**)



**Figure 1.14:** Image binarisée

### 3.2.2. Le lissage (Filtrage) :

Le filtrage est une technique pour modifier ou améliorer une image. Par exemple, vous pouvez filtrer une image pour mettre en valeur certaines caractéristiques ou en supprimer d'autres. Les opérations de traitement d'image mises en œuvre avec filtrage comprennent le lissage, l'accentuation et l'amélioration des contours. (**Figure 1.15**)



**Figure 1.15:** Exemple de lissage [5]

### 3.2.3. Amélioration d'image :

L'amélioration de l'image est un domaine le plus simple et le plus attrayant du traitement des images numériques. (Figure 1.16)



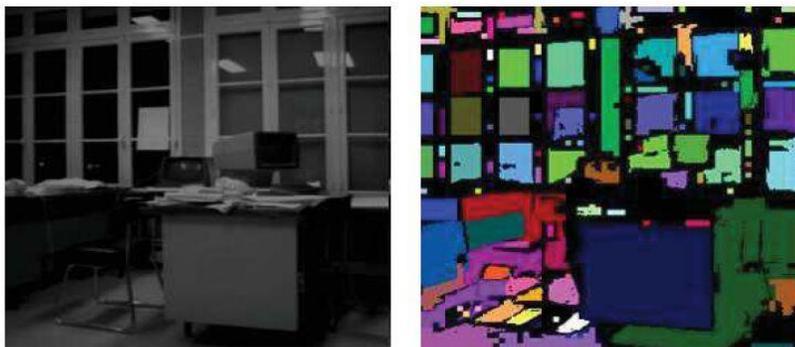
**Figure 1.16:** Amélioration d'image

L'idée sous-jacente aux techniques d'amélioration consiste à faire ressortir les détails obscurcis ou simplement à mettre en évidence certaines caractéristiques de l'image. Comme la luminosité changeante, etc.

### 3.3. Ségmentation:

Les procédures de segmentation divisent une image en ses parties ou objets constitutifs. En général, la segmentation autonome est l'une des tâches les plus difficiles du traitement numérique des images. (Figure 1.17)

Une procédure de segmentation robuste apporte une solution efficace aux problèmes d'imagerie qui nécessitent l'identification individuelle des objets.



(a) Image originale

(b) Ségmentation en régions

**Figure 1.17:** Ségmentation d'image

### 3.4. Extraction de caractéristiques:

Dans cette section, nous décrivons les caractéristiques des méthodes d'extraction utilisées dans la vérification de signature. L'étape d'extraction des caractéristiques réduit la dimension des images de signature originales tout en préservant et en extrayant les informations importantes encodées dans l'image.

Un ensemble de caractéristiques soigneusement sélectionnées transformera les images pour qu'il soit plus facile de distinguer les classes authentiques des classes falsifiées.

#### 3.4.1. Caractéristiques globales:

Les caractéristiques globales décrivent l'ensemble de l'image de signature, telles-que la largeur, la hauteur et le rapport hauteur/largeur. Ces caractéristiques sont utilisées en combinaison avec d'autres caractéristiques. Ces caractéristiques sont moins sensibles au bruit et peuvent être obtenues en considérant tous les points à l'intérieur d'une région, ou par les points à la limite d'une région (zone de signature). Il inclut les caractéristiques des régions dans les images, les moments, les descripteurs de Fourier, le périmètre.

#### 3.4.2. Caractéristiques locales:

Les caractéristiques locales font référence à un motif ou à une structure distincte que l'on trouve dans une image, comme un point, un bord ou un petit patch d'image. Ils sont généralement associés à une tache d'image qui diffère de son environnement immédiat par sa texture, sa couleur ou son intensité. Ce que l'élément représente réellement n'a pas d'importance, juste qu'il est distinct de son environnement.

Donc, une caractéristique globale signifie que vous regardez toute l'image, alors que caractéristique locale signifie que vous vous concentrez sur quelque chose.

### 3.5. Classification:

Après la segmentation et l'extraction de caractéristiques, une étape de reconnaissance basée sur la classification des caractéristiques.

Les techniques de la classification reposent sur une stratégie de décision qui permet de catégoriser un objet le mieux possible selon certains critères d'optimisation.

Le type d'une méthode de classification se décline généralement en trois familles : Le mode supervisé, le mode non supervisé et le mode semi supervisé.

- **Classification supervisée** : cette technique est basée sur l'étiquetage des observations en affectant chaque observation à une classe (supervisés où la sortie correcte doit être fournie à l'avance).
- **Classification non supervisée** : aucune des observations n'est étiquetée (non supervisés où la sortie correcte n'est pas exigée à l'avance, elle résulte après une étape d'apprentissage).
- **Classification semi supervisée** : cette technique est basée sur l'étiquetage d'une partie des observations.

#### 4. Présentation de certaines techniques de la classification :

Il existe plusieurs algorithmes de classification supervisée. Nous présentons quelques-uns, il s'agit de :

##### 4.1. K-plus proche voisin (KNN) :

K-plus proche voisin proches (K-Nearest Neighbors) est un algorithme simple qui stocke tous les cas disponibles et classe les nouveaux cas en fonction d'une mesure de similarité (par exemple, des fonctions de distance). Le KNN a déjà été utilisé dans l'estimation statistique et la reconnaissance des formes au début des années 1970 en tant que technique non paramétrique. [5]

##### 4.2. Machine à Vecteur Support (SVM) :

Les Machine à Vecteur Support (Support Vector Machines) souvent traduit par l'appellation de séparateur à Vaste marge (SVM) sont une classe d'algorithmes d'apprentissage initialement définis pour la discrimination c'est-à-dire la prévision d'une variable qualitative binaire. Ils ont été ensuite généralisés à la prévision d'une variable quantitative. [6]

#### Conclusion :

Dans ce chapitre, nous avons présenté les technologies utilisées dans les systèmes biométriques pour l'identification de personnes. Ainsi nous avons présenté la vérification de la signature constituent le principal objectif de notre travail. On a présenté aussi quelques algorithmes ou méthodes de classification (K-plus proche voisin, k-means, Machine à Vecteur Support,).

Dans le prochain chapitre, nous allons voir le principe et quelque type de l'apprentissage profond (Deep learning) et les réseaux de neurones Convolutif (CNN).

## **Chapitre 02**

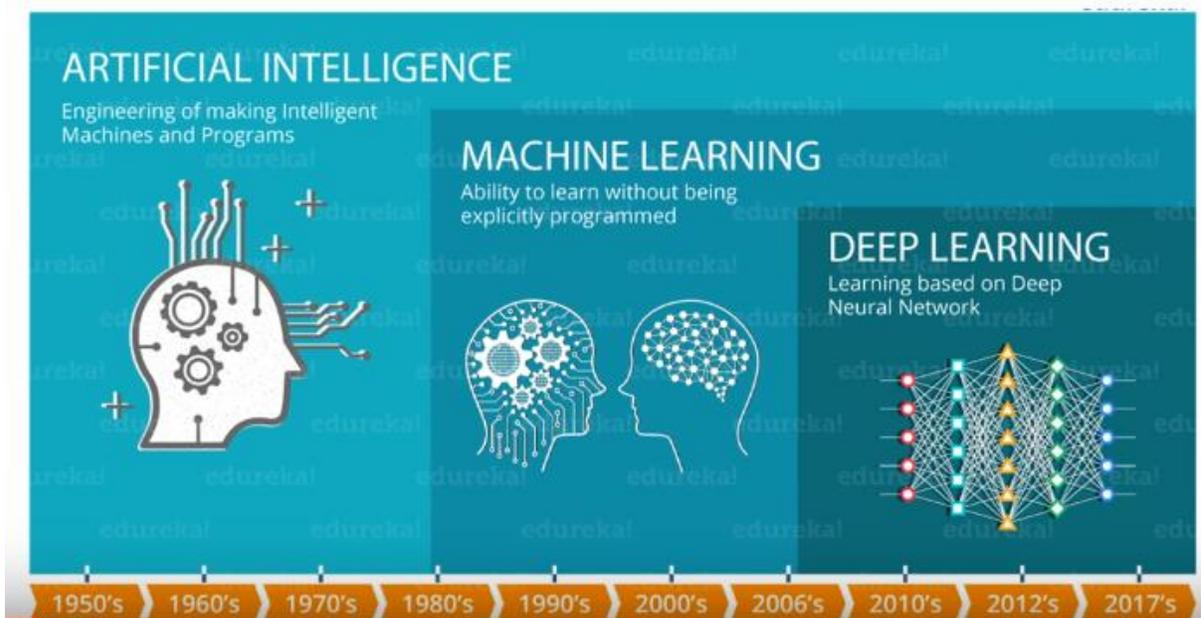
---

# **L'apprentissage profond (Deep Learning)**

---

L'intelligence artificielle est une discipline scientifique recherchant des méthodes de solution de problèmes à forte complexité logique ou algorithmique. L'apprentissage automatique (Machine Learning) est un sous-domaine de l'intelligence artificiel, son but est d'entraîner un ensemble d'algorithmes sur de grande quantité de données afin de pouvoir classifier des données futures (la précision dépendant de la quantité et la qualité des données) [7]. Par conséquent, L'apprentissage profond (Deep Learning) est un sous-domaine de l'apprentissage automatique. Conceptuellement, le fonctionnement de l'apprentissage profond se traduit par plusieurs couches de calques auxquels des données sont échangés pour générer un ou plusieurs rendu(s). [7]

Dans ce chapitre nous allons présenter les notions en relation avec l'apprentissage profond.



**Figure 2.1:** La relation entre IA, ML et DL [7]

## 1. Réseaux de Neurones Artificiels (RNA) :

Réseaux de neurones artificiels (Architecture of Neural Networks ou ANN) C'est une structure constituée de suite successive des couches des nœuds et qui permet de définir une fonction de transformation non linéaire des vecteurs d'entrées (composés dans le cas de classification des mots pondérés de leur poids) en vecteur de catégories. La disposition des neurones dans le réseau ainsi que les nombres des couches utilisées ont une influence sur le résultat de classification. Comparés aux autres méthodes de classification par apprentissage supervisé, les réseaux de neurones ont l'inconvénient que le coût d'apprentissage est assez élevé.[8]

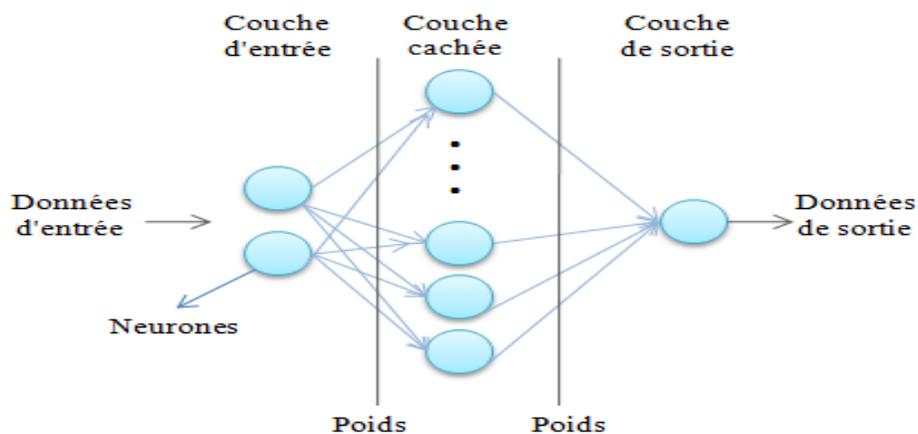


Figure 2.2: Réseaux de neurones artificiels

### 1.1. Perceptron:

Le perceptron peut être vu comme le type de réseau de neurones le plus simple, a été introduit en 1958 par Franck Rosenblatt. Il s'agit d'un neurone artificiel inspiré par la théorie cognitive de Friedrich Hayek et celle de Donald Hebb. Dans sa version la plus simple, le perceptron n'a qu'une seule sortie  $y$  à laquelle toutes les entrées  $x_i$  sont connectées, ses entrées et sorties étant booléennes. [9]

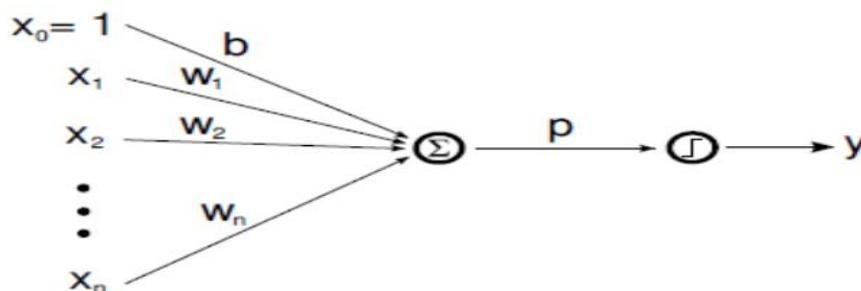
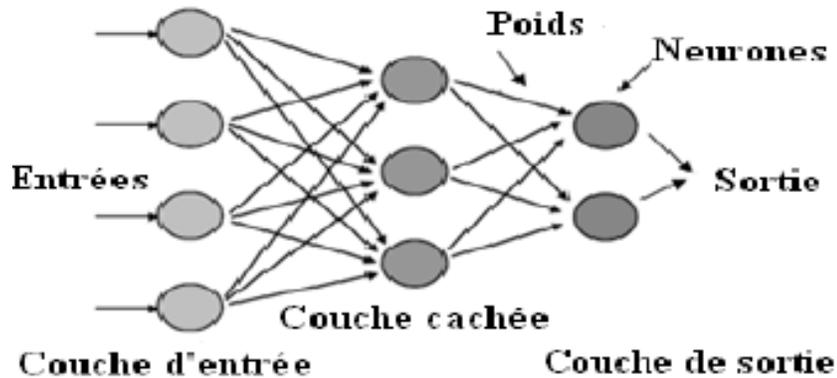


Figure 2.3: Modèle du perceptron [11]

## 1.2. Perceptron MultiCouche (PMC) :

Le perceptron multicouche (Multi Layer Perceptron ou MLP) est un classifieur linéaire de type réseau neuronal formel organisé en plusieurs couches (**Figure 2.4**) au sein desquelles une information circule de la couche d'entrée vers la couche de sortie uniquement. Chaque couche est constituée d'un nombre variable de neurones, les neurones de la couche de sortie correspondant toujours aux sorties du système. [10]



**Figure 2.4:** Perceptron MultiCouche [11]

## 2. Définition du l'apprentissage profond (Deep Learning):

L'apprentissage en profondeur (« deep learning ») est un ensemble de techniques d'apprentissage automatique qui a permis des avancées importantes en intelligence artificielle dans les dernières années.

Dans l'apprentissage automatique, un programme analyse un ensemble de données afin de tirer des règles qui permettront de tirer des conclusions sur de nouvelles données. L'apprentissage profond est basé sur ce qui a été appelé, par analogie, des «réseaux de neurones artificiels», composés de milliers d'unités (les « neurones ») qui effectuent chacune de petites opérations simples. Les résultats d'une première couche de « neurones » servent d'entrée aux calculs d'une deuxième couche et ainsi de suite. [10]

## 3. L'architecture de l'apprentissage profond:

### 3.1. Réseaux Neurones Convolutif (RNC) :

Cet algorithme doit être détaillé car nous l'avons choisi comme une méthode de vérification de la signature dans l'apprentissage profond.

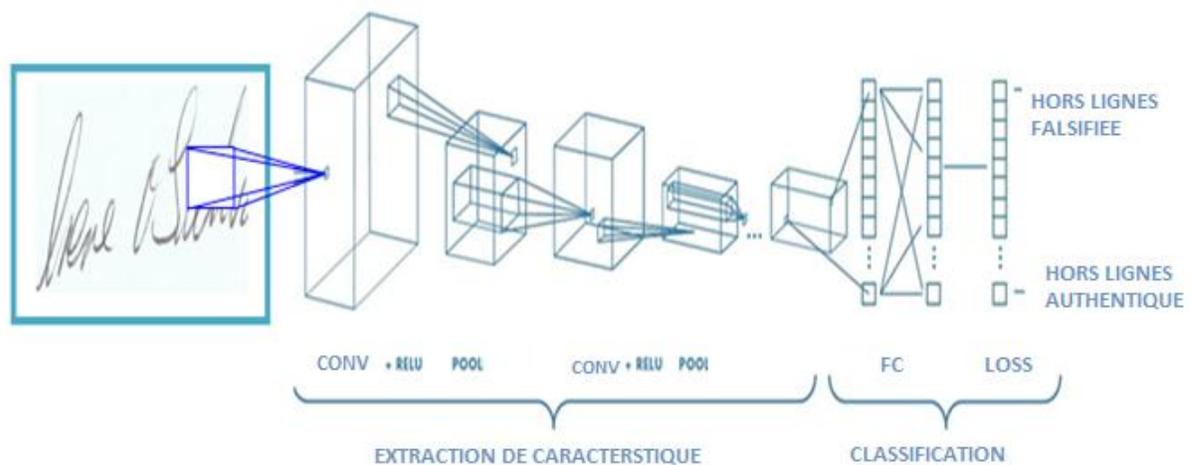
### 3.1.1. Définition de RNC:

Le Réseau de Neurone Convolutif (Convolutional Neural Networks, CNN ou ConvNet) est un type de réseau de neurones artificiels acycliques dans lequel le motif de connexion entre les neurones est inspiré par le cortex visuel des animaux. Les réseaux neuronaux convolutif ont été utilisés dans plusieurs applications, y compris la reconnaissance numérique des chiffres, la détection des visages et la vérification de la signature.

### 3.1.2. L'architecture de RNC:

La structure de CNN consiste en un ensemble de couches :

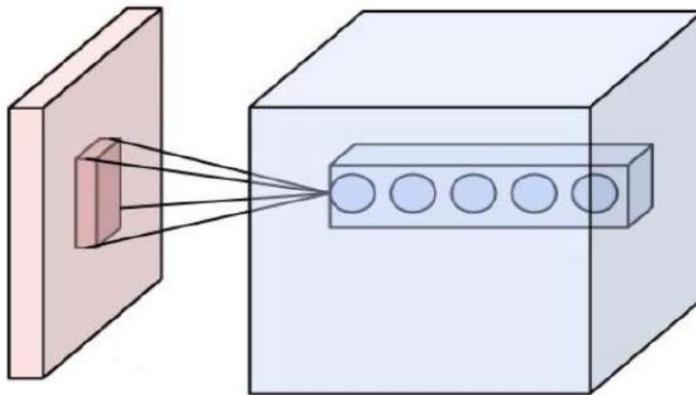
- **La couche de convolution (CONV):** est la première étape qui traite des données de champ du récepteur.
- **La couche de pooling (POOL):** est l'étape où vous compressez les informations en réduisant la taille de l'image intermédiaire.
- **La couche correction (Rectified Linear Unit (ReLU)).**
- **La couche "entièrement connecté" (FC).**
- **La couche de perte (LOSS).**



**Figure 2.5:** L'architecture de CNN L'architecture de CNN

### 3.1.2.1. La couche de convolution (CONV):

La classe convolution est l'étape de base de CNN. Les paramètres de couche sont constitués d'un ensemble de filtres (ou noyau) pouvant être appris, qui ont un petit champ de réception mais s'étendent sur toute la profondeur de la taille d'entrée. C'est inspiré des MLP traditionnels, mais avec des différences majeures. Les principales sont que chaque couche a un seul ensemble de poids pour tous les poids partagés des neurones, et que chaque neurone ne traite qu'une petite partie de l'espace d'entrée. [11]



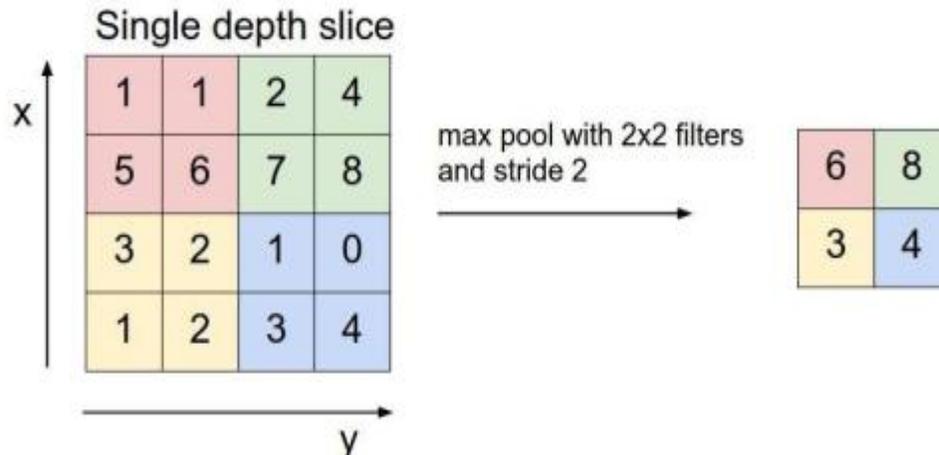
**Figure 2.6:** Représentation de la fonctionnalité Convolution [13]

### 3.1.2.2. La couche de pooling (POOL):

Un autre outil très puissant utilisé par les CNNs s'appelle le Pooling, ce qui est une forme de sous-échantillonnage de l'image.

Le Pooling est une méthode permettant de prendre une large image et d'en réduire la taille tout en préservant les informations les plus importantes qu'elle contient. Le Pooling peut être de différents types : max, moyenne, somme, etc.

En cas de Pooling max, on définit un voisinage spatial (par exemple, une fenêtre  $2 \times 2$ ) et de prendre le plus grand élément dans cette fenêtre. En pratique, le Pooling max a donné le meilleur résultat.



**Figure 2.7:** Max pooling avec un filtre  $2 \times 2$  et un pas de 2 [12]

### 3.1.2.3. La couche de correction (Rectified Linear Unit (ReLU)) :

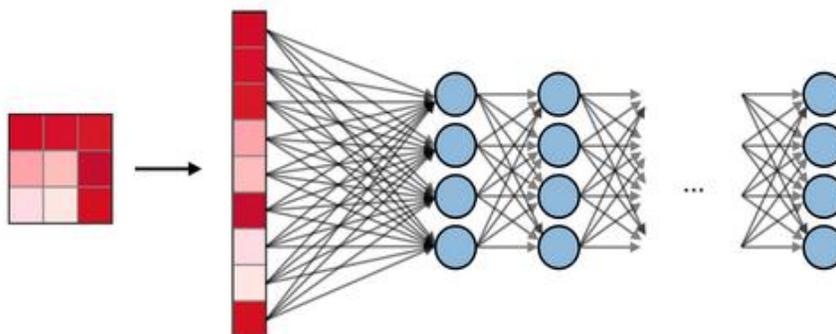
Une opération supplémentaire appelée ReLU a été utilisée après chaque opération de convolution.

Un ReLU applique la fonction  $y = \max(x, 0)$ , Cette fonction force les neurones à retourner des valeurs positives telles-que les tailles d'entrée et de sortie de cette couche sont identiques. L'avantage d'un ReLU est que le réseau s'entraîne beaucoup plus rapidement.

### 3.1.2.4. La couche entièrement connecté (Fully connected (FC)) :

La couche entièrement connectée utilisé après Après plusieurs couches de convolution, ReLU et de max-pooling. Les neurones dans une couche entièrement connectée ont des connexions vers toutes les sorties de la couche précédente.

Le but de la couche entièrement connectée est d'utiliser ces fonctions pour classer l'image d'entrée dans différentes classes en fonction de l'ensemble de données d'apprentissage.



**Figure 2.8 :** Représentation de la fonctionnalité FC

### 3.1.2.5. La couche de perte (LOSS):

La couche de perte spécifie comment l'entraînement du réseau pénalise l'écart entre le signal prévu et réel. Elle est normalement la dernière couche dans le réseau. Diverses fonctions de perte adaptées à différentes tâches peuvent y être utilisées. La fonction « Softmax » permet de calculer la distribution de probabilités sur les classes de sortie. [13]

### 3.2. Réseaux de Neurones Récurrents (RNR) :

Un réseau de neurones récurrents (Recurrent neural networks ou RNN) permettent d'analyser les séquences de vecteurs tout comme les modèles de Markov cachés. Le temps entre ici en ligne de compte car les sorties (de la couche de sortie et/ou de la couche cachées) calculées à l'instant  $t$  sont ré-injectées en entrée du réseau et/ou en entrée de la couche cachée. On peut en théorie conserver dans le réseau la mémoire de ce qui s'y est passé depuis le début. [13]

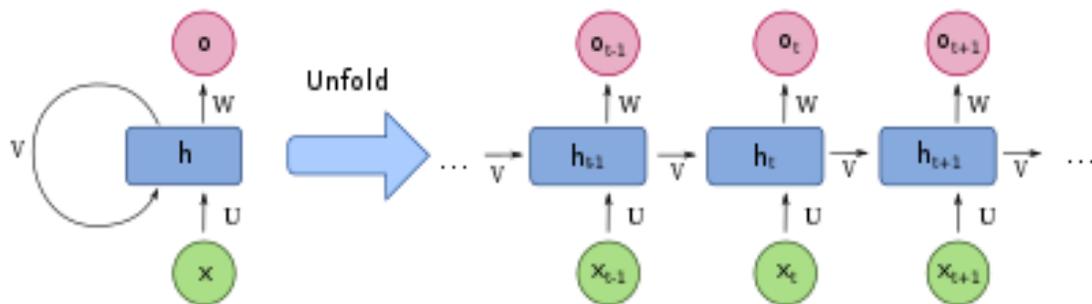


Figure 2.9: Réseaux de neurones récurrents

### 3.3. Mémoire à long terme à court terme (LSTM) :

Mémoire à long terme à court terme (Long-Short Term Memory Network ou LSTM) sont une extension pour les réseaux neuronaux récurrents, qui étend leur mémoire. Par conséquent, il est bien adapté pour apprendre des expériences importantes qui ont des retards très longs entre les deux. Les unités d'un LSTM sont utilisées comme unités de construction pour les couches d'un RNN, qui est alors souvent appelé un réseau LSTM.

Les LSTM permettent aux RNN de se souvenir de leurs intrants sur une longue période de temps. C'est parce que les LSTM contiennent leurs informations dans une mémoire, ce qui ressemble beaucoup à la mémoire d'un ordinateur parce que le LSTM peut lire, écrire et supprimer des informations de sa mémoire. [14]

### 3.4. Machine de Boltzmann Profonde (MBP) :

Une machine de Boltzmann restreinte (Deep Belief Network ou DBN) est un type de réseau de neurones artificiels inventé par Geoff Hinton, pionnier de l'apprentissage automatique et de la conception de réseaux de neurones.

Ce type de réseau génératif est utile pour le filtrage, l'apprentissage des fonctionnalités et la classification. Il utilise certains types de réduction de dimensionnalité pour aider à traiter des entrées compliquées.

### Conclusion :

Dans ce chapitre on a présenté les notions importantes qui sont en relation avec l'apprentissage profond. Aussi qu'une vision générale sur l'apprentissage profond et quelques exemples d'algorithmes d'apprentissage profond, toute on donnant en détail la méthode choisie dans notre travail de recherche qui est le CNN.

Le prochain chapitre, nous allons voir les travaux antérieurs pour la vérification de la signature avec CNN.

## **Chapitre 03**

---

# **Vérification de signature avec CNN**

---

Ce chapitre est dédié à la description de l'état de l'art dans le domaine de la vérification de la signature avec CNN. Quelques travaux de recherche en vérification de signature sont présentés et classés suivant un ordre chronologique. Finalement, une comparaison de différentes méthodes est élaborée et articulée sur un ensemble de critères dont le taux de performance et la base de données.

## **1. Les travaux ultérieurs :**

La littérature sur la vérification de la signature comprend plusieurs exemples. Les modèles de Markov cachés (HMM) [15], réseaux de neurones [16], SVM [17] et autre modèles d'apprentissage automatique. Cette section, pour bute d'arborer les différents travaux consacrés à la vérification de signature basé sur l'apprentissage profond en fonction de l'approche utilisée et le résultat obtenu.

### **1.1. CNN et MLP pour la vérification de signature Persan (Khalajzadeh *et al.* (2012)):**

Dans [18], Les auteurs ont présentés une approche pour la vérification de signature hors ligne basé sur le réseau de neurones de convolution (CNN) et le réseau multicouche de perceptron. Le CNN concentré sur les problèmes d'extraction de caractéristiques sans connaissance préalable des données. La tâche de classification est effectuée par un réseau multicouche de perceptron (MLP).

Le CNN est composé de neuf couches: cinq couches de convolution et quatre couches de sous-échantillonnage. Le réseau MLP est utilisé pour classifier les sorties de CNN ; la dernière couche du réseau CNN est considérée comme la couche d'entrée du réseau MLP. Cette couche est suivie d'une couche cachée de 84 neurones, qui est entièrement interconnectée avec la couche précédente. Enfin, la dernière couche de ce réseau est une couche avec un seul neurone qui est la cible du réseau. La cible est considérée comme 0 ou 1 qui signifient respectivement une signature originale ou falsifiée. La méthode proposée est évaluée sur un ensemble de signatures persanes initialement recueillies auprès de 22 personnes et a obtenu un pourcentage 99,85% de réussite.

## **1.2. CNN basé sur VGG16 pour la vérification de signature hors ligne (Alvarez *et al.* (2016)):**

Alvarez *et al.* [19] présentent un processus de vérification de signature hors ligne en utilisant des réseaux de neurones à convolution (CNN). Leur première tâche consistait à former CNN pour savoir si les signatures individuelles étaient falsifiées ou authentiques, après avoir vu des exemples de copies falsifiées et de copies authentiques de la même personne inscrite pendant la formation.

Leur modèle est basé sur la structure VGG16 [20] et ils ont utilisé la base de données ICDAR 2011 SigComp pour tester deux tâches. La tâche principale est une vérification Writer-Independent ; ils ont obtenu une précision de 97% pour les signatures Néerlandaises et de 95% pour les signatures Chinoises. Tandis que, la deuxième tâche est une vérification dépendant du signataire ; ils ont obtenu une précision de 67.1% pour les signatures Néerlandaises.

## **1.3. CNN pour détecter et réduire la falsification des signatures (Cozzens *et al.* (2017)):**

L'architecture du CNN proposé par Cozzens *et al.* dans [21] est une architecture simple basée sur les réseaux de neurone convolutif, où le CNN est créé à l'aide de la bibliothèque Keras en Python avec TensorFlow pour modifier l'image pour donner à la signature un aperçu plus clair. Ils ont utilisé le système de comparaison d'images, basé sur le système de classification d'images. Lorsqu'une signature est entrée dans le programme, celle-ci sera comparée à d'autres caractéristiques de signature portant la même étiquette.

La principale contribution de cette méthode est de détecter et de réduire la contrefaçon, en particulier dans le secteur bancaire.

La méthode de détection correcte de la signature était évaluée pour la base de données ICDAR 2011 SigComp qui donne un taux de 83,93%

#### **1.4. Ad hoc models CNN pour La vérification de signature (Multu Yapici *et al.* (2018)):**

Il consiste d'une méthode d'apprentissage profond pour la vérification de signature hors ligne.

Les auteurs [22] ont présenté une méthode simple basée sur les réseaux de neurone convolutifs de type ad hoc pour implémenter leur modèle d'apprentissage profond. Les réseaux de neurones de convolution utilisés ont été formés séparément en utilisant deux formats: Écrivain Dépendant (Writer Dependent ou WD) et Écrivain Indépendant (Writer Independent ou WI).

L'application a été développée en langage Python par en utilisant Keras Framework et Tensorflow comme un back-end.

La méthode proposée est évaluée sur la base de données GPDSsyntheticSignature et les résultats ont montré que WI avait atteint 62,5% et que WD avait atteint 75% de succès.

#### **1.5. CNN et AE pour de vérification signatures dynamique (Man *et al.* (2018)) :**

Dans cet article [23], Man *et al.* proposons une nouvelle approche de vérification dynamique pour les signatures tracées au doigt, qui offre une précision améliorée par rapport aux signatures falsifiées et aux signatures différées.

La méthode proposée exploite deux algorithmes d'apprentissage profond: le réseau de neurones à convolution (CNN) pour l'extraction de caractéristiques et un codeur automatique (autoencodeur (AE) [24] comme classificateur. L'AE est un type de réseau de neurones profonds (DNN) ayant les mêmes dimensions pour l'entrée et la sortie. Ils ont été formés le CNN pour distinguer les signatures falsifiées des signatures authentiques, la sortie de la couche intermédiaire de CNN, que nous appelons S-vector, est utilisée comme entrée d'un AE pour construire le modèle sujet.

La méthode proposée permet d'obtenir les meilleures performances (95.60%) pour les signatures différées dans le temps par une approche expérimentale.

### **1.6. CNN et SVM pour la vérification de signature manuscrite hors ligne (Bhanu Sronothara *et al.* (2018)):**

Bhanu Sronothara *et al.* [25] ont développés un système de vérification de signature manuscrite hors ligne capable de différencier les signatures authentiques des signatures falsifiées.

Le système de vérification de signature proposé implique CNN (réseau de neurones à convolution) pour l'extraction de caractéristiques et le SVM (Support Vector Machine) pour la classification.

L'architecture CNN se compose d'un certain nombre de couches telles que chaque couche effectue un calcul simple à partir du brut et envoie le résultat au calque suivant à l'aide de la touche le résultat final est envoyé à un classificateur. Le classificateur sélectionné est SVM avec le grain cubique pour montre le résultat.

La méthode proposée est évaluée sur la base de données et a obtenu un pourcentage 83% de réussite.

## 2. Comparaison des travaux :

Les performances et les approches utilisées pour chaque méthode s'illustre dans le tableau ci dessous.

Etude	Modèle du CNN	Nombre de couche	Classification	Base de données	Tâche (WI/WD)	Performance
01	Ordinaire	9 couches	Avec (MLP)	signature Persan	WI	99.85%
02	VGG16	/	Non	ICDAR 2011I	WI WD	Néerlandais:97% Chinoise : 95%
03	Ordinaire	13 couches	Non	ICDAR 2011	WD	83.93%
04	Ad hoc	/	Non	GPDSsyntheticSignature	WI WD	WI : 62.5% WD : 75%
05	Ordinaire	/	Avec (AE)	/	WI	95.60%
06	Ordinaire	10 couches	Avec(SVM)	GPDS-960	WD	83%

**Table 3.1:** Principaux travaux de recherche dans le domaine vérification de la signature

### Conclusion :

Dans ce chapitre nous avons présenté un aperçu sur état de l'art dans le domaine de vérification de signature. Dans la première partie, nous nous concentrons sur la présentation des principaux travaux de recherche dans ce domaine et discutons les diverses compétitions. Ensuite, nous terminons par une comparaison des différents travaux du domaine en nous basant, comme critères de comparaison, les bases de données utilisée, le Modèle du CNN choisies et bien sur les taux de performance obtenu.

Le chapitre suivant se consacre à la description l'architecture du CNN choisie et le résultat expérimental.

## **Chapitre 04**

---

**Méthode proposé**

**et**

**Résultats expérimentaux**

---

Ce chapitre a été alloué pour présenter les résultats obtenus pour la validation du système vérification de signature. Nous faire la conception d'application en utilisant le langage Python.

Dans ce chapitre, nous utilisons les réseaux des neurones Convolutif (CNN) qui peut être appliqué efficacement à la vérification de signature utilisant l'apprentissage profond, en utilisant la base de données ICDAR2011.

## **1. Présentation des outils de développement :**

### **1.1. Matériel :**

Le matériel réalisé est PC personnel Lenovo I3 avec un 4GB capacité mémoire, et un processeur Intel® Core™ i3 CPU M 370 @2.40 GHz 2.40 GHz, avec Windows 7 professionnel, 64 bit type du système.

### **1.2. Python :**

Python est un langage de programmation de haut niveau interprété (il n'y a pas d'étape de compilation) et orienté objet avec une sémantique dynamique, a été créé en 1989 par Guido van Rossum, aux Pays-Bas. Il est très sollicité par une large communauté de développeurs et de programmeurs. Python est un langage simple, facile à apprendre et permet une bonne réduction du cout de la maintenance des codes. Les bibliothèques (packages) python encouragent la modularité et la réutilisabilité des codes. Python et ses bibliothèques sont disponibles (en source ou en binaires) sans charges pour la majorité des plateformes et peuvent être redistribués gratuitement. [26]

### **1.3. Google Colab :**

Google Colaboratory (Colab) est un service de cloud basé sur Jupyter Notebooks destiné à diffuser des informations et des formations en apprentissage automatique.

Colaboratory fournit des temps d'exécutions sur Python 2 et 3, préconfigurées avec les bibliothèques d'apprentissage automatique, en profondeur et d'intelligence artificielle essentielles telles que TensorFlow, Matplotlib, et Keras, et un accès gratuit à un GPU robuste.

De plus, les documents Colab sont enregistrés directement votre compte Google Drive. [13]

## 1.4. TensorFlow :

TensorFlow est un framework de programmation pour le calcul numérique qui a été rendu Open Source par Google en Novembre 2015. Depuis son release, TensorFlow n'a cessé de gagner en popularité, pour devenir très rapidement l'un des frameworks les plus utilisés pour le Deep Learning et donc les réseaux de neurones. Son nom est notamment inspiré du fait que les opérations courantes sur des réseaux de neurones sont principalement faites via des tables de données multi-dimensionnelles, appelées Tenseurs (Tensor). Un Tensor à deux dimensions est l'équivalent d'une matrice. Aujourd'hui, les principaux produits de Google sont basés sur TensorFlow: Gmail, Google Photos, Reconnaissance de voix. [13]

## 2. Méthode proposée pour la vérification des signatures :

Les étapes de la méthode sont décrites ici :

Étape 1 : Obtenir les signatures de la base de données ICDAR2011 sigcomp.

Étape 2 : Effectuer le prétraitement sur les signatures.

Étape 3 : Architecture de CNN.

### 2.1. Base de données :

#### 2.1.1. Présentation de la base de données :

Notre base de données ICDAR 2011 provient du concours international SigComp de vérification des signatures de la Conférence internationale sur l'analyse et la reconnaissance des documents.

La base de données comprend des signatures en ligne et hors ligne pour les signataires chinois et néerlandais. L'ensemble de données est divisé en un ensemble d'apprentissage et un ensemble de tests de personnes non imbriqués.

L'ensemble d'apprentissage néerlandais comprend un total de 362 images pour 16 personnes, avec environ 24 signatures authentiques et 4 signatures falsifiées pour chaque personne, par contre l'ensemble d'apprentissage en chinois contient 575 images pour 10 personnes, avec environ 24 signatures authentiques et 12 contrefaçons pour chaque personne.

L'ensemble de test comprend un ensemble de "référence" et "question", les références étant des signatures originales connues et les signatures contestables étant originales ou falsifiées.

Le test néerlandais composé de 54 personnes, chacun personne comportant 12 signatures de référence et environ 3 signatures en vérification (en question), par contre le test chinois composé de 10 personnes, avec environ 12 signatures de référence et environ 3 signatures en question.



**Figure 4.1:** Exemples de signatures de la base de données ICDAR 2011. Rangée du haut: signatures du sous-ensemble chinois, rangée du bas: signatures du sous-ensemble néerlandais.

### 2.1.2. Acquisition de données :

Dans la phase de test, les signatures peuvent être authentiques : écrites par l'auteur de référence, ou simulées par un autre auteur que l'auteur de référence, la collection contient des échantillons de signatures hors ligne et en ligne.

En mode hors ligne, les signatures de vérification de signature seront constituées d'images PNG, numérisées à 400 dpi, couleur RVB. Chaque image de signature a une dimension de 1173\*1173 pixels.



**Figure 4.2:** Exemple de la signature hore ligne

## 2.2. Prétraitement :

Puisque les signatures sont des images acquises par un scanner, ils ont des tailles différentes et ils sont représentés en RVB, donc, l'étape de prétraitement est primordiale. Le prétraitement regroupe l'ensemble des processus visant à améliorer les caractéristiques des signatures de la base de données. Cette étape consiste à préparer les données qui seront fournies au module d'authentification.

Plusieurs traitements sont nécessaires, les deux suivants sont utilisés.

### 2.2.1. Conversion d'image en niveaux de gris :

Après l'acquisition numérique d'une signature, nous disposons d'une image RGB (à 16 millions couleurs). Utiliser des images en niveau de gris est plus fiable dans les systèmes de vérification de signature. Donc il faut calculer la valeur d'intensité lumineuse d'un pixel (valeur entre 0 et 255) au lieu de son couleur (valeur de 0 à 16 millions).

### 2.2.2. Redimensionnement de l'image

Suite à différentes tailles d'images contenant les signatures et afin de normaliser la taille des images d'entrées du réseau de neurone convolutif, un processus de redimensionnement est effectué. Les images sont d'abord recadrées dans une image de taille 1173\*1173 (la plus grande image), en suite les images de résultats sont redimensionnées en taille standard 180\*180.

### 2.3. L'architecture de CNN :

Avant tout, nous devons définir l'architecture du réseau CNN utilisé en construisant les différentes couches de traitement :

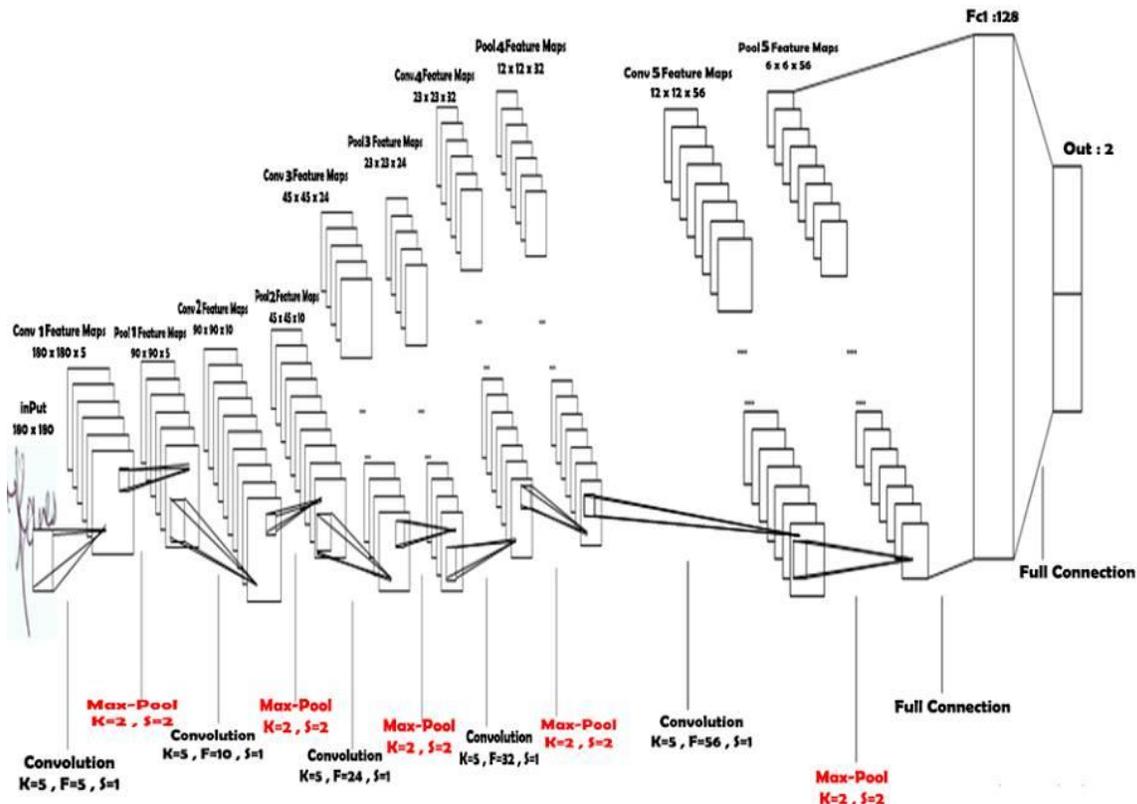


Figure 4.3: Proposition de CNN pour la vérification de la signature

Dans notre expérience, nous avons construit une architecture CNN pour la classification avec un backend Tensorflow en Python.

Le CNN proposé qui est représenté sur la Table 4.1. Prend une image de signature brute de taille 180\*180 pixels en entrée. Les images d'entrée sont normalisées entre 0 et 1 et sont transmises à un CNN. Le CNN est composé de 12 couches : cinq couches convolutives, cinq couches de max pooling et une couche entièrement connectée et une couche de sortie.

La structure du réseau est décrite dans la sous-section suivante.

La première couche convolutionnelle de la CNN proposée comporte cinq cartes de caractéristiques (Feature maps), dont chacune a une résolution de 180\*180, avec un champ récepteur de 5\*5. La deuxième couche, ou première couche de max pooling, contient 5 cartes

d'entités de taille  $90 \times 90$ , avec un champ réceptif de  $2 \times 2$ ; la troisième couche est une autre couche convolutionnelle et comprend 10 cartes d'entités de taille  $90 \times 90$ , avec un champ récepteur de  $5 \times 5$ . La quatrième couche contient également 10 cartes d'entités, dont chacune a une taille de  $45 \times 45$ . La cinquième couche convolutionnelle comprend 24 cartes de caractéristiques, dont chacune a une résolution de  $45 \times 45$ , avec un champ récepteur de  $5 \times 5$ . La sixième couche contient 24 cartes d'entités de taille  $23 \times 23$ , avec un champ réceptif de  $2 \times 2$ ; la septième couche est une autre couche convolutionnelle et comprend 32 cartes d'entités de taille  $23 \times 23$ , avec un champ récepteur de  $5 \times 5$ . La huitième couche contient également 32 cartes d'entités, dont chacune est de taille  $5 \times 5$ . La neuvième couche est une autre couche convolutionnelle et comprend 56 cartes d'entités de taille  $12 \times 12$ , avec un champ récepteur de  $5 \times 5$ . La dixième couche contient également 56 cartes d'entités, dont chacune a une taille de  $6 \times 6$ .

Avant dernière couche est entièrement connecté avec 128 cartes de caractéristiques, toujours avec un champ réceptif de  $1 \times 1$ , la couche entièrement connecté est lié avec la couche de sortie pour donnée les résultats. La dernière couche qui est la cible du réseau. Les cibles 01 et 10 signifient respectivement la signature originale et la signature falsifiée.

<b>Couche</b>	<b>Taille</b>	<b>Autres paramètres</b>
Entrée	180*180*1	
CONV1	180*180*5	K=5, S=1, F=5
POOL1	90*90*5	K=2, S=2
CONV2	90*90*10	K=5, S=1, F=10
POOL2	45*45*10	K=2, S=2
CONV3	45*45*24	K=5, S=1, F=24
POOL3	23*23*24	K=2, S=2
CONV4	23*23*32	K=5, S=1, F=32
POOL4	12*12*32	K=2, S=2
CONV5	12*12*56	K=5, S=1, F=56
POOL5	6*6*56	K=2, S=2
FC1	128	128
Sortie	2	

Table 4.1: Couches du CNN

### 3. Résultats et comparaison les travaux:

Dans notre travail, nous avons utilisé CNN comme méthode de classification. Dans la signature Néerlandais nous avons obtenu un pourcentage 95.95% pour le test. Par contre, pour la signature Chinois nous avons obtenu 76.18% l'expérience sont effectuées plusieurs fois pour 785 époques sur la base de données ICDAR2011 sigcomp.

Nous comparons notre travail avec les travaux précédents dans ce domaine dans le tableau ci-dessous:

Classement	Les travaux	L'année	La base	Taux (%)	
01	<b>Khalajzadeh</b> <i>et al.</i>	2012	Signature Persan	99.85	
02	<b>Alvarez</b> <i>et al.</i>	2016	ICDAR2011	Chinois 95	Néerlandais 97
03	<b>Man</b> <i>et al.</i>	2018	/	95.60	
04	<b>Méthode</b> <b>Proposé</b>	2019	ICDAR2011	Chinois 76.18	Néerlandais 95.95
05	<b>Cozzens</b> <i>et al.</i>	2017	ICDAR2011	83.93	
06	<b>Sronothara</b> <i>et al.</i>	2018	GPDS-960	83	
07	<b>Multu Yapici</b> <i>et al.</i>	2018	GPDSSsynth- eticSignature	WI 62.5	WD 75

**Table 4.2:** Comparaison de différents travaux

### Conclusion

dans ce chapitre, après avoir achevé notre conception nous avons donné les outils des développements nécessaires pour la réalisation de notre travail. A la fin nous avons présenté notre approche de classification basée sur les réseaux de neurones convolutifs en donnant quelques explications du fonctionnement de notre travail, ainsi que les résultats obtenus.

---

# **Conclusion générale**

---

### **Conclusion générale :**

Les dernières années ont été marquées par une augmentation significative des recherches dans différents domaines de la biométrie.

Malgré le développement considérable des différentes modalités biométriques, les signatures sont restées le mécanisme d'authentification le plus largement accepté dans les documents juridiques et les transactions financières.

C'est dans ce cadre que s'inscrit notre travail, qui a pour objectif de proposer une application qui réalise et de renforcer la capacité de vérification de signature. Le système de vérification de signature hors ligne est développé pour distinguer les signatures authentiques ou falsifiées.

Pour réaliser notre travail de vérification on a utilisé l'apprentissage profond, la méthode d'apprentissage qui a montré ses performances ces dernières années et il est une partie supplémentaire des algorithmes d'apprentissage automatique et est donc classé dans une section plus large de l'intelligence artificielle, et nous avons choisi la méthode CNNs comme une méthode de classification pour la vérification de signature, ce choix est justifié par la simplicité et l'efficacité de la méthode et on peut s'attendre à ce que les CNN obtiennent des résultats nettement meilleurs que les autres réseaux pour de nombreuses tâches.

Dans ce travail, nous avons obtenu du taux 95.95% pour les signatures Néerlandais et 76.18% pour les signatures Chinoise sur la base de données ICDAR 2011 sigComp.

### **Perspectives :**

Les perspectives d'évolution de ce travail sont :

- Utiliser une méthode de classification après l'extraction des caractéristiques par le réseau de neurone à convolution comme SVM ou MLP.
- Nous pouvons apporter Des modifications au modèle proposé pour améliorer le résultat.
- Il serait très intéressant d'exploiter la combinaison de caractéristiques proposées dans ce mémoire avec celles de l'état de l'art afin d'améliorer les performances du système proposé.

---

# **Référence bibliographique**

---

**Référence bibliographie :**

- [1] BENCHENNANE Ibteissam "Etude et mise au point d'un procédé biométrique multimodale pour la reconnaissance des individus ", Diplôme de Doctorat en Sciences, Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, 2016.
- [2] PJames\_L.\_Wayman,\_Anil\_K.\_Jain,\_Davide\_Maltoni,\_Da\_Biometric Systems  
James\_L.\_Wayman,\_Anil\_K.\_Jain,\_Davide\_Maltoni,\_Da\_Biometric Systems.
- [3] Florent PERRONNIN, Jean-Luc DUGELAY, "Introduction à la Biométrie Authentification des Individus par Traitement Audio-Vidéo", Traitement du Signal 2002 – Volume 19 – n°4.
- [4] ZITOUNI Sif Eddine et SACI Abdelmoumen " Authentification et Identification biométrique des personnes par les empreintes palmaires", Mémoire MASTER ACADEMIQUE, UNIVERSITE KASDI MERBAH OUARGLA, 2016.
- [5] Walid BOUAMRA et Mohamed El Amine ZOGHBI "Vérification des signatures manuscrites et détection de falsification en utilisant des caractéristiques texturales", Mémoire de Master, Université Larbi Tébéssi –Tébessa, 2016.
- [6] B Schölkopf, AJ Smola " Learning with kernels: support vector "
- [7] Nuri Kasimov, Responsable Technique chez OQTOR, " Quelle est la différence entre l'intelligence artificielle, l'apprentissage machine, l'apprentissage profond et le traitement du langage naturel ?", Université de Grenoble Alpes (2012), Mis à jour 18 mai 2017 <https://fr.quora.com/Quelle-est-la-diff%C3%A9rence-entre-lintelligence-artificielle-lapprentissage-machine-lapprentissage-profond-et-le-traitement-du-langage-naturel>
- [8] W Gerstner, WM Kistler, " Spiking neuron models: Single neurons, populations, plasticity", Cambridge university press, 2002.
- [9] Pierre Buysens, "Fusion de différents modes de capture pour la reconnaissance du visage appliquée aux e\_transactions", DOCTORAT de l'UNIVERSIT'E de CAEN Le 4 Janvier 2011
- [10] Parizeau, Marc, Réseaux de Neurones (Le perceptron multicouche et son algorithme de retropropagation des erreurs). s.l.: Université Laval, 2004.
- [11] Mokri Mohammed Zakaria, "Classification des images avec les réseaux de neurones convolutionnels ", Mémoire de fin d'études, Université Abou Bakr Belkaid Tlemcen, 2017.
- [12] [http:// www.qingpingshan.com/bc/jsp/163284.html](http://www.qingpingshan.com/bc/jsp/163284.html)

## REFERENCE BIBLIOGRAPHIE

- [13] Boughaba Mohammed et Boukhris Brahim, " L'apprentissage profond (Deep Learning) pour la classification et la recherche d'images par le contenu ", Mémoire Master Professionnel, UNIVERSITE KASDI MERBAH OUARGLA, 2017.
- [14] Réseaux neuronaux récurrents et LSTM, <https://www.datasciencetoday.net/index.php/fr/machine-learning/148-reseaux-neuronaux-recurrents-et-lstm> , le 30 Avril 2019.
- [15] S.Adebayo Daramola, T. Samuel Ibiyemi, "Offline Signature Recognition using Hidden Markov Model (HMM) ", in International Journal of Computer Applications (0975 – 8887) Volume 10– No.2, November 2010.
- [16] Joël MINOT, Philippe GENTRIC, "Authentification dynamique de signatures par réseaux de neurones ", olume 8 - n° 6.
- [17] AHMED ABDELRAHMAN, AHMED ABDALLAH, "Signature Verification System Based on Support Vector Machine Classifier ",The International Arab Conference on Information Technology (ACIT'2013).
- [18] H. Khalajzadeh, M. Mansouri, and M. Teshnehlab, "Persian Signature Verification using Convolutional Neural Networks", in International Journal of Engineering Research and Technology, vol. 1. ESRSA Publications, 2012.
- [19] Gabe Alvarez, Blue Sheffer et Gabe Alvarez, "Offline Signature Verification with Convolutional Neural Networks" in 2016.
- [20] K. Simonyan, A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition" in ICLR 2015.
- [21] Brittany Cozzens, Richard Huang, Maxwell Jay, Kyle Khembunjong, Sahan Paliskara, Felix Zhan, Mark Zhang and Shahab Tayeb, " Signature Verification Using a Convolutional Neural Network" in 24 sep 2017.
- [22] Med Multu Yapici, Adem Tekerek and Nurettin Topaloglu, "Convolutional Neural Network Based Offline Signature Verification Application", in Ankara, Turkey, 3-4 Dec, 2018.
- [23] Seungsoo Nam, Hosung Park, Changho Seo 1 and Daeseon Choi, "Forged Signature Distinction Using Convolutional Neural Network for Feature Extraction ", 2018.
- [24] Marchi, E.; Vesperini, F.; Eyben, F.; Squartini, S.; Schuller, B. A novel approach for automatic acoustic novelty detection using a denoising autoencoder with bidirectional LSTM neural networks. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), South Brisbane, QLD, Australia, 19–24 April 2015; pp. 1996–2000.

## REFERENCE BIBLIOGRAPHIE

[25] A.Bhanu Sronothara and M. Hanmandlu, "Offline Signature Verification using CNN", in International Journal on Future Revolution in Computer Science & Communication Engineering, Volume: 4 Issue: 9, 23 sep 2018.

[26] TIAGO CARNEIRO, RAUL V. MEDEIROS DA NÓBREGA, THIAGO NEPOMUCENO, GUI-BIN BIAN, VICTOR HUGO C. DE ALBUQUERQUE, AND PEDRO P. REBOUÇAS FILHO," Performance Analysis of Google Colaboratory as a Tool for Accelerating Deep Learning Applications "

[27] Ceyhan-ayse «. Identité, identification et surveillance : enjeux à l'heure de la biométrie ». dans Actes du colloque organisé par la Bibliothèque Publique d'Information du Centre Pompidou, Identification et surveillance des individus. Quels enjeux pour nos démocraties ? Paris : Edition de la Bibliothèque Publique d'Information, pp.33-40, 2010.