

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

L'APPRENTISSAGE PROFOND POUR LA DÉTECTION DES SIGNAUX  
D'INTERFÉRENCE RADIO FRÉQUENTIELS

MÉMOIRE  
PRÉSENTÉ  
COMME EXIGENCE PARTIELLE  
DE LA MAÎTRISE EN INFORMATIQUE

PAR  
YOSR GHANNEY

SEPTEMBRE 2019

UNIVERSITÉ DU QUÉBEC À MONTRÉAL  
Service des bibliothèques

Avertissement

La diffusion de ce mémoire se fait dans le respect des droits de son auteur, qui a signé le formulaire *Autorisation de reproduire et de diffuser un travail de recherche de cycles supérieurs* (SDU-522 – Rév.07-2011). Cette autorisation stipule que «conformément à l'article 11 du Règlement no 8 des études de cycles supérieurs, [l'auteur] concède à l'Université du Québec à Montréal une licence non exclusive d'utilisation et de publication de la totalité ou d'une partie importante de [son] travail de recherche pour des fins pédagogiques et non commerciales. Plus précisément, [l'auteur] autorise l'Université du Québec à Montréal à reproduire, diffuser, prêter, distribuer ou vendre des copies de [son] travail de recherche à des fins non commerciales sur quelque support que ce soit, y compris l'Internet. Cette licence et cette autorisation n'entraînent pas une renonciation de [la] part [de l'auteur] à [ses] droits moraux ni à [ses] droits de propriété intellectuelle. Sauf entente contraire, [l'auteur] conserve la liberté de diffuser et de commercialiser ou non ce travail dont [il] possède un exemplaire.»

## REMERCIEMENTS

J'aimerais tout d'abord remercier mon directeur de recherche prof. Wessam Ajib pour son aide, ses encouragements, ses conseils, ses motivations et sa rigueur, qui m'ont beaucoup aidés pour la réalisation de ce travail.

Un grand merci au prof. René Jr Landry de m'avoir offert l'opportunité de travailler dans le projet AVIO-601.

Enfin, J'adresse une reconnaissance particulière à ma mère, mon frère, Seif et mes amis pour leur soutien moral tout au long de mes études et leur support quotidien indéfectible.

## TABLE DES MATIÈRES

LISTE DES TABLEAUX . . . . .	v
LISTE DES FIGURES . . . . .	vi
LISTE DES ABRÉVIATIONS . . . . .	vi
RÉSUMÉ . . . . .	ix
CHAPITRE I MISE EN CONTEXTE ET MOTIVATIONS . . . . .	1
1.1 Introduction . . . . .	1
1.2 Motivation . . . . .	2
1.3 Problématique . . . . .	4
1.4 Objectifs . . . . .	5
1.5 Méthodologie . . . . .	6
1.6 Contributions . . . . .	7
1.7 Plan du mémoire . . . . .	7
CHAPITRE II REVUE DE LITTÉRATURE . . . . .	9
2.1 Introduction . . . . .	9
2.2 État de l'art . . . . .	10
2.2.1 Concepts et domaines d'application . . . . .	10
2.2.2 Techniques de détection d'anomalies . . . . .	14
2.2.3 Techniques de détection des interférences RF . . . . .	20
2.3 Conclusion . . . . .	26
CHAPITRE III APPRENTISSAGE PROFOND . . . . .	27
3.1 Introduction . . . . .	27
3.2 Concepts généraux . . . . .	27
3.3 Approfondissement dans les réseaux de neurones convolutifs . . . . .	28
3.3.1 Les couches convolutives . . . . .	30
3.3.2 Les couches de non-linéarité . . . . .	32
3.3.3 Les couches de pooling . . . . .	32
3.3.4 Couches totalement connectées . . . . .	33
3.4 Algorithmes de détection d'objets et apprentissage automatique . . . . .	34
3.5 Conclusion . . . . .	38
CHAPITRE IV SOLUTION PROPOSÉE ET RÉSULTATS . . . . .	39
4.1 Introduction . . . . .	39
4.2 YOLOv1 . . . . .	39

4.3	YOLOv2 . . . . .	42
4.4	YOLOv3 . . . . .	42
4.5	Méthode de détection basée sur YOLOv3 . . . . .	45
4.6	Partie expérimentale . . . . .	48
4.6.1	Description de jeu de données . . . . .	48
4.6.2	Indicateurs de performance des algorithmes de détection des objets et paramètres d'expérimentation . . . . .	49
4.6.3	Résultats et discussion . . . . .	51
	RÉFÉRENCES . . . . .	56

## LISTE DES TABLEAUX

Tableau	Page
3.1 Innovations et limitations des algorithmes de détection des objets.	36
4.1 Amélioration de YOLOv2 (Redmon et Farhadi, 2016) . . . . .	42
4.2 Métriques d'évaluation de YOLOv3 avec $\text{IoU} = 0,25, 0,5$ et $0,7$ .	53

## LISTE DES FIGURES

Figure	Page
1.1 93% de l'industrie des satellites souffre des interférences. (Newtec et IRG., 2013) . . . . .	4
2.1 Un exemple d'anomalies dans un ensemble de données bidimensionnelles (Chandola <i>et al.</i> , 2009) . . . . .	11
3.1 Architecture de LeNet-5 (LeCun <i>et al.</i> , 1998) . . . . .	29
3.2 Fonctions d'activation ReLu et sigmoid . . . . .	32
3.3 Max pooling (Karpathy., 2013) . . . . .	33
4.1 Architecture de YOLOv1 (Redmon <i>et al.</i> , 2015). . . . .	40
4.2 Darknet-53 (Redmon et Farhadi, 2018). . . . .	46
4.3 Exemple de la phase d'annotation. . . . .	47
4.4 Le processus de détection des interférences RF. . . . .	47
4.5 Calcul de IoU (IoU, 2019). . . . .	51
4.6 Précision en fonction rappel. . . . .	53
4.7 Résultats de détection d'interférence. . . . .	53

## LISTE DES ACRONYMES

AP Précision moyenne (en anglais Average Precision)

CNN Réseau de Neurones Convolutifs (en anglais Convolutional Neural Networks)

CRIAQ Consortium de recherche pour l'innovation en aérospatiale du Québec (en anglais Consortium for Research and Innovation in Aerospace in Québec)

CRSNG Conseil de Recherches en Sciences Naturelles et en Génie du Canada (en anglais Natural Sciences and Engineering Research Council of Canada, NSERC)

FFT Fast Fourier Transform

FN Faux Négatif

FP Faux Positif

GNSS Systèmes de Positionnement par Satellites (en anglais Global Navigation Satellite System)

ILSVRC ImageNet Large Scale Visual Recognition Challenge

IoU Intersection of Union

KD Détection de kurtosis

KLT Karhunen-Loeve Transform

R-CNN Region-based Convolutional Neural Networks

ReLU Rectified Linear Units



RF Radio Fréquence

SSD Single Shot Detector

TF Temporel-Fréquentiel

VOC Visual Object Challenge

VP Vrai Positif

YOLO You Only Look Once

## RÉSUMÉ

L'élimination d'interférence radio-fréquentielle (RF) est nécessaire puisque cette interférence pénalise la performance des systèmes de communication sans fil. Pour cette raison, le projet AVIO-601 cherche à éliminer l'interférence RF en suivant un processus qui se décompose en plusieurs étapes. Dans le cadre du projet AVIO-601, ce travail propose une nouvelle approche permettant une détection des interférences RF dans les systèmes de communication sans fil qui est à la fois robuste et en temps réel. L'approche proposée est basée sur un algorithme d'apprentissage profond. L'utilisation de l'apprentissage profond est justifiée puisqu'il a montré des excellents résultats pour la détection des objets en plusieurs domaines d'application. L'approche proposée réussit à obtenir un bon compromis entre la performance en termes de taux de détection des interférences et la complexité algorithmique. Ce travail examine l'efficacité de l'approche proposée pour satisfaire nos exigences en utilisant des indicateurs de performance des algorithmes de détection des objets

**Mots clés :** interférence RF, apprentissage profond, algorithme de détection des objets

# CHAPITRE I

## MISE EN CONTEXTE ET MOTIVATIONS

### 1.1 Introduction

Avec la croissance fulgurante de l'utilisation des systèmes de communication sans fil, l'interférence en fréquence radio (en anglais Radio Frequency (RF) interference) est de plus en plus présente. Cette interférence est significativement nuisible aux opérateurs et aux utilisateurs de ces systèmes de communication sans fil et elle réduit la capacité de transmission de ces systèmes et la qualité des communications sans fil. Dans le but d'assurer toujours une communication sans fil fiable et efficace pour satisfaire les besoins des utilisateurs, l'élimination de l'interférence RF est un processus indispensable.

Ce chapitre commence par une mise en contexte de mon projet de maîtrise en explicitant les motivations de ce projet. En outre, la problématique que nous abordons dans ce projet, les objectifs projetés et la méthodologie suivie sont abordées. Les contributions réalisées sont aussi énumérées. À la fin de ce chapitre, le plan du mémoire est présenté.

## 1.2 Motivation

En raison de l'utilisation accrue des ondes radio dans les systèmes de communication sans fil, le spectre radio devient de plus en plus encombré. Cet encombrement est remarqué non seulement pour les communications terrestres mais aussi pour les communications par satellite et les communications spatiales. Par conséquent, les données transmises via des signaux RF utilisant les fréquences radio sont de plus en plus contaminées par des signaux d'interférence RF.

Malgré les efforts fournis par les organisations de planification et par les instances de régulation des bandes de fréquences, la présence de l'interférence RF reste encore un problème persistant. Cette interférence RF, qui pénalise fortement la performance des systèmes de communication sans fil, est de plus en plus présente dans la communication des systèmes sans fil comme dans la radioastronomie (van der Tol et van der Veen, 2005), la radiométrie micro-onde (Guner *et al.*, 2007) et dans les communications par satellites (Borio *et al.*, 2016). Selon (AVIO-601, 2018), les principales sources de l'interférence RF sont les erreurs humaines, la mauvaise installation, des équipements aux normes inférieures, la défaillance d'équipement, l'absence d'adhésion à des réglementations communes et à des standards industriels, une conception médiocre, des systèmes de transmission RF adjacents, des brouilleurs terrestres, des brouilleurs orbitaux, des programmes malveillants et l'usurpation de liaisons.

Une enquête menée par Newtec (Newtec et IRG., 2013), qui est illustrée à la figure 1.1, montre que 93% des opérateurs de satellite subissent des interférences RF ; 24% des opérateurs de satellite ont recours à des interférences RF chaque semaine ; et 17 % des opérateurs de satellites subissent quotidiennement l'expérience des interférences RF. Selon certaines estimations de groupes industriels, les pertes d'efficacité des communications causées par les interférences RF peuvent coûter jusqu'à 2 millions de dollars par an à un opérateur gérant une petite flotte

de satellites. Cette réduction des marges de bénéfices a motivé les entreprises industrielles et la communauté scientifique pour collaborer ensemble afin de surmonter ces dégâts. D'où le lancement du projet AVIO-601 qui regroupe plusieurs industriels (Thales Canada, TeleSat, Atem, Vigilant Global), et plusieurs universités (Université du Québec à Montréal, École de Technologie Supérieure (ÉTS), École Polytechnique, Université Concordia). Ce projet est financé par le CRSNG (Conseil de recherches en sciences naturelles et en génie du Canada), nos partenaires industriels et par le consortium CRIAQ (Consortium de recherche pour l'innovation en aérospatiale du Québec).

Le projet AVIO-601 soulève le problème de la mitigation des interférences RF dans les communications par satellites. Le projet AVIO-601 commence par définir la saturation des bandes de fréquence dans les communications par satellites (L / S / C / Ku), la raréfaction des ressources du spectre de RF des communications par satellites et l'augmentation des cas d'interférence comme principales sources des interférences RF. Le but de ce projet est de proposer et d'implémenter des approches de détection et d'élimination, ou du moins d'atténuation, des interférences RF afin d'améliorer la capacité de transmission du réseau, la qualité de service offerte aux utilisateurs des réseaux sans fil et l'efficacité de l'utilisation du spectre. Pour toutes ces raisons, le processus de mitigation des interférences RF constitue un problème épineux pour lequel AVIO-601 va chercher les méthodes les plus récentes pour détecter rapidement les interférences RF et neutraliser efficacement leurs effets néfastes. Plus spécifiquement, le projet va (i) développer un cadre technique pour détecter, identifier, caractériser rapidement un interféreur et géolocaliser la position de l'émetteur fautif ; (ii) créer un atlas complet des interférences RF, qui facilitera le partage du spectre et la gestion des brouillages ; (iii) développer des techniques de mesure, de surveillance et de mitigation des interférences RF. Pour conclure, le développement du projet comprendra les éléments suivants : détection des interférences, caractérisation des interférences, identification des in-

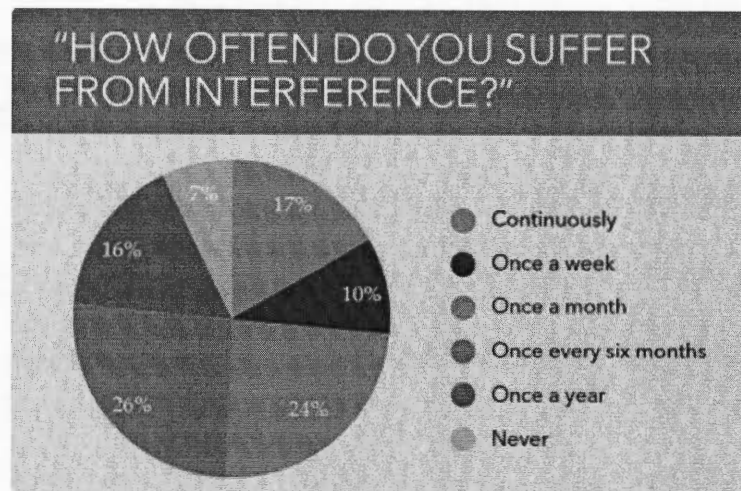


Figure 1.1 – 93% de l'industrie des satellites souffre des interférences. (Newtec et IRG., 2013)

terférences, géolocalisation des interférences et mitigation des interférences.

Dans ce cadre, ce présent mémoire s'intéresse à une partie essentielle du processus de mitigation des interférences RF qui est la détection.

### 1.3 Problématique

L'interférence RF dégrade les performances et la fiabilité de la communication par satellites et elle peut même conduire à une perte de données. Par conséquent, l'élimination des interférences devient de plus en plus obligatoire. Comme mentionné avant, le projet de maîtrise présenté dans ce mémoire s'intéresse à la résolution du problème de détection des interférences RF dans le cadre du projet AVIO-601. La détection d'interférence représente la première étape du processus de la chaîne de recherche. Comme elle déclenche le reste des procédures en chaîne, la détection de l'interférence RF joue un rôle critique. Si les interférences RF ne sont pas détectées, elles ne seront ni mesurées, ni caractérisées, ni localisées ou correctement

atténuées. Pour cette raison, la technique développée doit être capable de détecter les signaux de brouillage qui peuvent dégrader la qualité du trafic de communications par satellite.

Plusieurs solutions ont été développées pour résoudre le problème de détection des RF. Ainsi, ces solutions proposées peuvent être classées en six groupes selon la représentation adoptée de signal : solutions basées sur une représentation spectrale du signal (pour simplifier, ils portent le nom de solutions spectrales dans ce mémoire ; on utilise la même simplification pour le nom des autres solutions), solutions temporelles, solutions spectral-temporelles, solutions spatiales, solutions statistiques et solutions basées sur la transformation de domaine. Malgré la richesse de la littérature, la détection des interférences RF reste un domaine de recherche actif avec plusieurs défis. Ces défis sont difficiles à surmonter dû à une complexité de calcul ou à un manque de robustesse dans plusieurs algorithmes proposés (Getu *et al.*, 2017). En tenant compte de ces défis, ce travail cherche à résoudre le problème de détection des interférences RF via le développement d'une meilleure solution qui est à la fois simple, efficace, capable de détecter tous les types d'interférences et applicable à un large éventail de systèmes de communication sans fil.

#### 1.4 Objectifs

Dans ce mémoire, notre objectif est de proposer une solution intelligente capable de détecter à temps réel les différents types d'interférences RF dans les systèmes de communication sans fil, quelle que soit leur forme, c'est à dire capable de détecter les interférences RF à bande étroite, large bande, onde continue ou à impulsion. En effet, cette solution devrait aussi trouver le meilleur compromis entre la robus-

tesse et la complexité. Pour conclure, l’algorithme de détection des interférences RF à proposer devrait être :

- applicable à tous les types d’interférences,
- en temps réel,
- robuste, et
- de faible complexité.

## 1.5 Méthodologie

Ce mémoire traite le problème de la détection des interférences RF comme un problème de détection d’un objet et d’une classification binaire (1 signal contaminé par une interférence et 0 signal non contaminé). Une telle approche est traditionnellement traitée en concevant des caractéristiques conçues à la main, suivies d’un classificateur tel que les machines à vecteurs de support ou les forêts d’arbres décisionnels. Cependant, il est difficile de prendre en compte tous les caractéristiques des interférences RF complexes. D’autre part, l’utilisation de l’apprentissage profond offre généralement d’excellentes performances dans le domaine de traitement d’image (Krizhevsky *et al.*, 2012) et dans le domaine de la reconnaissance vocale (Sainath *et al.*, 2015, Hannun *et al.*, 2014). Par conséquent, dans ce mémoire, nous avons recours à l’utilisation de l’apprentissage profond, qui a démontré ces avantages pour capturer des mappages complexes en apprenant à partir d’exemples étiquetés. De nombreuses expériences scientifiques ont montré que les réseaux d’apprentissage profond possédaient une capacité impressionnante d’acquérir des informations et de détecter les cibles avec précision. Par rapport aux techniques traditionnelles, l’apprentissage profond présente l’avantage de pouvoir extraire de manière adaptative des caractéristiques profondes de données et d’obtenir une classification ou une détection de cible par le biais de réseaux de



neurones multicouches sans aucune connaissance préalable. Vu qu'on a un accès à une base de données réelles contaminées par des interférences RF et sachant que l'apprentissage profond est très gourmand du point de vue de l'utilisation des données pour entraîner son réseau, notre méthodologie consiste à appliquer un algorithme d'apprentissage profond afin de trouver une solution adéquate à notre besoin.

## 1.6 Contributions

Ce mémoire étudie le problème de la détection des interférences RF dans les systèmes de communication sans fil. Pour pallier ce problème, les contributions suivantes sont présentées. Ce mémoire :

- propose une solution robuste et de faible complexité, qui permet de détecter les différents types d'interférences RF. Cette solution est compatible avec tous les systèmes de communication sans fil.
- applique l'apprentissage profond afin d'atteindre cet objectif.
- utilise un jeu de données réelles pour tester la robustesse de la solution proposée.
- démontre via des métriques d'évaluation l'efficacité de la solution proposée.

## 1.7 Plan du mémoire

Le présent mémoire est organisé comme suit. Le chapitre 2 discute l'état de l'art du problème de détection d'anomalies particulièrement la détection des interférences RF dans les systèmes de communication sans fil. D'abord, il commence par définir la détection d'anomalies et quelques concepts en citant plusieurs techniques adaptées pour la détection d'anomalies. Ensuite, il présente un survol sur les travaux qui ont été faits dans le cadre de la détection d'interférences RF pour

la radiométrie, radioastronomie et les communications par satellite. Par la suite, une analyse critique à l'égard de ces approches est présentée. Le chapitre 3 montre une présentation des concepts généraux de l'apprentissage profond et ensuite, il se focalise sur les réseaux de neurones convolutifs (CNN) (LeCun *et al.*, 1989) et leurs domaines d'application. Le chapitre 4 détaille dans sa première partie la solution proposée et la méthodologie suivie ; tandis que la deuxième partie présente l'expérience faite pour l'évaluation de la solution proposée ainsi que les résultats obtenus. Le dernier chapitre présente les principales conclusions de ce mémoire et les possibilités de travaux futurs.

## CHAPITRE II

### REVUE DE LITTÉRATURE

#### 2.1 Introduction

Les systèmes de communication sans fil sont en plein essor ces dernières années vu leurs implications dans les domaines civils et militaires à travers plusieurs applications comme la surveillance, la télédétection, les télécommunications, etc. Par conséquent, le spectre de fréquences est devenu de plus en plus encombré. En raison de cet encombrement, l'interférence RF est devenue un problème courant pour les utilisateurs des systèmes de communication sans fil. Vu que l'interférence RF dégrade les performances des systèmes de communication sans fil, notre objectif est de proposer une solution qui permet d'avoir une communication fiable et robuste sans perdre beaucoup de données. Puisque les interférences RF montrent un comportement atypique par rapport au signal normal, la détection des interférences RF va être étudié dans ce présent mémoire comme un problème de détection d'anomalies. Afin de pouvoir proposer une solution adéquate à nos objectifs, il nous faut étudier et analyser les solutions proposées en effectuant une revue de littérature et apprendre les limites de ces solutions. Le but de ce chapitre est de donner au lecteur un aperçu général sur les techniques de détection d'anomalies et en particulier celles dédiées pour la détection des interférences RF. Ce chapitre commence par une définition générale de la détection d'anomalies

ensuite nous soulignons l'application de la détection d'anomalies dans plusieurs domaines d'application. Par la suite, nous catégorisons les techniques de détection d'anomalies. Dans ce qui suit, nous présentons un survol des différents travaux qui ont été réalisés par la communauté scientifique en ce qui concerne la détection d'anomalies pour détecter les interférences RF dans les systèmes de communication sans fil. Enfin, nous passons à une analyse critique afin de montrer les limites des approches proposées ou utilisées.

## 2.2 État de l'art

Dans cette section, nous commençons par définir le principe de la détection d'anomalies en énumérant quelques domaines d'application.

### 2.2.1 Concepts et domaines d'application

La détection d'anomalies s'occupe de l'identification des comportements atypiques dans les données. Elle vise à rechercher de modèles de données non conformes au comportement attendu (Chandola *et al.*, 2009). En d'autre terme, la détection d'anomalies consiste à trouver les objets qui sont différents par rapport à la majorité de jeux de données. La détection d'anomalies a été étudiée dans la communauté des statistiques dès le 19ème siècle (M.A., 1887). Au fil du temps, diverses techniques de détection d'anomalies ont été développées dans plusieurs communautés de recherche. Beaucoup de ces techniques ont été spécifiquement développées pour certains domaines d'application, tandis que d'autres sont plus génériques (Chandola *et al.*, 2009). Pour mieux comprendre le principe d'anomalies, la figure 2.1 illustre un exemple d'anomalies dans un ensemble de données bidimensionnelles. Les données ont deux régions normales,  $N1$  et  $N2$ , car la plupart des observations se situent dans ces deux régions. Les points remarquablement

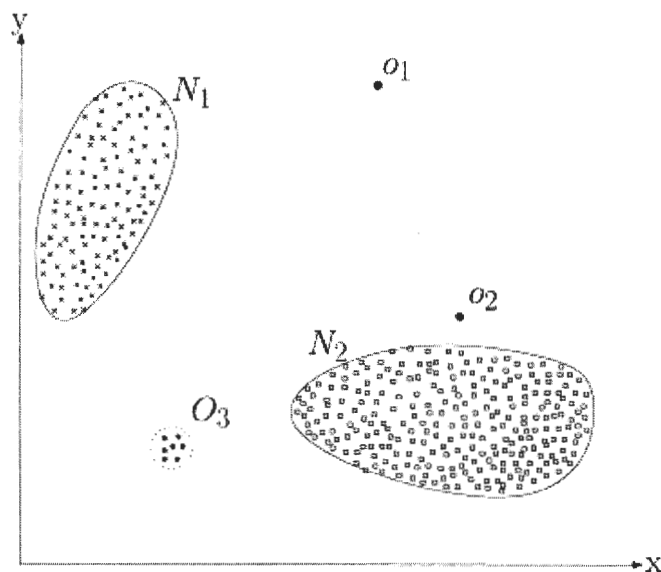


Figure 2.1 – Un exemple d’anomalies dans un ensemble de données bidimensionnelles (Chandola *et al.*, 2009)

éloignés de ces régions, par exemple les points  $o1$  et  $o2$  et les points de la région  $O3$ , sont des anomalies.

Il existe trois types d’anomalies : les anomalies ponctuelles, contextuelles et collectives. Il est important de bien identifier leur type pour ensuite choisir l’algorithme le plus adapté à leur détection. Le type d’anomalies considéré dépend du problème en question.

1. Anomalies ponctuelles : Une seule instance de données est anormale si elle s’écarte largement du reste des points de données.
2. Anomalies contextuelles : L’anomalie est spécifique au contexte car pour identifier si l’anomalie dépend de l’information contextuelle. Ce type d’anomalie est courant dans les données chronologiques.
3. Anomalies collectives : Si un groupe de données est anormal par rapport au reste des données, les données de ce groupe sont définies comme des anoma-

lies collectives. Si une collection d'instances de données liées est anormale par rapport à l'ensemble de données complet, mais pas de valeurs individuelles.

La détection d'anomalies a été largement appliquée dans plusieurs domaines d'application comme la détection d'intrusion pour détecter les tentatives qui contournent les mécanismes de sécurité d'un ordinateur ou d'un réseau, détection de fraude comme pour détecter les activités frauduleuses ou criminelles se produisant dans des organisations commerciales, diagnostic médical, traitement d'image, etc. Dans ce qui suit, une présentation brève de quelques domaines d'applications de la détection d'anomalies :

1. Pour la détection d'intrusion : la détection d'intrusion est probablement l'application la plus connue de la détection d'anomalie (García-Teodoro *et al.*, 2009) (Portnoy *et al.*, 2001) (Zarpelão *et al.*, 2017). Dans ce scénario d'application, les applications de trafic réseau et les serveurs sont surveillés. Les tentatives d'intrusion sont ensuite identifiées à l'aide d'algorithmes de détection d'anomalies. Un défi important dans ces systèmes de détection d'intrusion réside dans l'énorme quantité de données à traiter en temps quasi réel. Pour cette raison, ces systèmes utilisent généralement des algorithmes de détection d'anomalie simples mais rapides.
2. Pour la détection de fraude : la détection de fraude est une autre application de la détection d'anomalie très répandue vu la forte croissance des systèmes de paiement sur Internet et l'augmentation de l'offre de produits numériques (Abdallah *et al.*, 2016) (Wang, 2010). La détection de fraude désigne la détection d'activités criminelles se produisant dans des organisations commerciales comme les banques, les agences d'assurance, les sociétés de téléphonie mobile, etc. Les données sont analysées afin de détecter les utilisations suspects indiquant une fraude. En particulier, les transactions

par carte de crédit peuvent être utilisés pour détecter des cartes de crédit volées.

3. Détection d'anomalies médicale et de santé publique : dans les applications médicales et les sciences de la vie, la détection des anomalies est également utilisée. Un exemple est la surveillance des patients, où des signaux d'électrocardiographie (Lin *et al.*, 2005) ou d'autres capteurs corporels sont utilisés pour détecter des situations critiques pouvant mettre la vie en danger (Keogh *et al.*, 2006). De plus, la détection d'anomalie est utilisée pour analyser des images médicales, par exemple une tomodensitométrie afin de détecter des cellules anormales ou des tumeurs. Dans les sciences de la vie, la détection d'anomalies pourrait également être utilisée pour détecter des pathologies et des mutants.
4. L'analyse d'images : Dans ce cas, les données ont des caractéristiques spatiales et temporelles. Chaque point de données possède quelques attributs continus tels que la couleur, la luminosité, la texture, etc. Les anomalies intéressantes sont soit des points anormaux, soit des régions dans les images (anomalies ponctuelles et contextuelles). L'un des principaux défis dans ce domaine est la grande taille de l'entrée. Lorsqu'il s'agit de traiter des données vidéo, des techniques de détection d'anomalie en ligne sont nécessaires.
5. La détection des anomalies a été aussi appliquée sur les flux de données comme (Keogh *et al.*, 2005) (Rebbapragada *et al.*, 2009) (Pevný, 2016). Twitter utilise une méthode open source basée sur Seasonal Hybrid ESD (Hochenbaum *et al.*, 2017). Skyline est un autre projet open source populaire, qui utilise un ensemble de techniques statistiques pour détecter des anomalies dans les flux de données.

## 2.2.2 Techniques de détection d'anomalies

La détection d'anomalies est souvent menée à bien grâce à des techniques de statistiques, d'apprentissage machine et d'apprentissage profond, etc. Nous catégorisons les techniques de détection d'anomalies comme suit :

### 2.2.2.1 Techniques basées sur les statistiques :

Le principe de toute technique de détection d'anomalie basée sur les statistiques est le suivant : «Une anomalie est une observation soupçonnée d'être partiellement ou totalement dénuée de pertinence car elle n'est pas générée par le modèle stochastique supposé» (Anscombe, 1960). Autrement dit, les techniques de détection statistique des anomalies reposent sur l'hypothèse clé suivante : les données normales se produisent dans les régions à haute probabilité d'un modèle stochastique, tandis que les anomalies se produisent dans les régions à faible probabilité de ce modèle. Ça veut dire, les techniques statistiques ajustent un modèle statistique aux données fournies, puis appliquent un test d'inférence statistique pour déterminer si une instance non vue avant appartient à ce modèle ou non. Les instances ayant une faible probabilité d'être générées à partir du modèle appris, sur la base de la statistique de test appliquée, sont déclarées comme des anomalies.

Dans les techniques statistiques, l'activité de jeux de données est capturée en définissant son comportement stochastique. Deux ensembles de données sont pris en compte lors du processus de détection d'anomalies : Le comportement actuellement observé c'est à dire au moment de test, et le comportement statistique précédemment formé. Pendant la phase de test, le comportement actuel est déterminé en estimant un score d'anomalie par comparaison des deux comportements. Le score indique le degré d'irrégularité pour un événement spécifique, de sorte que le système de détection signale l'occurrence d'une anomalie lorsque le score



dépasse un certain seuil.

Les techniques de détection d'anomalies basées sur les statistiques peuvent être divisées en deux catégories (Markou et Singh, 2003) : des techniques paramétriques et non paramétriques. Alors que les techniques paramétriques supposent la connaissance de la distribution cachée et estiment les paramètres à partir des données fournies, les techniques non paramétriques ne supposent généralement pas la connaissance de la distribution cachée. Les approches statistiques paramétriques les plus classiques sont les approches qui consistent à élaborer des modèles statistiques probabilistes flexibles qui représentent la distribution des jeux de données testés comme les modèles gaussiens (Laxhammar *et al.*, 2009). Les paramètres sont estimés à l'aide d'estimations de vraisemblance maximale. Chaque objet reçoit un score d'anomalie qui caractérise sa déviation du modèle. Un score élevé signale une forte probabilité que l'objet en question soit une anomalie. Pour les approches statistiques non paramétriques, nous trouvons d'autres méthodes statistiques de détection d'anomalies comme les histogrammes et les fonctions à noyaux. Spécifiquement, les techniques à base d'histogrammes (Kind *et al.*, 2009) consistent à élaborer un profil fréquentiel des données. Les fonctions à noyau (Dit-Yan Yeung et Chow, 2002) offrent une approximation de la densité de distribution des données.

Les approches statistiques de la détection des anomalies présentent de nombreux avantages. Premièrement, ces systèmes, comme la plupart des systèmes de détection d'anomalies, ne nécessitent pas généralement une connaissance préalable. En outre, les approches statistiques peuvent fournir une notification précise des activités malveillantes qui se produisent souvent sur de longues périodes de temps. Cependant, les techniques de détection d'anomalies statistiques présentent également des inconvénients. Les attaquants qualifiés peuvent entraîner la détection des anomalies statistiques à accepter un comportement anormal comme normal. Il peut également être difficile de déterminer des seuils qui associent la probabilité

de faux positifs à la probabilité de faux négatifs. De plus, les méthodes statistiques ont besoin de distributions statistiques précises, mais tous les comportements ne peuvent pas être modélisés à l'aide de méthodes purement statistiques. En fait, une majorité des techniques de détection d'anomalie statistique proposées nécessitent l'hypothèse d'un processus quasi stationnaire, ce qui ne peut pas être supposé pour la plupart des données traitées par les systèmes de détection d'anomalie statistiques.

#### 2.2.2.2 Techniques de détection basées sur la théorie de l'information :

Les approches basées sur la théorie de l'information comme (Wenke Lee et Dong Xiang, 2001) introduisent un type différent de mesure de la normalité. L'hypothèse de base est que les anomalies modifient considérablement le contenu informationnel des données normales. Les entropies sont calculées globalement ou localement et leurs modifications sont évaluées afin de rechercher des données anormales. L'inconvénient principal de cette approche est le choix de la métrique spécifique qui est arbitraire et ne capture donc pas tous les types d'anomalies, en particulier les anomalies à court terme.

#### 2.2.2.3 Techniques de détection basées sur l'apprentissage machine traditionnelles :

Le processus d'apprentissage machine consiste à créer un modèle en se basant sur des exemples initialement disponibles, permettant de classer les nouveaux objets. En apprentissage supervisé, une étiquette est associée à chaque exemple (présence d'anomalie, absence d'anomalie), ce qui n'est pas le cas en apprentissage non supervisé qui se contente de regrouper (clustering) les objets selon leur ressemblance. Il est possible de traiter le problème de détection d'anomalie comme un problème

de classification supervisée lorsque nous disposons des labels des observations. Les techniques de détection des anomalies basées sur la classification fonctionnent de la même manière en deux phases. La phase d'apprentissage apprend un classificateur en utilisant les données de d'apprentissage étiquetées disponibles. La phase de test classe une instance de test comme normale ou anormale, à l'aide du classifieur.

— Approches supervisées :

Les réseaux de neurones ont été appliqués à la détection d'anomalies dans des environnements à une ou plusieurs classes. Nous citons par exemple le Replicator Neural Networks qui a été utilisé pour la détection d'anomalies à une classe (Hawkins *et al.*, 2002). Pour la détection d'anomalies à plusieurs classes, la technique de base est d'utiliser les réseaux de neurones fonctionnant en deux étapes. Premièrement, un réseau de neurones est entraîné sur les données d'entraînement normales pour apprendre les différentes classes normales. Deuxièmement, chaque instance de test est fournie en tant qu'entrée au réseau de neurones. Si le réseau accepte l'entrée de test, c'est normal et si le réseau refuse une entrée de test, il s'agit d'une anomalie (De Stefano *et al.*, 2000).

Les approches bayésiennes ont été utilisées pour la détection d'anomalies dans un environnement multi-classe. Une technique de base pour un ensemble de données catégorielles univariées utilisant un réseau bayésien naïf estime la probabilité a posteriori d'observer une étiquette de classe à partir d'un ensemble d'étiquettes de classe normales et de l'étiquette de classe d'anomalie, à partir d'une instance de données de test. L'étiquette de classe avec le plus grand postérieur est choisie comme classe prédite pour l'instance de test donnée. La probabilité d'observer l'instance de test étant donné une classe et la priorité sur les probabilités de classe est estimée à partir du jeu de données d'apprentissage.

Les machines à vecteurs de support (SVM) (Ratsch *et al.*, 2002) (Kun-Lun Li *et al.*, 2003). Bien que ces méthodes aient démontré leur efficacité dans diverses applications, elles risquent de ne pas bien fonctionner avec des séries chronologiques multivariées car elles ne peuvent pas saisir les dépendances temporelles de manière appropriée.

— Approches non supervisées :

Dans cette approche, les différents algorithmes tentent de distinguer les observations aberrantes en apprenant sur l'ensemble des données, sans avoir les labels des observations : il n'existe pas d'ensemble d'observations identifiées a priori comme anomalies. Les techniques basées sur le plus proche voisin sont les techniques les plus répandues dans le domaine de la détection d'anomalies non supervisée. Il existe deux catégories des techniques basées sur le plus proche voisin : méthodes basées sur la distance et méthodes basées sur la densité. L'hypothèse clé de l'approche basée sur la densité est que les anomalies sont localisées dans les régions de faible densité. Par contre, dans l'approche basée sur la distance, les anomalies sont loins et écartés de la majorité des autres points. Les approches basées sur la distance et l'approche basée sur la densité, sont inefficaces pour la gestion des caractéristiques non pertinentes ou des classes séparables non linéaires en raison de la malédiction de la dimensionnalité et de l'insuffisance de la capture des relations non linéaires.

#### 2.2.2.4 Les techniques de détection d'anomalies profonds

Les travaux les plus récents utilisent des réseaux de neurones profonds (Sabokrou *et al.*, 2017), qui ne nécessitent pas de construction de caractéristiques explicite contrairement aux méthodes mentionnées précédemment. Parmi les méthodes actuelles de détection des anomalies profondes les plus courantes sont les méthodes

basées sur les CNN, les méthodes basées sur un auto-encodeur et les méthodes basées sur des réseaux adverses génératifs (RAG). Une revue de littérature complète de l'utilisation des techniques supervisées plus précisément les CNN dans le domaine médical est présenté dans (Litjens *et al.*, 2017). Les algorithmes de détection d'anomalies non supervisés basés sur l'apprentissage profond (Zong *et al.*, 2018) (Zhai *et al.*, 2016) (Malhotra *et al.*, 2016) ont attiré beaucoup d'attention récemment. Le modèle de mélange gaussien à auto-encodage profond (Zong *et al.*, 2018) considère conjointement le modèle d'encodage automatique profond et le modèle de mélange gaussien pour modéliser la distribution de la densité de données multidimensionnelles. L'encodeur-décodeur Long short-term memory (LSTM) (Malhotra *et al.*, 2016) modélise la dépendance temporelle en série chronologique des réseaux LSTM et permet une meilleure capacité de généralisation que les méthodes traditionnelles. Malgré leur efficacité, ils ne peuvent pas prendre en compte conjointement la dépendance temporelle, la résistance au bruit et l'interprétation de la gravité des anomalies. L'utilisation des RAG pour la détection d'anomalies est relativement explorée (Schlegl *et al.*, 2017) (Zenati *et al.*, 2018), qui sont adaptés à la modélisation des distributions complexes à haute dimension de données du monde réel.

Nous mentionnons que les techniques présentées dans cette section ne représentent pas une liste exhaustive des méthodes de détection d'anomalies. Nous trouvons plusieurs autres techniques dans la littérature particulièrement dans (Chandola *et al.*, 2009)(Chalapathy et Chawla, 2019).

Afin d'éliminer les anomalies de signal RF, ce mémoire va traiter la détection des interférences RF en utilisant une détection supervisée des anomalies en impliquant l'apprentissage d'un classifieur binaire, à l'aide d'étiquettes d'instances de données normales et anormales. Notre approche de détection des interférences RF appartient à la classe des méthodes de détection d'anomalies supervisées. Le

but est de localiser cette anomalie dans une image de spectre du signal. Pour justifier notre choix, nous représentons, dans ce qui suit, une revue de littérature des différents techniques de la détection d'anomalies appliquées pour la détection des interférences RF en présentant ensuite leurs limites.

### 2.2.3 Techniques de détection des interférences RF

L'état de l'art en matière de détection des interférences RF englobe divers algorithmes. Ces algorithmes ont été proposés principalement pour les applications de la radiométrie, de la radioastronomie et les systèmes de positionnement par satellites (en anglais Global Navigation Satellite System ou GNSS). Nous divisons les approches proposées en deux parties : (i) des approches traditionnelles réactives et non adaptatives basées sur la technique utilisée pour présenter le signal et (ii) des approches intelligentes proactives et adaptatives basées sur les techniques de l'apprentissage machine. Dans la suite, certains de ces algorithmes sont brièvement présentés .

#### 2.2.3.1 Les approches de détection traditionnelles

les algorithmes de détection des interférences RF sont basées sur les statistiques de signal. Ces algorithmes peuvent être catégorisés en six groupes : algorithmes spectraux, temporels, spectraux-temporels, statistiques, de filtrage spatial et basés sur la transformation de domaine. Cette catégorisation est basée sur la manière utilisée pour représenter le signal.

### 2.2.3.1.1 Les algorithmes de détection spectraux

La liste suivante présente les exemples les plus répandus de cette catégorie d'algorithmes.

- L'algorithme de fréquences croisées (Johnson et Guner, 2007) (Guner *et al.*, 2007), est une technique de mitigation des interférences RF dans le domaine fréquentiel qui consiste essentiellement en trois opérations de seuillage en fonction de la fréquence. Lors de la première opération, les seuils de température de brillance absolue sont définis et les points situés en dehors de ces seuils sont ignorés. Ensuite, la moyenne et l'écart type des luminosités restantes sont calculés. Les points qui se situent en dehors de 5 écart-types par rapport à la moyenne sont également considérés comme corrompus. Toutes les luminosités corrompues sont ensuite remplacées par la luminosité moyenne obtenue. Enfin, les luminances à haute résolution spectrale (résolution de 0,1 MHz) sont intégrées en fréquence à une résolution de 10 MHz afin de produire un produit à faible résolution spectrale. Cette technique réussit à atténuer les faibles interférences RF. Néanmoins, elle est relativement efficace pour un grand nombre de canaux.
- Une approche d'estimation spectrale non paramétrique basée sur la méthode de Welch est proposée dans (Tani et Fantacci, 2008). L'algorithme de (Tani et Fantacci, 2008) repose sur une méthode de pré corrélation afin de détecter les interférences RF dans les systèmes GNSS.
- L'approche proposée dans (Chen *et al.*, 2010) permet de reconstruire l'interférence par l'estimation de la fréquence, l'amplitude et les paramètres de phase dans le spectre du signal. Ensuite, l'interférence reconstruite est soustraite du signal d'entrée. Cependant, la méthode proposée est impuissante pour la mitigation des interférences à large bande.

### 2.2.3.1.2 Les algorithmes de détection temporels

Dans le cas où le signal est représenté sous forme temporel, la méthode de la suppression d'impulsion asynchrone proposée en (Niamsuwan *et al.*, 2005) est la technique la plus répandue. Cette méthode permet de supprimer la partie dans laquelle l'amplitude du signal dépasse un certain niveau de seuil par rapport au bruit. Cette technique est efficace surtout pour les interférences à impulsion (Niamsuwan *et al.*, 2005). D'autre part, sa performance est sensible au choix de la valeur de seuil.

### 2.2.3.1.3 Les algorithmes de détection spectraux-temporels

L'interférence est estimée dans le domaine temporel-fréquentiel (TF) et ensuite soustraite du signal en suivant trois étapes : la représentation TF, l'unité d'estimation de fréquence instantanée et le filtre d'excision (Borio *et al.*, 2008). Dans ce cas, les filtres à réponse impulsionnelle infinie montrent de meilleures performances que les filtres à réponse impulsionnelle finie (Borio *et al.*, 2008).

### 2.2.3.1.4 Les algorithmes de détection basés sur la transformation de domaine

Les techniques de la transformation de domaine permettent d'obtenir une représentation du signal reçu dans des domaines différents. Après la transformation, la détection d'interférence est obtenue en comparant la nouvelle représentation avec un seuil prédéterminé. Dans ce cadre, Des algorithmes ont été développés pour les systèmes GNSS (Musumeci et Dovic, 2012) :

- La décomposition du signal en utilisant la transformée Wavelet (Dovic et Musumeci, 2011) permet la détection de fonctionnement dans chaque échelle de la décomposition des ondelettes. Ces échelles d'ondelettes sont



ensuite modifiées après la détection d'interférence et utilisées pour reconstruire le signal sans interférence en effectuant une transformée en ondelettes inverse.

- Karhunen-Loeve transform (KLT) est une transformation qui permet la décomposition du signal en utilisant des fonctions propres. Ces fonctions propres sont obtenues avec l'estimation de sa fonction d'auto-corrélation puis le calcul de la matrice de Toeplitz. Cette approche a montré des bonnes performances pour détecter les signaux très faibles cachés par le bruit (Musumeci et Dovic, 2012) (Dovic et Musumeci, 2016).

#### 2.2.3.1.5 Les algorithmes de détection statistiques

Quand le signal est représenté sous forme statistique, la méthode de la détection de kurtosis (KD) évalue le quatrième moment central d'un signal divisé par le carré de son deuxième moment central. Par la suite, cette méthode de détection considère les valeurs qui diffèrent de celles d'un signal distribué gaussien comme des interférences RF (Ruf *et al.*, 2006). KD repose sur le fait que le kurtosis d'une source gaussienne est de trois et, dans la plupart des cas, s'écarte de trois en présence d'une source d'interférence. Il est mentionné que les interférences qui ont une distribution gaussienne ou approximativement gaussienne sont impossibles à détecter en utilisant cette technique (Misra *et al.*, 2009).

#### 2.2.3.1.6 Les algorithmes de détection spatiaux

Les algorithmes de détection de l'interférence RF qui sont basés sur le filtrage spatial et les algorithmes d'excision estiment d'abord le sous-espace de l'interférence RF. Par la suite, ces algorithmes exécutent la projection du sous-espace des interférences RF estimé afin d'éliminer l'interférence RF. Pour effectuer l'estima-

tion de sous-espace cette interférence RF, la décomposition en valeurs propres de la matrice d'auto-corrélation de signal reçu (van der Tol et van der Veen, 2005) ou la décomposition en valeurs singulières (Jeffs *et al.*, 2005) de la matrice de corrélation croisée sont toujours utilisées.

#### 2.2.3.1.7 Limitations

Malgré la richesse de la littérature scientifique à ce sujet en utilisant des approches de traitement de signal traditionnelles, les divers algorithmes de détection des interférences RF présentent les limitations suivantes :

- La complexité : Les divers solutions proposées souffrent d'une énorme complexité de calcul induite par de nombreuses non-linéarités.
- Inadaptation à la détection à temps réel : Les algorithmes proposés ne fournissent pas une détection à temps réel.
- Détection pour un certain type des interférentes RF uniquement : Certaines techniques ne peuvent pas détecter les interférences RF gaussiennes (quasi gaussiennes) ; Par exemple, KD ne parvient pas à détecter les interférences RF gaussiennes (quasi gaussiennes) (Ruf *et al.*, 2006) (Misra *et al.*, 2009). Néanmoins, la détection des interférences RF doit être faite quel que soit le type des interférences RF.
- Applicabilité limitée : La plupart des solutions proposées ont été dédiées à une application bien spécifique comme la radioastronomie ou la radiométrie. Par contre, une solution est jugée meilleure s'elle peut être applicable à un large nombre des systèmes de communication sans fil et pour plusieurs applications .

### 2.2.3.2 Les approches de détection intelligentes

Les dernières années ont connues des avancées importantes dans les domaines de l'intelligence artificielle et de l'apprentissage automatique. Il est donc tout à fait naturel que la communauté scientifique s'intéresse à utiliser ces techniques et algorithmes d'apprentissage automatique au domaine du traitement de signal et notamment pour la détection de l'interférence RF. Dans la suite, nous discutons quelques exemples de ces travaux. Les auteurs de (Mosiane *et al.*, 2016) appliquent les techniques traditionnelles d'apprentissage automatique supervisées telles que les K-voisins les plus proches, les forêts d'arbres décisionnels et la classification naïve bayésienne pour classifier les signaux d'interférence RF. Ces algorithmes exigent un processus d'extraction des caractéristiques avant l'application d'un classificateur. Ce prétraitement consomme beaucoup de temps. En plus, il ne garantit pas une bonne extraction des caractéristiques profondes de données. Une approche basée sur la combinaison entre le réseau de neurones convolutifs et le Long Short-Term Memory (LSTM) a été proposée dans le but d'identifier les sources des interférences RF transitoires dans l'article (Czech *et al.*, 2018). D'un autre côté, les auteurs (Grunau *et al.*, 2018) proposent une classification multi-label des interférences RF. Cet approche est capable d'identifier plusieurs interférences RF en présence du signal utilisé en utilisant les réseaux de neurones convolutifs (CNN). Cette méthode permet juste de classifier les interférences RF sans les localiser. Les auteurs de (Akeret *et al.*, 2017) proposent d'utiliser un type particulier de réseaux de neurones convolutifs, nommé le U-Net, qui permet d'identifier et de mitiger les interférences RF. L'architecture de réseau de neurones a été entraîné par des données produites par simulation. La méthode proposée pourrait être plus intéressante avec l'utilisation d'un ensemble de données plus grand et avec une vérité au sol améliorée (ground truth) pour les données réelles. L'article (Zhang *et al.*, 2018) propose de détecter les interférences RF

dans le système de radar à ondes de surface à haute fréquence. En analysant les caractéristiques de la cible, les interférences dans les images radar sont détectés à l'aide d'un classificateur basé sur l'architecture CNN et nommé le Faster R-CNN.

Toutes ces approches adaptatives ont utilisé soit des données produites par des simulations pour tester la performance de leur méthode soit elles ont utilisé des petits jeux de données ou bien elles ont réussi à classifier les interférences RF sans les localiser . Dans ce mémoire, nous allons appliqué l'apprentissage profond sur un jeu de données plus large en utilisant des données réelles contaminées par plusieurs sources d'interférences RF afin d'obtenir une détection et une localisation des interférences RF plus performante.

### **2.3 Conclusion**

Ce chapitre a présenté une revue de littérature des principaux travaux de recherche en relation avec notre problématique, soit la détection d'anomalies en général, et en particulier la détection des interférences RF. Malgré le grand nombre de travaux qui traitent avec différents aspects le problème de la détection des interférences RF, plusieurs d'entre eux souffrent d'un certain nombre de limitations citées ci-dessus. Dans le chapitre suivant, nous allons passer à expliquer et justifier les outils utilisés pour le fondement de notre approche.

## CHAPITRE III

### APPRENTISSAGE PROFOND

#### 3.1 Introduction

Dans ce chapitre, nous présentons tout d'abord une brève introduction sur les concepts généraux de l'apprentissage profond, avec une emphase particulière sur les CNN ainsi que la détection profonde des objets en utilisant les CNN vu qu'elle va être utilisée dans ce mémoire comme un outil de détection des interférences RF. Ensuite, nous présentons une étude comparative des algorithmes de détection des objets pour justifier notre choix d'algorithme utilisé.

#### 3.2 Concepts généraux

L'apprentissage profond est une sous branche de l'apprentissage automatique (Goodfellow *et al.*, 2016) . Son architecture se base sur un réseau de neurones à plusieurs couches cachées dans le but d'imiter le fonctionnement du cerveau humain. Le concept d'apprentissage profond consiste à apprendre à travers plusieurs niveaux de représentation et d'abstraction qui aident à donner un sens aux données. En effet, les algorithmes d'apprentissage profond cherchent à exploiter la structure inconnue dans la distribution en entrée afin de découvrir de bonnes représentations, souvent à plusieurs niveaux, avec des fonctionnalités de niveau

supérieur apprises définies en termes de fonctionnalités de niveau inférieur (Bengio, 2012). L'histoire de l'apprentissage profond doit commencer par l'histoire des réseaux de neurones qui remonte à 1943, lorsque le neurophysiologiste Warren McCulloch et le mathématicien Walter Pitts ont modélisé un réseau de neurones simple à l'aide de circuits électriques (McCulloch et Pitts, 1943) afin de décrire le fonctionnement des neurones dans le cerveau. Passant après par la création de la perceptron en 1958, ensuite le premier réseau de neurones avec huit couches en 1971. En 1989, les scientifiques ont été en mesure de créer des algorithmes utilisant des réseaux de neurones profonds, mais le temps d'entraînement a été mesuré en jours, ce qui les rend pas pratiques pour une utilisation dans le monde réel. Grâce à l'énorme quantités de données auxquelles nous avons accès et au développement de la puissance de calcul des ordinateurs au milieu des années 2000, l'apprentissage profond a connu un vaste succès en montrant une performance exceptionnelle dans différents domaines d'application en matière de vision par ordinateur, de reconnaissance de la parole, de traitement du langage naturel et de reconnaissance audio, etc. Les réseaux de neurones convolutifs sont les architectures les plus connues dans l'apprentissage profond grâce à leurs résultats impressionnants. Dans ce qui suit, nous présentons une description détaillé des réseaux de neurones convolutifs.

### **3.3 Approfondissement dans les réseaux de neurones convolutifs**

Les réseaux de neurones convolutifs sont un type spécialisé de réseau de neurones pour le traitement de données possédant une topologie connue sous la forme d'une grille (Goodfellow *et al.*, 2016). Les réseaux de convolution sont simplement des réseaux de neurones qui utilisent la convolution à la place de la multiplication de matrice générale dans au moins une de leurs couches. Ces réseaux ont été inspirés par les travaux de Hubel et Wiesel (Wiesel et Hubel, 1963) sur le cortex

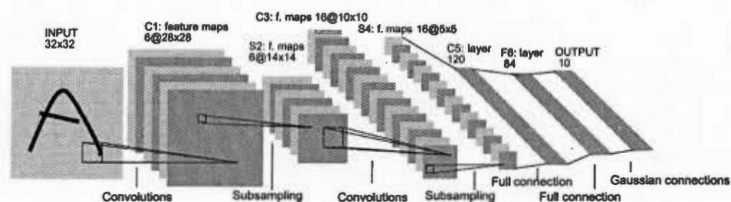


Figure 3.1 – Architecture de LeNet-5 (LeCun *et al.*, 1998)

visuel chez les mammifères, notamment au niveau de leur architecture ainsi que certaines de leur propriétés comme le partage des poids. Dans les années 1990, ces réseaux ont été popularisés avec les travaux de (LeCun *et al.*, 1998) sur la reconnaissance de caractères. Les CNN (LeCun *et al.*, 1998) conçus pour reconnaître directement les motifs visuels à partir d'images en pixels avec un minimum de prétraitement. Les CNN sont des réseaux en couches composés principalement de trois types d'opérations : (i) des opérations linéaires locales et invariantes dans l'espace (convolutions), (ii) des fonctions d'activation non linéaires et (iii) des opérations de sous-échantillonnage. L'opérateur de convolution balaie les unités de la couche précédente à la manière d'une fenêtre coulissante et transforme les entrées de manière linéaire en un espace de fonctions dicté par ses paramètres internes. Ceci est suivi d'une fonction d'activation non linéaire telle que sigmoïde ou ReLU. Le sous-échantillonnage spatial via la moyenne, le pooling maximal ou l'échantillonnage aléatoire est également utilisé à différentes étapes du réseau pour réduire la sensibilité de la sortie aux petits déplacements et aux variations de l'entrée. Les réseaux de neurones convolutifs font aussi souvent appel à des couches entièrement connectées pour résumer les caractéristiques locales de différentes régions d'image en représentations globales au niveau de l'image. Une architecture typique de réseaux de neurones convolutifs, le LeNet, est présenté dans la figure 3.1. Les réseaux de neurones convolutifs se basent sur trois idées architecturales clés :

- Des champs récepteurs locaux associés à des convolutions qui permettent de détecter des caractéristiques élémentaires d'image, formant ainsi une carte de caractéristiques (en anglais *feature map*).
- Un principe appelé partage des poids, qui consiste à apprendre les mêmes paramètres (ou poids) d'une convolution (et par conséquent extraire les mêmes caractéristiques) pour toutes les positions sur l'image. Ce principe représente l'idée clé des réseaux de neurones convolutifs, puisqu'il permet de réduire considérablement la complexité en diminuant le nombre de paramètres à apprendre. Il permet ainsi d'avoir des architectures multi-couches qui opèrent sur des entrées de grande dimension tout en étant de taille réaliste. De plus, le partage des poids permet d'améliorer les performances en terme de généralisation du réseau.
- Des opérations de sous-échantillonnage qui permettent de réduire le coût du traitement.

Les architectures des réseaux de neurones utilisant des convolutions permettent d'extraire des caractéristiques sous forme hiérarchiques, sous formes simples ou sous formes complexes, tout en ayant une certaine invariance sur leur position et taille dans l'entrée. Un réseau de neurones convolutif se compose de plusieurs couches que nous présentons ici :

### 3.3.1 Les couches convolutives

Les couches convolutives constituent le noyau du réseau convolutif. Une convolution est une opération linéaire qui implique la multiplication d'un ensemble de pondérations avec l'entrée. Les couches de convolution se composent d'une grille rectangulaire de neurones qui ont un petit champ réceptif étendu à travers toute la profondeur du volume d'entrée. Ainsi, la couche convulsive est juste une convolution d'image de la couche précédente, où les poids spécifient le filtre de convolution



(Frizzi *et al.*, 2017). Étant donné que la technique a été conçue pour une entrée en deux dimensions, la multiplication est effectuée entre un tableau de données en entrée et un tableau de poids en deux dimensions, appelé filtre de convolution. Ce filtre est plus petit que les données d'entrée et le type de multiplication appliqué entre une imagerie de l'entrée de la taille du filtre et le filtre est un produit scalaire. Un produit scalaire est la multiplication élément par élément entre l'imagerie de l'entrée et le filtre de la taille d'un filtre, qui est ensuite additionné, ce qui donne toujours une valeur unique. Comme il en résulte une valeur unique, l'opération est souvent appelée "produit scalaire". L'utilisation d'un filtre plus petit que l'entrée est intentionnelle, car elle permet de multiplier le même filtre (ensemble de pondérations) par le tableau d'entrée plusieurs fois à différents points de l'entrée. Plus précisément, le filtre est appliqué systématiquement à chaque partie superposée ou à chaque imagerie de la taille d'un filtre, de la taille d'un filtre, de gauche à droite et de haut en bas. Cette application systématique du même filtre sur une image est une idée puissante. Si le filtre est conçu pour détecter un type spécifique d'entité dans l'entrée, son application systématique sur l'ensemble de l'image en entrée offre au filtre une occasion de découvrir cette entité n'importe où dans l'image. Comme le filtre est appliqué plusieurs fois au tableau d'entrée, le résultat est un tableau à deux dimensions de valeurs de sortie représentant un filtrage de l'entrée. En tant que tel, le tableau de sortie bidimensionnel issu de cette opération s'appelle une «carte de caractéristiques». Une fois qu'une carte de caractéristiques est créée, nous pouvons transmettre chaque valeur de la carte de caractéristiques à une non-linéarité, telle qu'une ReLU. En résumé, nous avons une entrée, telle qu'une image de valeurs de pixel, et un filtre, qui est un ensemble de pondérations, et le filtre est systématiquement appliqué aux données d'entrée pour créer une carte de caractéristiques.

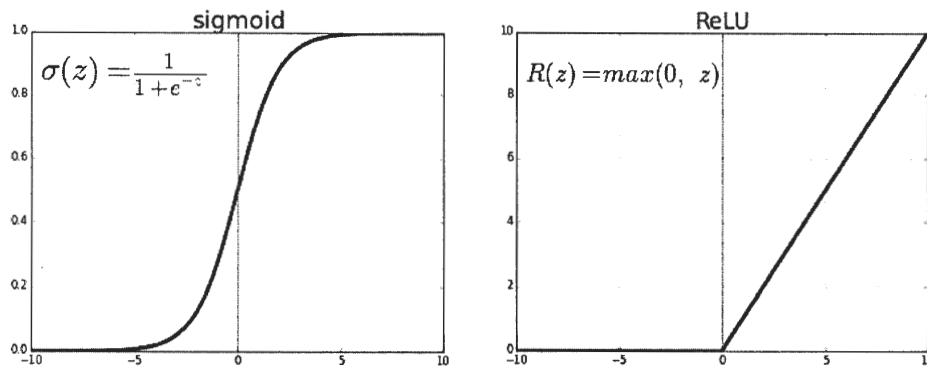


Figure 3.2 – Fonctions d’activation ReLu et sigmoid

### 3.3.2 Les couches de non-linéarité

Une couche de non-linéarité consiste en une fonction d’activation qui prend la carte de caractéristiques calculée et crée la carte d’activation en tant que sortie. Les non-linéarités les plus couramment utilisées dans CNN sont sigmoid et ReLu. La figure 3.2 illustre les deux fonctions d’activation.

### 3.3.3 Les couches de pooling

Une couche de pooling sous-échantillonne son entrée en préservant les informations les plus importantes qu’elle contient. En effet, après avoir procédé au pooling, l’image a un plus petit nombre de pixels qu’au départ. Il y a plusieurs façons pour faire ce sous échantillonnage, comme par exemple prendre la moyenne ou le maximum. Le max Pooling est la technique la plus répandue, parce qu’elle garde à chaque pas la valeur maximale contenue dans le filtre. Le pooling préserve les meilleures caractéristiques de ce filtre. La figure 3.3 montre le max pooling sur un filtre  $2 \times 2$  et un pas de 2.

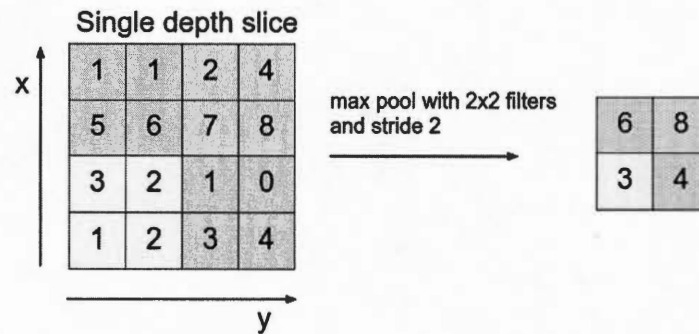


Figure 3.3 – Max pooling (Karpathy., 2013)

### 3.3.4 Couches totalement connectées

Après plusieurs couches de convolution et de pooling, le raisonnement de haut niveau dans le réseau de neurones se fait à travers des couches totalement connectées. Ces couches sont capables de faire une classification très spécifique en utilisant toutes les caractéristiques spécifiques détectées par les couches précédentes. Autrement dit, cette dernière couche du réseau permet de classifier l'image en entrée du réseau en envoyant un vecteur de taille  $N$ , où  $N$  est le nombre de classes du problème de classification. Chaque élément du vecteur indique la probabilité pour l'image en entrée d'appartenir à une classe. Par exemple, si le problème consiste à distinguer un signal d'interférence ou un signal sans interférence, le vecteur final sera de taille 2 : le premier élément (respectivement, le deuxième) donne la probabilité d'appartenir à la classe "interférence RF" (respectivement "absence d'interférence RF"). Ainsi, le vecteur  $[0.9 \ 0.1]$  signifie que l'image a 90 % représente une interférence RF.

### 3.4 Algorithmes de détection d'objets et apprentissage automatique

La détection des objets est considérée parmi les problèmes les plus difficiles dans le domaine de la vision par ordinateur. En effet, les algorithmes de détection d'objets offrent une compréhension complète de l'image puisque ils visent à la fois à classifier et à localiser les objets existants dans une image et à les étiqueter avec des traits rectangulaires en montrant le facteur de confiance de détection. La communauté de recherche scientifique dans le domaine de la vision par ordinateur a accordé une grande attention à ce problème en lançant des défis comme le PASCAL Visual Object Challenge ( VOC ) en 2005 et après le ImageNet Large Scale Visual Recognition Challenge (ILSVRC) en 2010. Le ILSVRC est devenu la référence en matière de détection des objets. En 2012, le défi a été marqué par un grand progrès au niveau de performances grâce à l'utilisation des réseaux de neurones convolutifs pour la première fois par (Krizhevsky *et al.*, 2012). Cette utilisation a réussi à une réduction des erreurs de classification de 26,2 % à 15,3 % et de l'erreur de localisation de 50 % à 34,3 %. Depuis ce moment, les architectures des réseaux de neurones convolutifs sont devenues la base de tous les algorithmes de détection des objets les plus puissants grâce à leurs architectures de plus en plus profondes qui permettent d'apprendre des fonctionnalités plus complexes. En 2014, l'erreur de classification s'affaiblit à 6,67% (Szegedy *et al.*, 2014). L'erreur de localisation est tombée à 25% grâce à (Simonyan et Zisserman, 2015) et la meilleure moyenne de la précision moyenne de détection (en anglais *mean Average Precision*(mAP)) est passée de 22,58% en 2013 à 43,93% en 2014. Les auteurs de (He *et al.*, 2015) ont réussi à affaiblir l'erreur de classification à 3,57% en 2015. Au cours des dernières années, avec l'augmentation continue du volume de données et la mise à jour constante du matériel des appareils, les algorithmes de détection basés sur apprentissage profond ne cessent d'obtenir des performances concurrentielles en temps réel par rapport aux méthodes traditionnelles et de

commencer à gagner la reconnaissance du secteur à l'échelle mondiale. Dans le milieu académique, en raison de l'importance accordée aux performances et à la précision en temps réel, les algorithmes de détection d'objets d'apprentissage en profond se sont progressivement développés dans plusieurs domaines d'application comme la détection faciale (Jiang et Learned-Miller, 2017), (Ranjan *et al.*, 2019) et la détection des piétons (Nguyen *et al.*, 2017), (Zhang *et al.*, 2016) dans les réseaux de trafic routier, la détection d'anomalies.

Selon (Zhao *et al.*, 2019), les algorithmes de détection se catégorise en deux parties :

- Les algorithmes de détection à deux étapes : la détection d'objet est faite en deux étapes. Ces algorithmes de détection des objets incluent une étape de prétraitement pour extraire les propositions de région, ensuite se focalise sur les régions d'intérêt.
- Les algorithmes de détection des objets à une étape est une méthode à étape unique proposée qui ne sépare pas la proposition de détection, ce qui rend le pipeline global à une étape plus rapide. Ces algorithmes sont basés sur une régression / classification globale, mappant directement à partir de pixels d'image aux coordonnées du cadre de sélection et aux probabilités de classe. Les algorithmes de détection d'objets à une étape sont axés sur la vitesse de détection contrairement aux algorithmes a deux étapes qui s'intéressent plus à la précision.

Le tableau 3.1 montre les innovations et les faiblesses de nombreux algorithmes de détection d'objets au cours des dernières années, notamment les algorithmes à deux et à une étapes.

Tableau 3.1 – Innovations et limitations des algorithmes de détection des objets.

Algorithme		Innovations	Limitations
À deux étapes	R-CNN (Girshick <i>et al.</i> , 2013)	Utilise un algorithme de recherche sélective afin d'extraire des régions de l'image appelées des propositions de région, puis, il classe les objets présents dans ces régions proposées.	La phase d'apprentissage coûte cher en espace et en temps. En plus, la phase de test est lente.
	Fast-RCNN (Girshick, 2015)	Propose que le CNN traite l'image entière en entrée au lieu de l'appliquer sur chaque région proposée (R-CNN).	La phase de test reste toujours lente pour la détection en temps réel.
	Faster-RCNN (Ren <i>et al.</i> , 2015)	Remplace l'algorithme de recherche sélective par le Region Proposal Network (RPN) qui permet de générer directement des propositions de région, prédire les cadres de sélection c'est à dire les cadres englobants des objets et détecter des objets.	N'arrive pas toujours à faire une détection en temps réel.

Suite du tableau 3.1

Algorithme		Innovations	Limitations
	R-FCN (Dai <i>et al.</i> , 2016)	Utilise un réseau de détection entièrement convolutionnel.	Toujours lent par rapport aux algorithmes de détection à une étape.
À une étape	YOLO (Redmon <i>et al.</i> , 2015)	Se base sur la régression et prédit les classes et les cadres de sélection pour l'ensemble de l'image en une seule exécution de l'algorithme. Une détection plus rapide par rapport aux algorithmes à deux étapes.	Faible précision de détection surtout pour les petits objets.
	SSD (Liu <i>et al.</i> , 2015)	Réussit mieux à détecter les petits objets grâce à une carte de caractéristiques multi-échelles pour la détection des objets.	La précision de la détection pour les petits objets reste toujours faible.
	YOLOv2 (Redmon et Farhadi, 2016)	Utilise le Darknet-19 pour extraire les caractéristiques avec la normalisation par lots en supprimant les couches entièrement connectées.	Faible précision de détection pour les petits objets.

Suite du tableau 3.1

Algorithme		Innovations	Limitations
	YOLOv3 (Redmon et Farhadi, 2018)	Utilise un nouveau réseau pour extraire les caractéristiques, le Darknet-53.	La précision de détection s'améliore mais reste toujours inférieure par rapport aux algorithmes à deux étapes.
	RetinaNet (Lin <i>et al.</i> , 2017a)	Utilise une nouvelle fonction de perte, la perte focale, qui focalise dans la phase d'apprentissage sur un nombre restreint des cas concrets et difficiles. Cette utilisation a amélioré beaucoup la précision de détection.	Lent par rapport aux YOLOV3 et SSD.

### 3.5 Conclusion

Dans le cadre de ce mémoire, les dernières avancées de l'apprentissage profond dans le domaine des algorithmes de détection vont être appliquées pour la détection et la localisation des interférences RF. Dans ce chapitre, nous avons présenté quelques avancées algorithmiques traitant la problématique de la détection des objets. Bien que les détecteurs à deux étapes offrent une grande précision dans la détection des objets, ils sont très lent en raison de leur coût de calcul élevé. Au lieu de cela, nous adoptons un détecteur à une étape qui offre le meilleur compromis entre la précision et la rapidité.



## CHAPITRE IV

### SOLUTION PROPOSÉE ET RÉSULTATS

#### 4.1 Introduction

Comme mentionné dans le chapitre précédent, ce mémoire utilise les avancés de l'apprentissage profond en matière d'algorithmes de détection des objets pour détecter et localiser l'interférence RF. Par conséquent, nous proposons dans ce chapitre d'appliquer l'algorithme de détection des objets qui offre le meilleur compromis entre la vitesse et la précision. En se basant sur une comparaison entre les algorithmes de détection les plus performants faite dans (Redmon et Farhadi, 2018), notre choix s'est porté sur You Only Look Once v3 YOLOv3 basé sur un réseau de neurones convolutifs. L'utilisation de cet algorithme est une première dans le domaine de détection des interférences. Le chapitre commencera par définir et détailler le YOLOv3 ensuite on décrira les étapes suivies pour la réalisation de la solution proposée. Enfin, l'efficacité de l'approche proposée sera testée en fonction des indicateurs de performance des algorithmes de détection d'objets.

#### 4.2 YOLOv1

L'architecture YOLOv1 a été présentée dans (Redmon *et al.*, 2015). Un seul réseau de neurones est utilisé pour prédire à la fois les boîtes englobantes et les



la fonction de perte suivante

$$\begin{aligned}
& \lambda_{coord} \sum_{i=0}^{S^2} \sum_{j=0}^B \mathbb{1}_{ij}^{obj} [(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2] \\
& + \lambda_{coord} \sum_{i=0}^{S^2} \sum_{j=0}^B \mathbb{1}_{ij}^{obj} [(\sqrt{w_i} - \sqrt{\hat{w}_i})^2 + (\sqrt{h_i} - \sqrt{\hat{h}_i})^2] \\
& + \sum_{i=0}^{S^2} \sum_{j=0}^B \mathbb{1}_{ij}^{obj} (C_i - \hat{C}_i)^2 \\
& + \lambda_{noobj} \sum_{i=0}^{S^2} \sum_{j=0}^B \mathbb{1}_{ij}^{noobj} (C_i - \hat{C}_i)^2 \\
& + \sum_{i=0}^{S^2} \mathbb{1}_{ij}^{obj} \sum_{c \in \text{classes}} (p_i(c) - \hat{p}_i(c))^2
\end{aligned} \tag{4.2}$$

where

$$\mathbb{1}_{ij}^{obj} = \begin{cases} 1, & \text{if there is an object.} \\ 0, & \text{otherwise,} \end{cases} \tag{4.3}$$

$\mathbb{1}_{ij}^{noobj}$  est la fonction inverse de  $\mathbb{1}_{ij}^{obj}$ ,  $\lambda_{coord}$  et  $\lambda_{noobj}$  sont des constants pour augmenter la perte de la prédiction des coordonnées du cadre de sélection et réduire la perte de la prédiction de la confiance pour les boîtes ne contenant pas d'objets. YOLOv1 était plus rapide que la plupart des approches existantes pour la détection d'objet, il avait un mAP relativement faible de 57,9% sur l'ensemble de tests VOC 2012.

Tableau 4.1 – Amélioration de YOLOv2 (Redmon et Farhadi, 2016)

	YOLO								YOLOv2
batch norm ?		✓	✓	✓	✓	✓	✓	✓	✓
hi-res classifier ?			✓	✓	✓	✓	✓	✓	✓
convolutional ?				✓	✓	✓	✓	✓	✓
anchor boxes ?				✓	✓				
new network ?					✓	✓	✓	✓	✓
dimension priors ?						✓	✓	✓	✓
location prediction ?						✓	✓	✓	✓
pass through ?							✓	✓	✓
muti-scale ?								✓	✓
hi-res detector ?									✓
VOCO2007 mAP	63,4	65,8	69,5	69,2	69,6	74,4	75,4	76,8	<b>78,6</b>

### 4.3 YOLOv2

Le modèle amélioré YOLOv2 a été introduit dans (Redmon et Farhadi, 2016). Cette version est meilleure, plus rapide et plus puissante de YOLOv1. Cette amélioration des performances est expliquée grâce à l'ajout de la normalisation par lots et l'utilisation des images avec une résolution supérieure pour entraîner le réseau. Les auteurs ont également supprimé les couches entièrement connectées et utilisé des boîtes d'ancrage pour prévoir les boîtes englobantes, ce qui a entraîné une légère diminution de la mAP de 69,5% à 69,2%, mais elle a également augmenté le rappel de 81% à 88%. Nous pouvons voir comment les changements appliqués ont amélioré les performances du réseau dans le tableau 4.1.

### 4.4 YOLOv3

L'algorithme YOLOv3 (Redmon et Farhadi, 2018) est une extension de l'algorithme YOLO qui offre un meilleur compromis entre la vitesse et la précision en appliquant les modifications nécessaires. Les performances de l'algorithme YOLO

v3 le rendent le plus utile en ingénierie par rapport aux autres algorithmes de détection d'objets. Cet algorithme appartient à la famille des algorithmes de détection d'objets génériques. L'objectif de la détection d'objet générique est de localiser et de classifier des objets existants dans une image donnée, et à les étiqueter avec des cadres de sélection rectangulaires pour montrer les valeurs de confiance de l'existence (Liu *et al.*, 2018). YOLOv3 présente plusieurs avantages par rapport aux algorithmes basés sur l'utilisation de classificateurs. YOLOv3 examine l'ensemble de l'image au moment du test afin que ses prédictions soient influencées par le contexte global de l'image. Il effectue également des prévisions avec une seule évaluation de réseau, contrairement aux autres systèmes à deux étapes tels que les réseaux de neurones convolutifs basés sur les régions (dit R-CNN), qui nécessitent des milliers d'images pour avoir des prévisions pour une seule image. Cela rend l'algorithme YOLOv3 extrêmement rapide, plus de 1000 fois plus rapide qu'avoir des prévisions pour les réseaux de neurones convolutifs basés sur les régions (dit R-CNN) R-CNN et 100 fois plus rapide que Fast R-CNN. YOLOv3 est également meilleur que le Single Shot Detector (SSD) en ce qui concerne la rapidité et la précision de la détection. Pour comprendre le processus de détection des interférences RF, il est nécessaire d'abord de comprendre les caractéristiques et la conception de l'algorithme YOLOv3 utilisé. Donc, cette partie se focalise sur la description de l'algorithme YOLOv3. L'approche de cet algorithme consiste à appliquer un réseau qui divise l'image en régions et prédit des boîtes englobantes et des probabilités pour chaque région. Ces boîtes englobantes sont pondérées par les probabilités prédites. L'algorithme utilise la détection d'objets comme problème de régression pour le traitement de bout en bout (en anglais *end-to-end*) et utilise des réseaux plus profonds pour la prédiction multi-échelle. La complexité de la formation en réseau a été simplifiée par rapport aux anciennes versions de l'algorithme YOLO. La rapidité de détection, le taux de précision ont été aussi améliorés, ce qui garantira une meilleure détection des interférences. Les

caractéristiques de l'algorithme YOLOv3 qui nous poussent à l'utiliser peuvent être résumées comme suit :

- L'utilisation de la classification multi-étiquettes c-à-d plusieurs étiquettes peuvent être attribuées à chaque instance.
- L'architecture bénéficie de connexions de saut résiduelles et de suréchantillonnage.
- La v3 effectue des détections permettant de prédire des tenseurs 3D à trois échelles différentes. Les trois échelles sont conçues pour détecter des objets de différentes tailles. YOLOv3 extrait des caractéristiques de ces échelles en utilisant un concept similaire à celui des réseaux pyramidaux (Lin *et al.*, 2017b). La dimension de tenseur 3D est :

$$N \times N \times (B \times (4 + 1 + C)), \quad (4.4)$$

avec :

- N la taille de l'échelle ;
- B le nombre de cadres de sélection qu'une cellule de la carte de caractéristiques peut prédire ;
- 4+1 correspondant aux 4 attributs du cadre de sélection et à la confiance d'un objet ;
- C le nombre de classes qui, dans notre cas, est égal à 2.
- L'utilisation de plusieurs classificateurs logiques indépendants et le calcul de la perte de classification à l'aide de la perte d'entropie croisée binaire afin de résoudre le problème de chevauchement possible entre plusieurs étiquettes (la boîte de prédiction peut contenir plus d'une catégorie) au lieu de softmax qui attribue des probabilités décimales à chaque classe d'un problème à plusieurs classes.
- L'extracteur de caractéristiques Darknet-53 spécialisée dans la détection

rapide d'objets, combinant les idées d'autres réseaux de neurones convolutifs, est utilisé. La figure 4.2 montre l'architecture de Darknet-53. Darknet est un framework pour l'apprentissage de réseaux de neurones, il est open source et écrit en C / CUDA et sert de base à YOLO. Darknet est utilisé comme cadre pour la formation de YOLO, ce qui signifie qu'il définit l'architecture du réseau. Darknet, est étendu dans cette version pour avoir 53 couches convolutives d'où le nom Darknet-53.

#### 4.5 Méthode de détection basée sur YOLOv3

La détection des interférences RF basée sur YOLOv3 est conçue en traitant des images de spectre des signaux RF de format JPG vu que l'amplitude d'un signal augmente à la présence des interférences RF ce qui facilite leur détection en utilisant les algorithmes de détection des objets. La première étape est la phase d'annotation des images qui consiste à la préparation manuelle de l'ensemble de données en étiquetant les images de la phase d'entraînement. Cette préparation manuelle est coûteuse et prend beaucoup de temps. L'étape d'annotation consiste à identifier l'objet d'intérêt en utilisant des boîtes englobantes qui sont des boîtes rectangulaires dont l'intérieure comprend l'objet recherché. Dans notre cas, les régions contaminées par des interférences RF sont notre objet d'intérêt pour cette raison nous les identifions avec les boîtes englobantes de vérité terrain (en anglais *ground truth*). Ces régions sont étiquetées séparément même si elles apparaissent dans la même image. La figure 4.3 illustre un exemple de la phase d'annotation. Cette figure présente la transformée de Fourier rapide (en anglais *Fast Fourier Transform*, FFT) des données réelles obtenues par l'une des antennes du Very Large Array (VLA). Les encadrés sont les boîtes englobantes qui contiennent les régions dans lesquelles les interférences RF sont localisées. Après avoir préparé l'ensemble de données étiquetées, nous l'utilisons ensuite comme entrée pour l'al-

	Type	Filters	Size	Output
	Convolutional	32	$3 \times 3$	$256 \times 256$
	Convolutional	64	$3 \times 3 / 2$	$128 \times 128$
1x	Convolutional	32	$1 \times 1$	
	Convolutional	64	$3 \times 3$	
	Residual			$128 \times 128$
	Convolutional	128	$3 \times 3 / 2$	$64 \times 64$
2x	Convolutional	64	$1 \times 1$	
	Convolutional	128	$3 \times 3$	
	Residual			$64 \times 64$
	Convolutional	256	$3 \times 3 / 2$	$32 \times 32$
8x	Convolutional	128	$1 \times 1$	
	Convolutional	256	$3 \times 3$	
	Residual			$32 \times 32$
	Convolutional	512	$3 \times 3 / 2$	$16 \times 16$
8x	Convolutional	256	$1 \times 1$	
	Convolutional	512	$3 \times 3$	
	Residual			$16 \times 16$
	Convolutional	1024	$3 \times 3 / 2$	$8 \times 8$
4x	Convolutional	512	$1 \times 1$	
	Convolutional	1024	$3 \times 3$	
	Residual			$8 \times 8$
	Avgpool		Global	
	Connected		1000	
	Softmax			

Figure 4.2 – Darknet-53 (Redmon et Farhadi, 2018).



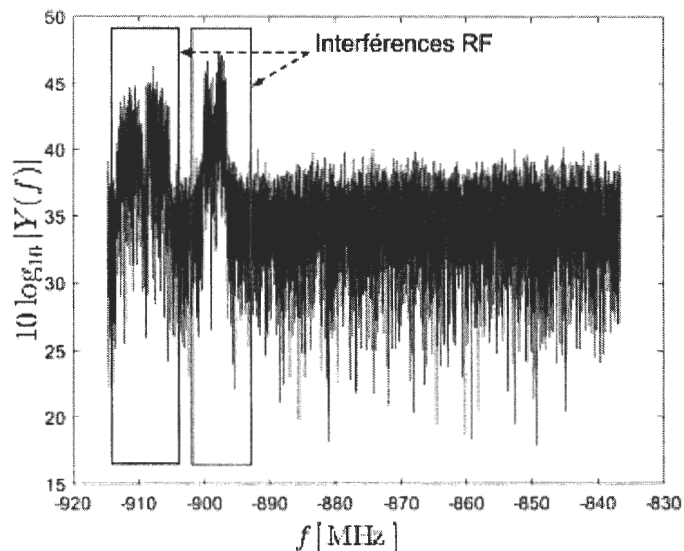


Figure 4.3 – Exemple de la phase d’annotation.

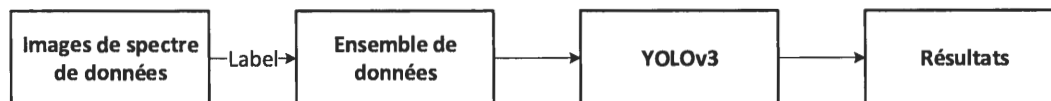


Figure 4.4 – Le processus de détection des interférences RF.

gorithme YOLOv3 afin de l’entraîner. Après la phase d’apprentissage, nous testons notre modèle en utilisant des images du jeu de données de test et nous analysons les résultats contenant des boîtes de prédiction et des étiquettes. Ce processus de détection décrit ci-dessus est illustré dans la figure 4.4.

## 4.6 Partie expérimentale

### 4.6.1 Description de jeu de données

Les jeux de données ont joué un rôle extrêmement important tout au long de l'histoire de la recherche sur l'utilisation de l'apprentissage automatique supervisé pour la détection des objets. Ils ont été l'un des facteurs les plus importants des progrès considérables accomplis dans ce domaine, non seulement en tant que base commune de mesure et de comparaison des performances d'algorithmes concurrents, mais également en poussant l'utilisation de l'apprentissage automatique supervisés à des applications et à des problèmes de plus en plus complexes et difficiles. La préparation de jeu de données est considérée comme une étape importante dans notre processus de détection des interférences RF. Dans ce mémoire, nous préparons notre propre jeu de données en nous basant sur des images de spectre des données réelles RF. Ces images sont obtenues après avoir transformé des données réelles binaires enregistrées à partir d'un convertisseur analogique-numérique contaminé par des interférences RF dans le monde réel à l'aide d'un code MATLAB. Ces données sont reçues par l'une des antennes du Very Large Array (VLA) de l'observatoire national de la radio astronomie aux États Unis (en anglais *National Radio Astronomy Observatory*, NRAO) (NRAO, 2019). Le code MATLAB permet de représenter le spectre des données reçues et échantillonnées à une fréquence d'échantillonnage de 2048 MHz en utilisant la transformée de Fourier rapide (en anglais *Fast Fourier Transform*, FFT) et diviser le spectre résultant en images qui s'étendent sur des fréquences pour construire la base de données.

La partie expérimentale de notre étude contient dans la phase d'apprentissage 15448 images annotées avec 13005 interférences RF étiquetées alors que la phase

de test contient 3862 images avec 1548 interférences RF.

#### 4.6.2 Indicateurs de performance des algorithmes de détection des objets et paramètres d'expérimentation

Afin d'évaluer l'approche proposée, nous considérons les critères d'évaluation suivants :

–VP : le nombre de vrais positifs, c-à-d, le nombre d'interférences RF correctement identifiées.

–FP : le nombre de faux positifs, c-à-d, le nombre de signaux non contaminés par des interférences RF mais identifiés comme des signaux contaminés.

–FN : le nombre de faux négatifs, c-à-d, le nombre des signaux contaminés par des interférences RF mais identifiées comme des signaux non contaminés.

–Précision : ce paramètre indique dans quelle proportion la détection d'interférence RF est réellement correcte. Ce paramètre est calculé selon l'équation suivante.

$$Precision = \frac{VP}{VP + FP} \quad (4.5)$$

–Rappel : ce paramètre décrit la proportion d'interférences RF détectées c-à-d à quel point l'algorithme YOLOv3 réussit à trouver tous les signaux contaminés par des interférences RF. Le paramètre Rappel est donné par l'équation suivante :

$$Rappel = \frac{VP}{VP + FN} \quad (4.6)$$

–La courbe de Précision-Rappel (PR) : cette courbe montre le compromis entre la précision et le rappel pour différents seuils. Une zone haute sous la courbe représente à la fois un rappel élevé et une précision élevée, où une précision élevée

correspond à un faible taux de faux positifs et un rappel élevé correspond à un faible taux de faux négatifs. Des scores élevés pour les deux montrent que le classificateur renvoie des résultats précis (haute précision), ainsi que la majorité des résultats positifs (rappel élevé).

–Précision moyenne (en anglais *Average Precision* ou AP) : ce paramètre est une métrique standardisée qui permet d'évaluer les performances de la détection d'interférence RF. Plus concrètement, il s'agit de l'aire sous la courbe de Précision-Rappel (PR). Plus la valeur de AP est élevée, meilleure est la performance.

Afin d'évaluer l'approche proposée, nous considérons les paramètres d'expérimentation suivants :

–Le rapport intersection sur union (en anglais *Intersection over Union* ou IoU) : Lorsqu'une interférence RF est prédite, une boîte de délimitation apparaît autour de signal d'interférence RF en question. D'autre part, le jeu de données contient les boîtes de délimitation avec la vérité terrain, c'est-à-dire les coordonnées exactes de la boîte de délimitation. L'indicateur IoU est le quotient entre la surface de chevauchement de ces deux boîtes de délimitation et l'addition de leur surfaces conjointes. La figure 4.5 détaille le principe de calcul de l'IoU. Donc, pour déterminer si la prédiction est un vrai positif ou un faux positif, il faut mesurer l'IoU. L'IoU est simplement le rapport entre la zone de chevauchement entre la boîte englobante de vérité au sol et la boîte englobante prédite, et la zone englobée à la fois par la boîte englobante de vérité au sol et par la boîte englobante prédite. Si l'IoU dépasse un seuil prédéfini, la prédiction est considérée comme vraie. Sinon, c'est un faux positif. Pour l'évaluation, nous avons choisi des différentes valeurs de IoU.

–Seuil de confiance (SC) : ce paramètre indique le niveau de confiance que le

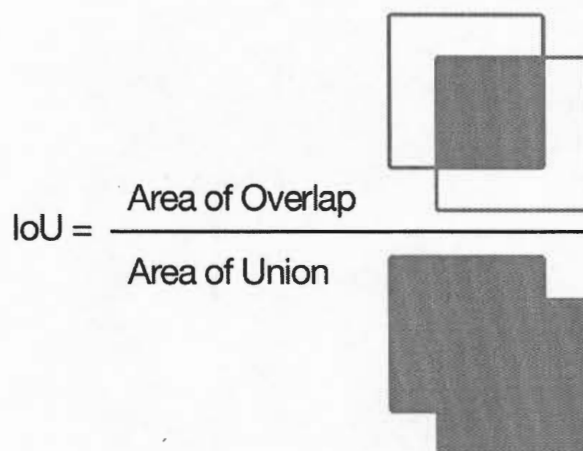


Figure 4.5 – Calcul de IoU (IoU, 2019).

réseau doit avoir pour pouvoir classer une caractéristique comme une interférence RF dans notre cas. L'utilisation d'une valeur petite pour le seuil de confiance permet d'accepter d'avantage d'objets, mais augmente la probabilité de détecter des objets erronés.

#### 4.6.3 Résultats et discussion

L'expérimentation de test est réalisée sur un NVIDIA GeForce GTX 1080 Ti. Nous ré-entraînons l'algorithme YOLOv3 en utilisant des poids pré-entraînés sur Imagenet (Deng *et al.*, 2009). L'algorithme du gradient stochastique est choisi comme optimiseur durant la phase d'apprentissage. Quand la phase d'apprentissage est terminée, le réseau est utilisé comme détecteur d'interférences RF. L'approche proposée est évaluée en utilisant les critères d'évaluation décrits ci-dessus. Pour tester l'efficacité de notre solution proposée, le calcul des valeurs de rappel, précision et précision moyenne sera effectué en utilisant différents seuils de confiance (SC). La valeur du seuil de confiance dans cette expérience varient de 0,2 à 0,6. Les valeurs de rappel, de la précision et de la précision moyenne ont été calculées

aussi en utilisant différentes valeurs de IoU allant de la valeur 0,25 (chevauchement de 25 % entre la boîte de délimitation de prédiction et celle de la vérité terrain) à 0,7. Les performances du réseau de neurones pour tous les seuils de confiance et les différentes valeurs de IoU utilisés sont résumées dans le tableau 4.2. Les seuils de confiance les plus faibles produisent généralement des valeurs de rappel plus élevées, mais des précisions plus faibles. Quand la valeur de IoU diminue, la valeur du rappel et de la précision s'améliorent. La figure 4.6 illustre la courbe de Précision-Rappel en se basant sur les valeurs de précision et rappel du tableau 4.2. Cette figure montre une zone haute sous la courbe ce qui prouve que l'algorithme Yolov3 a réussi de détecter les interférences RF avec un rappel élevé et une précision élevée. La figure 4.7 illustre des exemples de détection des interférences RF pour démontrer la capacité de l'algorithme YOLOv3 entraîné à la détection avec un temps de traitement par image moyen d'environ 0,9 s pour la configuration matérielle décrite. La figure 4.7 montre que notre solution proposée a réussi à détecter rapidement l'interférence RF avec un coefficient de confiance de détection qui atteint 100%. Les résultats indiquent que l'algorithme YOLOv3 est capable de détecter les interférences RF rapidement et avec une précision très élevée. Comme prévu, quand les valeurs du seuil de confiance sont plus élevées, les résultats sont plus fiables (en d'autres mots, la valeur de la précision augmente), mais avec une valeur de seuil de confiance élevée, l'algorithme n'est pas en mesure de détecter toutes les interférences RF présentes. Par observation, un seuil de confiance de 0,4 ou de 0,5 offre le meilleur compromis entre la valeur de rappel et la valeur de la précision.

L'utilisation de petites valeurs IoU améliore également les performances de notre approche.

Tableau 4.2 – Métriques d'évaluation de YOLOv3 avec IoU = 0,25, 0,5 et 0,7

SC	AP <sub>25</sub>	Rappel <sub>25</sub>	Précision <sub>25</sub>	AP <sub>50</sub>	Rappel <sub>50</sub>	Précision <sub>50</sub>	AP <sub>70</sub>	Rappel <sub>70</sub>	Précision <sub>70</sub>
0,2	0,89	0,98	0,49	0,81	0,96	0,36	0,66	0,89	0,3
0,3		0,92	0,66		0,87	0,56		0,73	0,41
0,4		0,8	0,82		0,74	0,80		0,65	0,63
0,5		0,64	0,97		0,67	0,92		0,52	0,78
0,6		0,5	1		0,48	0,95		0,39	0,86

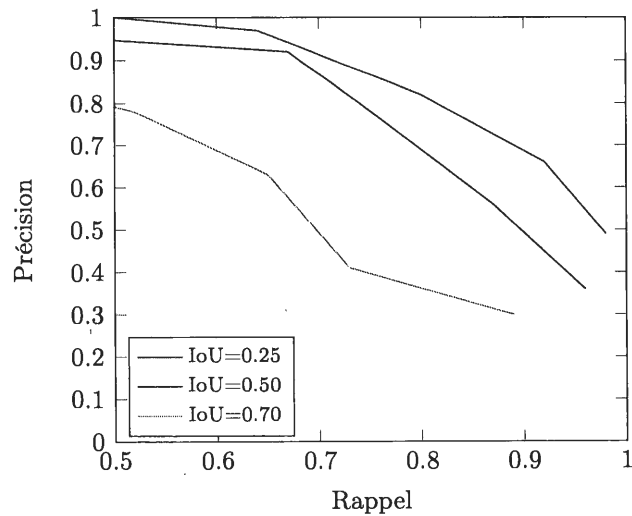


Figure 4.6 – Précision en fonction du rappel.

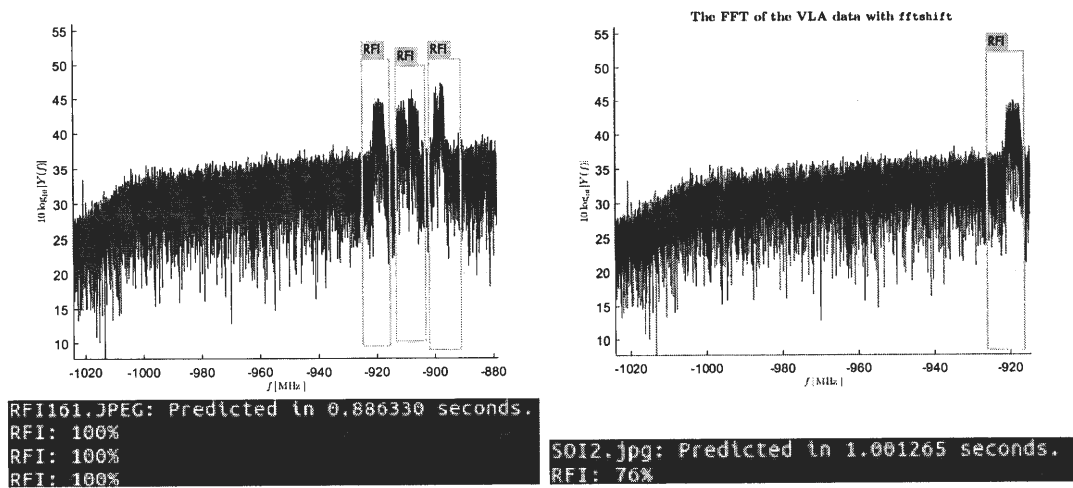


Figure 4.7 – Résultats de détection d'interférence.

## CONCLUSION

Dans ce travail, une méthode de détection des interférences RF pour les systèmes de communication sans fil en utilisant l'apprentissage profond a été présentée. Dans le premier chapitre de ce document, nous avons présenté une mise en contexte en explicitant les motivations de ce projet ainsi que la problématique que nous avons abordée dans ce projet, les objectifs projetés et la méthodologie suivie. Nous avons énuméré à la fin de ce chapitre les contributions réalisées.

Ensuite, nous avons fourni dans le deuxième chapitre de ce mémoire un survol sur les principaux travaux dans le domaine de la détection d'anomalies en général et la détection des interférences RF en particulier. Dans un premier temps, nous avons présenté les approches de détection d'anomalies en général. Ensuite, nous avons passé à la présentation des approches traditionnelles de détection des interférences RF en les catégorisant en six catégories selon la manière utilisée pour représenter le signal. Nous avons cité les algorithmes les plus répandus de chacune de ces catégories ainsi que leurs principaux avantages et inconvénients. Par la suite, nous avons décrit les approches de détection intelligentes en mettant l'accent sur leurs limitations.

Le troisième chapitre de ce document a présenté une introduction des concepts généraux de l'apprentissage profond tout en détaillant l'architecture la plus populaire en matière d'apprentissage profond en utilisant les réseaux de neurones convolutifs. Par la suite, nous avons présenté les algorithmes de détection des objets en montrant leur efficacité dans plusieurs domaines d'applications. Cette présentation nous a motivé à les appliquer dans le contexte de notre problème.



Le dernier chapitre a décrit notre contribution principale. Nous avons commencé par justifier notre choix de l'algorithme de détection YOLOv3 en décrivant ses avantages et en les comparant avec les autres algorithmes de détection d'objets. Ensuite, nous avons présenté le processus de détection des interférences avec toutes les étapes suivies. À la fin, l'évaluation des performances de l'approche proposée a été faite en utilisant les indicateurs de performance des algorithmes de détection des objets. Nous avons montré que l'algorithme YOLOv3 est efficace en terme de précision, temps et complexité. Ce mémoire est une première étape de l'ensemble du processus de détection et mitigation des interférences RF. Dans le cadre de projet AVIO-601, des autres travaux de recherche sont au cours pour la caractérisation des interférences, identification des interférences, géolocalisation des interférences et mitigation des interférences.

À long terme, nous visons d'abord améliorer notre solution :

- en ajoutant le processus d'élimination des interférences une fois les interférences détectées ;
- en regroupant une base de données plus large venant de plusieurs sources d'interférences ; et
- en utilisant de l'apprentissage non supervisé.

## RÉFÉRENCES

- (2019). Iou. <https://www.pyimagesearch.com/2016/11/07/intersection-over-union-iou-for-object-detection/>.
- Abdallah, A., Maarof, M. A. et Zainal, A. (2016). Fraud detection system : A survey. *Journal of Network and Computer Applications*, 68, 90 – 113. <http://dx.doi.org/https://doi.org/10.1016/j.jnca.2016.04.007>. Récupéré de <http://www.sciencedirect.com/science/article/pii/S1084804516300571>
- Akeret, J., Chang, C., Lucchi, A. et Refregier, A. (2017). Radio frequency interference mitigation using deep convolutional neural networks. *Astronomy and computing*, 18, 35–39.
- Anscombe, F. J. (1960). Rejection of outliers. *Technometrics*, 2(2), 123–146. <http://dx.doi.org/10.1080/00401706.1960.10489888>. Récupéré de <https://amstat.tandfonline.com/doi/abs/10.1080/00401706.1960.10489888>
- AVIO-601 (2018). AVIO-601 project : Interference mitigation in satellite communications. <https://lassena.etsmtl.ca/IMG/pdf/-6.pdf>.
- Bengio, Y. (2012). Deep learning of representations for unsupervised and transfer learning. Dans I. Guyon, G. Dror, V. Lemaire, G. Taylor, et D. Silver (dir.). *Proceedings of ICML Workshop on Unsupervised and Transfer Learning*, volume 27 de *Proceedings of Machine Learning Research*, 17–36., Bellevue, Washington, USA. PMLR. Récupéré de <http://proceedings.mlr.press/v27/bengio12a.html>
- Borio, D., Camoriano, L., Savasta, S. et Presti, L. L. (2008). Time-frequency excision for gnss applications. *IEEE Systems Journal*, 2(1), 27–37. <http://dx.doi.org/10.1109/JSYST.2007.914914>
- Borio, D., Dovis, F., Kuusniemi, H. et Presti, L. L. (2016). Impact and detection of gnss jammers on consumer grade satellite navigation receivers. *Proceedings of the IEEE*, 104(6), 1233–1245. <http://dx.doi.org/10.1109/JPROC.2016.2543266>

- Chalapathy, R. et Chawla, S. (2019). Deep learning for anomaly detection : A survey. *CoRR, abs/1901.03407*. Récupéré de <http://arxiv.org/abs/1901.03407>
- Chandola, V., Banerjee, A. et Kumar, V. (2009). Anomaly detection : A survey. *ACM Comput. Surv.*, 41(3), 15 :1–15 :58. <http://dx.doi.org/10.1145/1541880.1541882>. Récupéré de <http://doi.acm.org/10.1145/1541880.1541882>
- Chen, G., Zhao, Z., Zhu, G., Huang, Y. et Li, T. (2010). Hf radio-frequency interference mitigation. *IEEE Geoscience and Remote Sensing Letters*, 7(3), 479–482. <http://dx.doi.org/10.1109/LGRS.2009.2039340>
- Czech, D., Mishra, A. et Inggs, M. (2018). A cnn and lstm-based approach to classifying transient radio frequency interference. *Astronomy and computing*, 25, 52–57.
- Dai, J., Li, Y., He, K. et Sun, J. (2016). R-FCN : object detection via region-based fully convolutional networks. *CoRR, abs/1605.06409*. Récupéré de <http://arxiv.org/abs/1605.06409>
- De Stefano, C., Sansone, C. et Vento, M. (2000). To reject or not to reject : that is the question-an answer in case of neural classifiers. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 30(1), 84–94. <http://dx.doi.org/10.1109/5326.827457>
- Deng, J., Dong, W., Socher, R., jia Li, L., Li, K. et Fei-fei, L. (2009). Imagenet : A large-scale hierarchical image database. Dans *In CVPR*.
- Dit-Yan Yeung et Chow, C. (2002). Parzen-window network intrusion detectors. Dans *Object recognition supported by user interaction for service robots*, volume 4, 385–388 vol.4. <http://dx.doi.org/10.1109/ICPR.2002.1047476>
- Dovis, F. et Musumeci, L. (2011). Use of wavelet transforms for interference mitigation. Dans *2011 International Conference on Localization and GNSS (ICL-GNSS)*, 116–121. <http://dx.doi.org/10.1109/ICL-GNSS.2011.5955275>
- Dovis, F. et Musumeci, L. (2016). Use of the karhunen–loève transform for interference detection and mitigation in gnss. *ICT Express*, 2(1), 33–36.
- Frizzi, S., Kaabi, R., Bouchouicha, M., Ginoux, J.-M., Fnaiech, F. et Moreau, E. (2017). Détection de la fumée et du feu par réseau de neurones convolutifs.

Dans *Conférence Nationale sur les Applications Pratiques de l'Intelligence Artificielle*, Caen, France. Récupéré de <https://hal.archives-ouvertes.fr/hal-01561518>

García-Teodoro, P., Díaz-Verdejo, J., Maciá-Fernández, G. et Vázquez, E. (2009). Anomaly-based network intrusion detection : Techniques, systems and challenges. *Computers Security*, 28(1), 18 – 28.  
<http://dx.doi.org/https://doi.org/10.1016/j.cose.2008.08.003>.  
 Récupéré de <http://www.sciencedirect.com/science/article/pii/S0167404808000692>

Getu, T. M., Ajib, W. et Yeste-Ojeda, O. A. (2017). Tensor-based efficient multi-interferer rfi excision algorithms for simo systems. *IEEE Transactions on Communications*, 65(7), 3037–3052.  
<http://dx.doi.org/10.1109/TCOMM.2017.2694006>

Girshick, R. B. (2015). Fast R-CNN. *CoRR*, *abs/1504.08083*. Récupéré de <http://arxiv.org/abs/1504.08083>

Girshick, R. B., Donahue, J., Darrell, T. et Malik, J. (2013). Rich feature hierarchies for accurate object detection and semantic segmentation. *CoRR*, *abs/1311.2524*. Récupéré de <http://arxiv.org/abs/1311.2524>

Goodfellow, I., Bengio, Y. et Courville, A. (2016). *Deep Learning*. MIT Press.  
<http://www.deeplearningbook.org>.

Grunau, S., Block, D. et Meier, U. (2018). Multi-label wireless interference classification with convolutional neural networks. Dans *2018 IEEE 16th International Conference on Industrial Informatics (INDIN)*, 187–192.  
<http://dx.doi.org/10.1109/INDIN.2018.8471956>

Guner, B., Johnson, J. T. et Niamsuwan, N. (2007). Time and frequency blanking for radio-frequency interference mitigation in microwave radiometry. *IEEE Transactions on Geoscience and Remote Sensing*, 45(11), 3672–3679.  
<http://dx.doi.org/10.1109/TGRS.2007.903680>

Hannun, A. Y., Case, C., Casper, J., Catanzaro, B., Diamos, G., Elsen, E., Prenger, R., Satheesh, S., Sengupta, S., Coates, A. et Ng, A. Y. (2014). Deep speech : Scaling up end-to-end speech recognition. *CoRR*, *abs/1412.5567*.  
 Récupéré de <http://arxiv.org/abs/1412.5567>

Hawkins, S., He, H., Williams, G. et Baxter, R. (2002). Outlier detection using replicator neural networks. Dans Y. Kambayashi, W. Winiwarter, et M. Arikawa (dir.). *Data Warehousing and Knowledge Discovery*, 170–180., Berlin, Heidelberg. Springer Berlin Heidelberg.

He, K., Zhang, X., Ren, S. et Sun, J. (2015). Deep residual learning for image recognition. *CoRR*, *abs/1512.03385*. Récupéré de <http://arxiv.org/abs/1512.03385>

Hochenbaum, J., Vallis, O. S. et Kejariwal, A. (2017). Automatic anomaly detection in the cloud via statistical learning. *CoRR*, *abs/1704.07706*. Récupéré de <http://arxiv.org/abs/1704.07706>

Jeffs, B. D., Li, L. et Warnick, K. F. (2005). Auxiliary antenna-assisted interference mitigation for radio astronomy arrays. *IEEE Transactions on Signal Processing*, *53*(2), 439–451. <http://dx.doi.org/10.1109/TSP.2004.840787>

Jiang, H. et Learned-Miller, E. (2017). Face detection with the faster r-cnn. Dans *2017 12th IEEE International Conference on Automatic Face Gesture Recognition (FG 2017)*, 650–657. <http://dx.doi.org/10.1109/FG.2017.82>

Johnson, J. T. et Guner, B. (2007). Cross frequency blanking for rfi mitigation : A c-band case study. Dans *2007 IEEE International Geoscience and Remote Sensing Symposium*, 2710–2713. <http://dx.doi.org/10.1109/IGARSS.2007.4423402>

Karpathy., A. (Sep. 2013). Convolutional neural networks for visual recognition. <http://cs231n.github.io/convolutional-networks/#pool>.

Keogh, E., Lin, J. et Fu, A. (2005). Hot sax : efficiently finding the most unusual time series subsequence. Dans *Fifth IEEE International Conference on Data Mining (ICDM'05)*, 8 pp.–. <http://dx.doi.org/10.1109/ICDM.2005.79>

Keogh, E., Lin, J., Fu, A. W. et VanHerle, H. (2006). Finding unusual medical time-series subsequences : Algorithms and applications. *IEEE Transactions on Information Technology in Biomedicine*, *10*(3), 429–439. <http://dx.doi.org/10.1109/TITB.2005.863870>

Kind, A., Stoecklin, M. P. et Dimitropoulos, X. (2009). Histogram-based traffic anomaly detection. *IEEE Transactions on Network and Service Management*, *6*(2), 110–121. <http://dx.doi.org/10.1109/TNSM.2009.090604>

Krizhevsky, A., Sutskever, I. et Hinton, G. E. (2012). Imagenet classification with deep convolutional neural networks. In F. Pereira, C. J. C. Burges, L. Bottou, et K. Q. Weinberger (dir.), *Advances in Neural Information Processing Systems 25* 1097–1105. Curran Associates, Inc.

- Kun-Lun Li, Hou-Kuan Huang, Sheng-Feng Tian et Wei Xu (2003). Improving one-class svm for anomaly detection. Dans *Proceedings of the 2003 International Conference on Machine Learning and Cybernetics (IEEE Cat. No.03EX693)*, volume 5, 3077–3081 Vol.5.  
<http://dx.doi.org/10.1109/ICMLC.2003.1260106>
- Laxhammar, R., Falkman, G. et Sviestins, E. (2009). Anomaly detection in sea traffic - a comparison of the gaussian mixture model and the kernel density estimator. Dans *2009 12th International Conference on Information Fusion*, 756–763.
- LeCun, Y., Boser, B., Denker, J. S., Henderson, D., Howard, R. E., Hubbard, W. et Jackel, L. D. (1989). Backpropagation applied to handwritten zip code recognition. *Neural Computation*, 1(4), 541–551.  
<http://dx.doi.org/10.1162/neco.1989.1.4.541>
- LeCun, Y., Bottou, L., Bengio, Y., Haffner, P. *et al.* (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, 86(11), 2278–2324.
- Lin, J., Keogh, E., Ada Fu et Van Herle, H. (2005). Approximations to magic : finding unusual medical time series. Dans *18th IEEE Symposium on Computer-Based Medical Systems (CBMS'05)*, 329–334.  
<http://dx.doi.org/10.1109/CBMS.2005.34>
- Lin, T., Goyal, P., Girshick, R. B., He, K. et Dollár, P. (2017a). Focal loss for dense object detection. *CoRR*, *abs/1708.02002*. Récupéré de <http://arxiv.org/abs/1708.02002>
- Lin, T.-Y., Dollár, P., Girshick, R., He, K., Hariharan, B. et Belongie, S. (2017b). Feature pyramid networks for object detection. Dans *The IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*.
- Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., van der Laak, J. A., van Ginneken, B. et Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, 42, 60 – 88. <http://dx.doi.org/https://doi.org/10.1016/j.media.2017.07.005>. Récupéré de <http://www.sciencedirect.com/science/article/pii/S1361841517301135>
- Liu, L., Ouyang, W., Wang, X., Fieguth, P. W., Chen, J., Liu, X. et Pietikäinen, M. (2018). Deep learning for generic object detection : A survey. *CoRR*, *abs/1809.02165*.

Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S. E., Fu, C. et Berg, A. C. (2015). SSD : single shot multibox detector. *CoRR*, *abs/1512.02325*. Récupéré de <http://arxiv.org/abs/1512.02325>

M.A., F. E. (1887). Xli. on discordant observations. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, *23*(143), 364–375. <http://dx.doi.org/10.1080/14786448708628471>. Récupéré de <https://doi.org/10.1080/14786448708628471>

Malhotra, P., Ramakrishnan, A., Anand, G., Vig, L., Agarwal, P. et Shroff, G. (2016). Lstm-based encoder-decoder for multi-sensor anomaly detection. *CoRR*, *abs/1607.00148*. Récupéré de <http://arxiv.org/abs/1607.00148>

Markou, M. et Singh, S. (2003). Novelty detection : a review—part 1 : statistical approaches. *Signal Processing*, *83*(12), 2481 – 2497. <http://dx.doi.org/https://doi.org/10.1016/j.sigpro.2003.07.018>. Récupéré de <http://www.sciencedirect.com/science/article/pii/S0165168403002020>

McCulloch, W. S. et Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics*, *5*(4), 115–133.

Misra, S., Mohammed, P. N., Guner, B., Ruf, C. S., Piepmeier, J. R. et Johnson, J. T. (2009). Microwave radiometer radio-frequency interference detection algorithms : A comparative study. *IEEE Transactions on Geoscience and Remote Sensing*, *47*(11), 3742–3754. <http://dx.doi.org/10.1109/TGRS.2009.2031104>

Mosiane, O., Oozeer, N. et Bassett, B. A. (2016). Radio frequency interference detection using machine learning. Dans *2016 IEEE Radio and Antenna Days of the Indian Ocean (RADIO)*, 1–2. <http://dx.doi.org/10.1109/RADIO.2016.7772036>

Musumeci, L. et Dosis, F. (2012). A comparison of transformed-domain techniques for pulsed interference removal on gnss signals. Dans *2012 International Conference on Localization and GNSS*, 1–6. <http://dx.doi.org/10.1109/ICL-GNSS.2012.6253131>

Newtec et IRG. (Sep. 2013). 93 <https://www.newtec.eu/article/release/93-of-the-industry-suffers-from-satellite-interference>.

Nguyen, V. D., Van Nguyen, H., Tran, D. T., Lee, S. J. et Jeon, J. W. (2017). Learning framework for robust obstacle detection, recognition, and tracking. *IEEE Transactions on Intelligent Transportation Systems*, *18*(6), 1633–1646.

<http://dx.doi.org/10.1109/TITS.2016.2614818>

Niamsuwan, N., Johnson, J. T. et Ellingson, S. W. (2005). Examination of a simple pulse-blanking technique for radio frequency interference mitigation. *Radio Science*, 40(05), 1–11. <http://dx.doi.org/10.1029/2004RS003155>

NRAO (2019). Very large array of the national radio astronomy observatory. <http://www.vla.nrao.edu/>.

Pevný, T. (2016). Loda : Lightweight on-line detector of anomalies. *Machine Learning*, 102(2), 275–304.

<http://dx.doi.org/10.1007/s10994-015-5521-0>. Récupéré de <https://doi.org/10.1007/s10994-015-5521-0>

Portnoy, L., Eskin, E. et Stolfo, S. (2001). Intrusion detection with unlabeled data using clustering. Dans *In Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001)*, 5–8.

Ranjan, R., Patel, V. M. et Chellappa, R. (2019). Hyperface : A deep multi-task learning framework for face detection, landmark localization, pose estimation, and gender recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41(1), 121–135.

<http://dx.doi.org/10.1109/TPAMI.2017.2781233>

Ratsch, G., Mika, S., Scholkopf, B. et Muller, K. . (2002). Constructing boosting algorithms from svms : an application to one-class classification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 24(9), 1184–1199. <http://dx.doi.org/10.1109/TPAMI.2002.1033211>

Rebbapragada, U., Protopapas, P., Brodley, C. E. et Alcock, C. (2009). Finding anomalous periodic time series. *Machine Learning*, 74(3), 281–313. <http://dx.doi.org/10.1007/s10994-008-5093-3>. Récupéré de <https://doi.org/10.1007/s10994-008-5093-3>

Redmon, J., Divvala, S. K., Girshick, R. B. et Farhadi, A. (2015). You only look once : Unified, real-time object detection. *CoRR*, *abs/1506.02640*. Récupéré de <http://arxiv.org/abs/1506.02640>

Redmon, J. et Farhadi, A. (2016). YOLO9000 : better, faster, stronger. *CoRR*, *abs/1612.08242*. Récupéré de <http://arxiv.org/abs/1612.08242>

Redmon, J. et Farhadi, A. (2018). Yolov3 : An incremental improvement. *arXiv preprint arXiv :1804.02767*.

Ren, S., He, K., Girshick, R. B. et Sun, J. (2015). Faster R-CNN : towards real-time object detection with region proposal networks. *CoRR*,



*abs/1506.01497*. Récupéré de <http://arxiv.org/abs/1506.01497>

Ruf, C. S., Gross, S. M. et Misra, S. (2006). Rfi detection and mitigation for microwave radiometry with an agile digital detector. *IEEE Transactions on Geoscience and Remote Sensing*, 44(3), 694–706.  
<http://dx.doi.org/10.1109/TGRS.2005.861411>

Sabokrou, M., Fayyaz, M., Fathy, M. et Klette, R. (2017). Deep-cascade : Cascading 3d deep neural networks for fast anomaly detection and localization in crowded scenes. *IEEE Transactions on Image Processing*, 26(4), 1992–2004. <http://dx.doi.org/10.1109/TIP.2017.2670780>

Sainath, T. N., Weiss, R. J., Senior, A. W., Wilson, K. W. et Vinyals, O. (2015). Learning the speech front-end with raw waveform cldnns. Dans *INTERSPEECH*.

Schlegl, T., Seeböck, P., Waldstein, S. M., Schmidt-Erfurth, U. et Langs, G. (2017). Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. Dans M. Niethammer, M. Styner, S. Aylward, H. Zhu, I. Oguz, P.-T. Yap, et D. Shen (dir.). *Information Processing in Medical Imaging*, 146–157., Cham. Springer International Publishing.

Simonyan, K. et Zisserman, A. (2015). Very deep convolutional networks for large-scale image recognition. Dans *International Conference on Learning Representations*.

Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S. E., Anguelov, D., Erhan, D., Vanhoucke, V. et Rabinovich, A. (2014). Going deeper with convolutions. *CoRR*, *abs/1409.4842*. Récupéré de <http://arxiv.org/abs/1409.4842>

Tani, A. et Fantacci, R. (2008). Performance evaluation of a precorrelation interference detection algorithm for the gnss based on nonparametrical spectral estimation. *IEEE Systems Journal*, 2(1), 20–26.  
<http://dx.doi.org/10.1109/JSYST.2007.914772>

van der Tol, S. et van der Veen, A. . (2005). Performance analysis of spatial filtering of rf interference in radio astronomy. *IEEE Transactions on Signal Processing*, 53(3), 896–910. <http://dx.doi.org/10.1109/TSP.2004.842177>

Wang, S. (2010). A comprehensive survey of data mining-based accounting-fraud detection research. Dans *2010 International Conference on Intelligent Computation Technology and Automation*, volume 1, 50–53.  
<http://dx.doi.org/10.1109/ICICTA.2010.831>

Wenke Lee et Dong Xiang (2001). Information-theoretic measures for

anomaly detection. Dans *Proceedings 2001 IEEE Symposium on Security and Privacy. S P 2001*, 130–143.

<http://dx.doi.org/10.1109/SECPRI.2001.924294>

Wiesel, T. N. et Hubel, D. H. (1963). Single-cell responses in striate cortex of kittens deprived of vision in one eye. *Journal of Neurophysiology*, 26(6), 1003–1017. PMID : 14084161,

<http://dx.doi.org/10.1152/jn.1963.26.6.1003>. Récupéré de

<https://doi.org/10.1152/jn.1963.26.6.1003>

Zarpelão, B. B., Miani, R. S., Kawakani, C. T. et de Alvarenga, S. C. (2017). A survey of intrusion detection in internet of things. *Journal of Network and Computer Applications*, 84, 25 – 37.

<http://dx.doi.org/https://doi.org/10.1016/j.jnca.2017.02.009>.

Récupéré de <http://www.sciencedirect.com/science/article/pii/S1084804517300802>

Zenati, H., Foo, C. S., Lecouat, B., Manek, G. et Chandrasekhar, V. R.

(2018). Efficient gan-based anomaly detection. *CoRR*, *abs/1802.06222*.

Récupéré de <http://arxiv.org/abs/1802.06222>

Zhai, S., Cheng, Y., Lu, W. et Zhang, Z. (2016). Deep structured energy based models for anomaly detection. *CoRR*, *abs/1605.07717*. Récupéré de

<http://arxiv.org/abs/1605.07717>

Zhang, L., You, W., Wu, Q. M. J., Qi, S. et Ji, Y. (2018). Deep

learning-based automatic clutter/interference detection for hfswr. *Remote Sensing*, 10(10). <http://dx.doi.org/10.3390/rs10101517>. Récupéré de

<http://www.mdpi.com/2072-4292/10/10/1517>

Zhang, S., Benenson, R., Omran, M., Hosang, J. et Schiele, B. (2016). How far are we from solving pedestrian detection? Dans *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 1259–1267.

<http://dx.doi.org/10.1109/CVPR.2016.141>

Zhao, Z., Zheng, P., Xu, S. et Wu, X. (2019). Object detection with deep learning : A review. *IEEE Transactions on Neural Networks and Learning Systems*, 1–21. <http://dx.doi.org/10.1109/TNNLS.2018.2876865>

Zong, B., Song, Q., Min, M. R., Cheng, W., Lumezanu, C., Cho, D. et Chen, H. (2018). Deep autoencoding gaussian mixture model for unsupervised

anomaly detection. Dans *International Conference on Learning*

*Representations*. Récupéré de