People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Kasdi Merbah Ouargla University
Faculty of New Information and Communication Technologies
Communication
Department of Computing and Information Technology

ACADEMIC MASTER Thesis
Domain: Mathematics and Computer science
Specialty: Fundamental

Presented by:
Fatima Zohra Difani
Khadidja Merhabaoui

Theme :

Machine Learning Based Model For Fake News Spreaders Detection

Publicly discussed:

20/06/2022

Before the jury:

Professor.Ahmed KORICHI	MCB	President	UKM Ouargla
Miss Chahrazad TOUMI	MCB	Supervisor	UKM Ouargla
Mister Bachir MAHDJOUB	MCB	Examiner	UKMOuargla

Academic year: 2021-2022

Dedication

This thesis is dedicated to:

My great Mother, who never stop giving of herself in countless ways

My dearest family, who leads me through the valley of darkness with light of hope and support

My beloved friends who stand by me when things look bleak

My beloved students: all of them from the oldest to the youngest whom i consider as family members.

To all my big family, the symbol of love and giving,

All the people in my life who touch my heart, I dedicate this work.

khadidja MERHABAOUI

Dedication

Praise be to God

who has enabled us to complete this step in our academic journey with this thesis

the fruit of effort and success, by His grace, i dedicate :

To my mother, may God have mercy on her

to my father, may God protect him, and perpetuate him as a light to my path To my sisters (Hayat, Siham, Laila, Amina, Ahlam)

and my brothers (Abdul-Fattah, Muhammad, Abdul-Basit, Elias)

my step mother and all the members of my honorable family

may God protect them.

And to my friends and those who have helped me in my journey, even with their prayers.

Fatima Zohra DIFANI

Acknowledgments

In the name of Allah, the Most Gracious and the Most Merciful. All praises to Allah and His blessing for the completion of this thesis.

Our humblest gratitude to the holy Prophet Muhammad (Peace be upon him) whose way of life has been a continuous guidance for us.

We thank God for all the opportunities, trials and strength that have been showered on us to finish writing the thesis. We experienced so much during this process, not only from the academic aspect but also from a personal one.
First and foremost, we would like to sincerely thank our supervisor Prof. Dr. Chahrazad TOUMI for her guidance, understanding, and patience and most importantly she provided positive encouragement to finish this thesis. It has been a great pleasure and honor to have her as our supervisors and teacher.
We wish to acknowledge the support and great love of our parents, brothers and sisters, friends and classmates for their motivation, prayers and their sincere help during our studies, They kept us going on, And this work would not have been possible without their support.
We also wish to thank all the people whose assistance was a milestone in the completion of this project wherever they are.

May god bless everybody.

Abstract

Technological developments and social media, have come with so many benefits and facilities in the last two decades. However, it have also gave a big opportunity for some negative phenomenons to grow such as the false information and more specifically fake news which became a real threat for individuals and communities.

Indeed, the spread of fake news has negatively affected the user's of social media. Consequentially, it has become imperative to combat the spread of fake news and reduce reliance on fake information from these sources.

Recent advances in deep learning techniques in complex natural language processing tasks also make it a promising solution for detecting fake news and fake news spreaders. In this work, we propose a machine learning model for fake news spreaders detection on Twitter. We used a machine learning based model using the Support Vector Machine (SVM) and the Random Forest (RF) algorithms. We obtained an average accuracy of 72%.

Keywords

False Information, Fake News, PAN 2020, Support Vector Machine (SVM) , Random Forest (RF)

Résumé

Les développements technologiques et les médias sociaux ont apporté de nombreux avantages au cours des deux dernières décennies. Cependant, cela a également donné une grande opportunité à certains phénomènes néfastes de se développer tels que les fausses informations et plus particulièrement les fausses nouvelles qui sont devenues une véritable menace pour les individus et les communautés. En effet, la diffusion de fausses nouvelles a affecté négativement les utilisateurs des réseaux sociaux. Par conséquent, il est devenu impératif de lutter contre la diffusion de fausses nouvelles et de réduire la dépendance à l'égard des fausses informations provenant de ces sources. Les progrès récents des techniques d'apprentissage en profondeur dans les tâches complexes de traitement du langage naturel en font également une solution prometteuse pour détecter les fausses nouvelles et les diffuseurs de fausses nouvelles. Dans ce travail, nous proposons un modèle d'apprentissage automatique pour la détection des diffuseurs de fausses nouvelles sur Twitter. Nous avons utilisé un modèle basé sur l'apprentissage automatique utilisant les algorithmes Support Vector Machine (SVM) et Random Forest (RF) et nous avons obtenu une précision moyenne de 72%

Mots clés

Fausses Informations, Fake News, PAN 2020, Support Vector Machine (SVM), Random Forest (RF)

الملخص

لقَد أتت التطورات التكنولوجية ووسائل التواصل الاجتماعي بالعديد من الفوائد و المرافق في العقَدين الماضيين. ومع ذلك ، فقَد أعطت أيضًا فرصة كبيرة للبعض الظواهر السيئة بالظهور مثل نشر المعلومات الخاطئة والأخبار المزيفة بشكل أكثر تحديدًا التي أصبحت تهديدًا حقيقيًا للأفراد والمجتمعات. في الواقع ، انتشار الاخبار المزيفة أثرت سلبًا على مستخدمي وسائل التواصل الاجتماعي. نتيجة لذلك ، فقَد أصبح من الضرورة مكافحة انتشار الأخبار المزيفة وتقَليل الاعتماد عليها خاصة من هذه المصادر الالكترونية. التطورات الحديثة في تقَنيات التعلم العميق تجعل من معالجة هذه المشاكل مثل اكتشاف الأخبار المزيفة وناشريها حلاً واعدًا. في هذا العمل ، نقَترح نموذجًا مبني على اليات التعلم الآلي لاكتشاف ناشري الأخبار المزيفة على منصة تويتر. استخدمنا نموذجًا قائمًا على التعلم الآلي باستخدام خوارزميتي Support Vector Machine و Random Forest . فكانت نسبة متوسط الدقة المتحصل عليه هو72٪.

الكلمات المفتاحية

معلومات كاذبة ، أخبار مزيفة ، Support Vector Machine ، PAN 2020 ، Random Forest

Table of Contents

List of Figures

List of Tables

General Introduction

Since the rise of the internet, it had brought enormous changes to our live digital platforms, including social media systems and messaging applications such as Facebook, Twitter, Instagram... etc , 4.20 billion active social media users to January 2021, representing about 54% of the global population [46]. These platforms have significantly changed the way users interact and communicate with one another. Also, they have opened up a whole new waves of applications and changes to the information ecosystems. Besides communicating with people from all around the world, social media plays an important role in the lives of many people, some far more than others. Some people make a living from social media, whether by promoting business or entertainment [40].

However, these platforms allow the dissemination and the consumption of a huge number of news, and some of this content is hardly filtered or controlled. Also, that lead to opening unforeseen opportunities for creating and spreading false information, in general, and fake news precisely. Fake news is a fabricated information that mimics news media content in form but not in organizational process or intent [48] Fake news have created many big problems in different domains example the fake news campaigns that were against some COVID19 vaccines [41]. Part of the reason for the increase of this phenomenon is the nature of these digital media Platforms: (i) producing and consuming news is generally more modern and less costly ,most of the times free, compared to traditional news media such as newspapers or TV; (ii) easier to share, comment and discuss news with friends or other readers in digital platforms.

The questions asked are how can the fake news spreading on social media can be solved? Are there modern ways to detect fake news and their authenticity? or at least minimized? How can the fake news be detected? How can fake news spreaders be detected?

So many previous works have tried to solve the fake news problem, some by detecting the fake news from the true news, some by detecting the fake news spreaders from non

spreaders using different approaches such as machine learning and deep learning [51, 49, 42, 35]. Automatic detection techniques using artificial intelligence and machine learning have been investigated. Recent advances in deep learning techniques in complex natural language processing tasks also make it a promising solution for detecting fake news. This work has the objective to solve the fake news spreaders problem and proposes a machine learning based model using Support Vector Machine (SVM) and Random Forest (RF) algorithms for detecting the fake news spreader in Twitter with a good accuracy.

Our thesis is structured as follows: it starts with a general introduction followed by three chapters. The first chapter is about the background of false information,their history, their categories and their components and fake news, provided with some examples, their types and their spreaders and the dangers of fake news and methods detecting them. The second chapter is about artificial intelligence, its history and its sub-fields , we also talked about machine learning applications and types and at the end we explained some of the machine learning algorithms. Finally the third chapter is about the conception of our model, implementation tools used and the obtained results. We end our thesis with a general conclusion and the references we used to write it.

Chapter 1

False Information and Fake News

Introduction

The spread of true information or false or misleading – whether by word-of-mouth, media, or otherwise – is an age-old phenomenon. Yet advances in technology day after day. The changes in how people interact with information are propelling the spread of false information at a speed and scale that is not seen before. This has resulted in information ecosystems that are dangerously affected by information disorder, including mis/disinformation.

In this chapter, first we will present false information; its history; its categories and its components, then we will talk about fake news, their types, we will give some examples of them and we will talk about their spreaders as they are the main topic of our work, at the end of the chapter we will focus more on the fight against fake news, the dangers they bring and some methods of detecting them.

1.1 False Information

Let's first try to clarify the meaning of false information:

1.1.1 Definition

False information means any written or verbal statement or representation of fact that is not true and that was made intentionally, knowingly or without having taken reasonable steps to ascertain whether or not the information was true.[11]

So it is misleading information that is communicated with innocent intention or with the aim of harming people. These are attempts at misinformation. Indeed, they can be used to tarnish the reputation of someone, a political party, a company for example.

The Internet allows a massive and mostly very rapid dissemination of fake news using the social networks, where they are more and more present. People are taken by catchy headlines and fabricated information, which helps their creators increase views and shares of their content.

1.1.2 The history of false information

There are many examples of fake news throughout history:

- It was used by Nazi propaganda to create anti-Semitic fervor. [24]
- It was instrumental in catalyzing the Enlightenment, when the Catholic Church's false explanation of the 1755 Lisbon earthquake prompted Voltaire to denounce religious domination. [17]
- the United States, in the 1800s, a publication of false stories about the alleged shortcomings and crimes of African Americans took place because of a racist sentiment.[12]
- Yellow journalism, 1890s: was a style of newspaper reporting that emphasized sensationalism and exaggeration over facts. During its heyday in the late 19th century it was one of many factors that helped push the United States and Spain into war in Cuba and the Philippines, leading to the acquisition of overseas territory by the United States. [27] [50]

1.1.3 False information Categories

False Information can be divided into three important categories: Misinformation, Disinformation and Mal-information.

Misinformation

Misinformation is information that is false, but the person who is disseminating it believes that it is true.[15]
However, misinformation and its effects are not new, but have become increasingly powerful as they are fueled by new technologies and rapid online dissemination. The consequence is that digital misinformation, in contexts of polarization, risks eclipsing quality journalism, and the truth.
Indeed, the fight against misinformation, at this stage, is more about advocacy and education than litigation. However, this is expected to change as digital rights litigation lawyers engage in more strategic litigation and test cases aimed at mitigating misinformation while protecting and promoting free speech [53].

Disinformation

Disinformation is information that is false, and disseminated on purpose. "It is a deliberate, intentional lie, and points to people being actively disinformed by malicious

actors".[15]

It is also information deliberately and often covertly spread (as by the planting of rumors) in order to influence public opinion or obscure the truth [8]

Malinformation

Malinformation is the Information that may be true but is spread with malicious intent or taken out of context. Examples include divulging private information or manipulating facts to fit a false narrative. Vladimir Volkoff defines it as follows in his Short History of Disinformation: "Disinformation is a manipulation of public opinion, for political purposes, with information processed by devious means. [39]

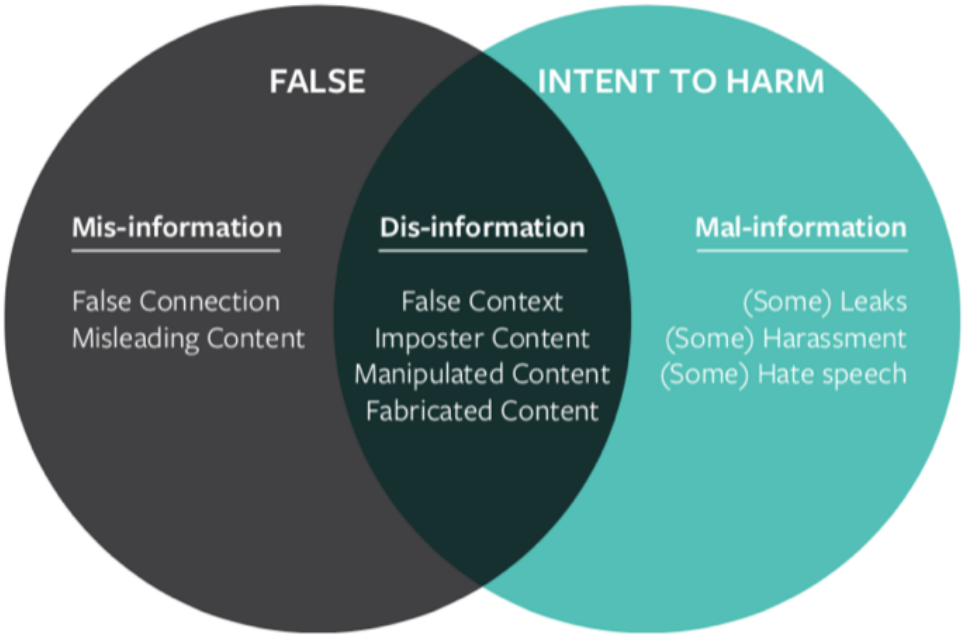

Figure 1.1: categories of false information.

[60]

1.1.4 The components of fake information

The term fake information is based on four main components: creator/spreader, target or victim, news content and social context.

Creator/Spreader

Creators of online misinformation is the one who creates the the false information, the spreader is the one who disseminates the false information, these two actors may or may not be human beings. (we talk more about the spreaders in the coming headlines)

Targeted victims

The victims can be any social media or other modern platforms and websites user. There may be several groups in society that can be targets such as students, voters, parents, senior citizens...etc.

News content

by news content, we mean the heart of the news. That is, it contains both physical content (such as title, body text, and multimedia) and intangible content (such as purpose, sentiment, and themes).

Social context

the social context indicates how news is distributed on the Internet. Social context analysis includes user, network analysis (how online users engage with news) and broadcast pattern analysis.

1.2 Fake News

1.2.1 Fake news definition

So many researchers have studied the Fake news phenomenon and came up with so many definitions, we mention from them:

Definition 1

We define “fake news” to be fabricated information that mimics news media content in form but not in organizational process or intent. Fake-news outlets, in turn, lack the news media’s editorial norms and processes for ensuring the accuracy and credibility of information. Fake news has primarily drawn recent attention in a political context but

it also has been documented in topics such as vaccination, nutrition, and stock values. It is particularly pernicious in that it is parasitic on standard news outlets, simultaneously benefiting from and undermining their credibility. [48].

Definition 2

Generally news is supposedly—and normatively—based on truth, which makes the term "fake news" an oxymoron. The word "fake" is often used interchangeably with words such as copy, forgery, counterfeit, and inauthentic.
The Oxford Dictionary defines "fake" as an adjective which means "not genuine; imitation or counterfeit." . A study about fake online reviews also specified the role of intention in defining what is fake. The study defined fake reviews "as deceptive reviews provided with an intention to mislead consumers in their purchase decision making, often by reviewers with little or no actual experience with the products or services being reviewed" [34].
Fake news is based primarily on a very catchy headline that produces the effect of a bomb. A scoop that mainstream media do not have, and that readers supposedly will discover exclusively. A call for clicks that is hard to resist. The contents of these messages are completely untrue or misguided, with lies often covered with a layer of truth (the black sheep with the white markings). Once created, fake news is boosted by social networks and circulates at very high speed. Manipulators take advantage of our limited attention span and our tendency to believe that everything that is read on the Internet is true, to introduce fake news. Moreover, the creators of fake news are great seducers of algorithms. They know what keywords to use and how to place them, insert content like videos and photos that will please the algorithms and propel their fake news to the forefront of the web. [36] False information actors and types have different motives behind them. We mention some of them: Malicious Intent, Influence (1. aiming to get leverage or followers (power) 2. changing the norms of the public by disseminating false information), Profit and Passion[61].

1.2.2 The different types of fake news

Fake news is largely used to manipulate the public for so many different reasons. Here are the four most common types of fake news [61]:

- Targeted disinformation

This is information that is invented and distributed for selfish purposes. More often, this fake news targets groups that are particularly sensitive to this type of information, classifying polarizing content as credible without verification and sharing it on social media.

- Misleading Headlines

  Headlines, which present fabricated facts to grab attention. Often, when reading the article, it turns out that the title is deliberately misleading and does not correspond to the content of the text. These titles are also called “clickbait titles”.

- Viral publications

  on social media, an infinity of new publications appear every second. Hence, users do not take the time to verify the authenticity of each one. As the major platforms are oriented towards shares, likes and followers, the most popular posts are more often distributed, even if they are fake.

- Satire

  It refers to mock news programs, which typically use humor or exaggeration to present news updates. An example: The Daily Show on Comedy Central in the United States by Trevor Noah. These programs are focused on current situations and often use the style of a television news broadcast (a “talking head” behind a desk, with illustrative graphics and video), much as a regular news program. Nonetheless, a key difference is that they promote themselves as delivering entertainment first and foremost rather than information, with hosts calling themselves comedians.

- Parody

  It shares many characteristics with satire as both rely on humor as a means of drawing an audience. It also uses a presentation format which mimics mainstream news media.

  But the difference is their use of non-factual information to inject humor. Parody plays on the ludicrousness of issues and highlights them by making up entirely fictitious news stories,instead of providing direct commentary on current situations through humor One of the most common examples is the parody website The Onion..

- News Fabrication

This refers to articles which have no factual basis but are published in the style of news articles to create legitimacy. Unlike parody, there is no implicit understanding between the author and the reader that the item is false. Indeed, the intention is often quite the opposite. The producer of the item often has the intention of misinforming.

Fabricated items can be published on a website, blog or on social media platforms. The difficulty in distinguishing fabricated fake news occurs when partisan organizations publish these stories, providing some semblance of objectivity and balanced reporting.

- Photo Manipulation

  Fake news has also been used to refer to the manipulation of real images or videos to create a false narrative. Where the previous categories generally referred to text-based items, this category describes visual news. Manipulation of images has become an increasingly common occurrence with the advent of digital photos, powerful image manipulation software, and knowledge of techniques. Effects may range from simple to complex. Simple adjustments can include increasing color saturation and removing minor elements. More-invasive changes can include removing or inserting a person into an image.

- Propaganda

  Propaganda refers to news stories which are created by a political entity to influence public perceptions. The overt purpose is to benefit a public figure, organization or government.

1.2.3 Examples of fake news

While some fake news is relatively harmless, others can cause great harm by pitting people against each other, or encouraging undemocratic thinking. Experts suspect that fake news, combined with social bots, has had a significant impact on crucial world events such as the Brexit vote in 2016 or the US presidential election in 2017, especially in recent years. Here are three examples of "successful" fake news, which have gone around the world and influenced the public:

- COVID-19 misinformation: It includes misconceptions about the disease, wishful thinking about the wrong treatments, and fantasies about how the virus spreads.

Some of this is purely speculation from well-meaning people who then publish their opinions as fact[41].

- On August 21, 1835, the New York Sun published a series of articles about the discovery of life on the moon. These were erroneously, falsely attributed to the famous astronomer of the time, Sir John Herschel. [1]
- Social media sites are currently circulating a photo of a crying young woman who, in various languages, claims that the president's 17-year-old daughter Oleksandra Zelenska "hates her father" and calls him a "Nazi" and "Ukrainians Killer". The Russian website also shared the claim. When the photo is actually from a video that appeared online in 2017.[10]

1.2.4 Fake news spreaders

When dealing with fake news spreading online, we individuate more than a category, human/non-human, publisher/spreader:

1. First we explain the human or non-human category:
    - Human: fake news can be spread by humans such as journalists, who seek to disrupt the credibility of the online social community.
    - Non-human: Social robots or Cyborgs are the most common non-human creators of fake news. These are computer programs designed to display behaviors similar to humans, and to automatically produce content and interact with humans via social media, spread rumors, spam, malware, misinformation.[]
2. Now we explain more the publisher/spreader category: the news publisher is the part who initiated the news and the fake news spreader is the part who is responsible for diffusing the news among the social media users:
    - News Publishers : They are fake news websites, with the intent of either promote opinions or generate clickbait traffic. Many of these websites are counterfeit websites that are disguised as legitimate sites. Some examples are ABCnews.com.co and Bloomberg.ma.
    - Fake News Spreaders: the definition of fake news spreader includes both bad actors such as bots and sockpuppets that deliberately spread disinformation with the intent of deceiving, and regular users who may unintentionally spread misleading information.

3. More types of fake news spreaders [61]:
   - Criminal/Terrorist Organizations:

     Criminal gangs and terrorist organizations are exploiting OSNs as the means to diffuse false information to achieve their goals.
   - Activist or Political Organizations:

     Various organizations share false information in order to either promote their organization, demote other rival organizations, or for pushing a specific narrative to the public. examples include political parties that share false information, especially near major elections.
   - Governments:

     Historically, governments were involved in the spreading of fake news for various reasons. More recently, with the proliferation of the Internet, governments utilize the social media to manipulate public opinion on specific topics. Furthermore, there are reports that foreign governments share fake news on other countries in order to manipulate public opinion on specific topics that regard the particular country. Some examples include the alleged involvement of the Russian government in the 2016 US elections and Brexit.
   - Hidden Paid Posters and State-sponsored Trolls:

     They are a special group of users that are paid in order to disseminate fake news on a particular content or targeting a specific demographic. Usually, they are employed for pushing an agenda; e.g., to influence people to adopt certain social or business trends. Similar to bots, these actors disseminate fake news for profit. However, this type is substantially harder to distinguish than bots because they exhibit characteristics similar to regular users.
   - Journalists:

     Individuals that are the primary entities responsible for disseminating news both to the online and to the offline world. However, in many cases, journalists are found in the center of controversy as they post fake news for various reasons. For example, they might change some stories so that they are more appealing, in order to increase the popularity of their platform, site, or newspaper.
   - Useful Idiots:

     Useful idiots are users that share fake news mainly because they are manipu-

lated by the leaders of some organization or because they are naive. Usually, useful idiots are normal users that are not fully aware of the goals of the organization, hence it is extremely difficult to identify them.

- Individuals that benefit from false information:

  Refer to various individuals that will have a personal gain by spreading fake news. This is a very broad category ranging from common persons like an owner of a cafeteria to popular individuals like political persons.

- Trolls:

  The term troll is used in great extend by the Web community and refers to users that aim to do things to annoy or disrupt other users, usually for their own personal amusement. In the context of fake news propagation, we define trolls as users that post controversial news to provoke other users or inflict emotional pressure.

- Bots:

  In the context of fake news, bots are programs that are part of a bot network (Botnet) and are responsible for controlling the online activity of several fake accounts with the aim of disseminating fake news. Note that various types of bots exist, which have varying capabilities; for instance, some bots only repost content, promote content (e.g., via vote manipulation on Reddit or similar platforms), and others post "original" content.

1.3 The fight against fake news

1.3.1 The dangers of fake news

The rapid spread of Fake News and disinformation online can have profound consequences. Examples include:

- Distrust in the media: so many people have lost trust in social media because of the increasing amount of stressful fake news examples include the recent COVID19 crisis. that also helped in the spread of false or discredited science – e.g. anti-vax movement
- Platforms for harmful conspiracy theories and hate speech: thanks to internet bots in almost all social media platforms that plant their hate speech seeds against

minorities.

- Confusion of ideas, creating an atmosphere of suspicion and confusion among people, through economic and political pressure, films..etc.
- Attracting minorities, directing their thinking and opinions to serve the source of the fake news, and this is practiced through international organizations and global non-profit bodies, so that these minorities become a pressure card against any country that opposes the decisions of the great powers or stands in their way.
- Destroying the national, religious and social affiliation of peoples, by creating a void between people, their governments, their religion and their history.

1.3.2 Recognizing Fake news

In order to protect ourselves from fake news we need to first recognize the fake news, and that's a hard task to do just like we explained through the pages of this chapter, so the most effective way is to only trust news that can be verified. In today's fast-paced world of social media, fake news surrounds us every day, everywhere.thus we have to be careful and think twice before disseminating any information, these steps down below can help to fight against fake news:

- Considering the Source

  Thinking about the actual source of the news and the supporting Sources and looking at the sources cited in the article. Are they themselves credible? Do they even exist?
- Checking multiple sources

  Relying on a single article is a mistake. Reading from various sources and diverse sources and perspectives can help in drawing accurate conclusions.
- Checking the Author

  Researching the credibility of authors and their field of expertise , their reputation in the community, whether they have a specific agenda, or if the person posting is a real person.
- Checking the Date

  Ensuring the publication date is recent and not just an older story rehashed.
- Checking the comments

  Even if the article, video, or post is legitimate, checking the comments posted in

response is a must. Quite often links or comments posted in response can be auto-generated by bots or by people hired to put out bad, confusing, or false information.

- Checking the one's Biases

  Being objective. Because the biases influence the response to the article. Instead of only reading sources that simply confirm our beliefs,it is good if we challenge ourselves by reading other sources that we normally would not review.

- Checking the Funding

  Even legitimate publications have sponsors and advertisers who can influence an article or source.

- Reposting carefully

  Fake news relies on believers to repost, retweet, or otherwise forward false information. So it is always a good advice to think twice or hold off on sharing it with others.

1.3.3 Detecting fake news

Although many fake news stories may seem misleading at first glance, most can be uncovered through simple methods. The more the strategies listed below are used, the easier it will be to distinguish fake news from real ones.[62]

1. Content based identification
   - Cue and Feature-based Methods

     -Scientific Content Analysis (SCAN)

     -Linguistic-based Cue Set (LBC)
   - Linguistic Analysis-based Methods

     -N-gram Approach

     - Part-of-Speech Tags

     -Probabilistic Context Free Grammar
   - Deep Learning Content–based Methods

     -Convolutional Neural Networks(CNN)

     -Recurrent neural network(RNN)
2. Feedback based identification
   - Propagation Pattern Analysis

     -Propagation Tree Kernels

-Propagation Tree Neural Networks

-Propagation Process Modeling

- Temporal Pattern Analysis

  -Temporal Variation Features

  -Temporal Pattern with Recurrent Neural Networks

- Response Text Analysis

  -User Response Generation

  -Deep Attention

  -Stance Detection

- Response User Analysis

  -User Features

  -User Group Analysis

3. Intervention based identification

   - Mitigation Strategies

     - Decontamination

     - Competing Cascades

     - Multi-stage Intervention

   - Identification Strategies

     - Network Monitoring

     - Crowd-sourcing

     - User Behavior Modeling

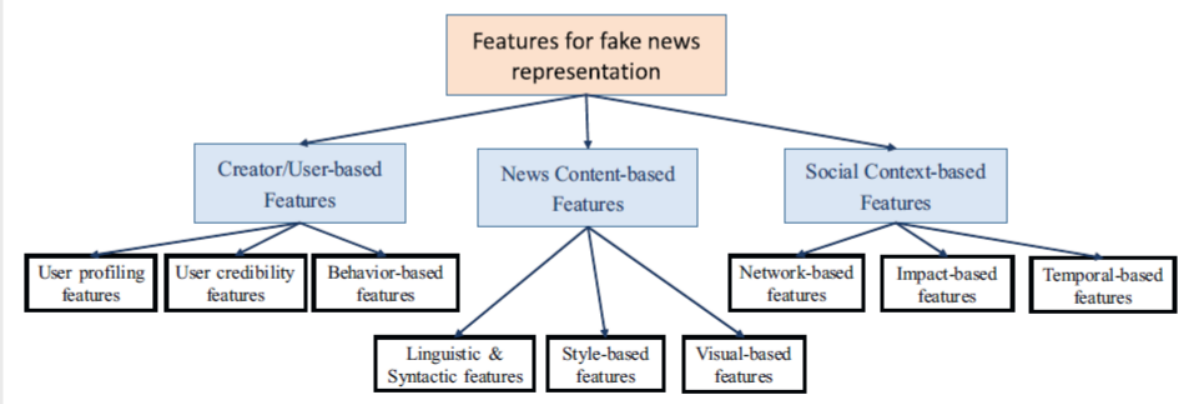

Figure 1.2: Different types of features for fake news representation and identification.

[60]

Conclusion

In this chapter, we defined the meaning of false information and fake news, their types, how to create them and ways to detect them. We have also mentioned some examples. In the next chapter, we will talk about machine learning and artificial neural networks, which are widely used in the field of computer science and many other fields, and we will also discuss the SVM and Random Forest algorithms.

Chapter 2

Artificial Intelligence and Machine Learning

Introduction

Today, artificial intelligence (AI) has become the most important field of computer science, and many fields such as economics, industry, medicine and information systems have greatly benefited from the emergence of this sophisticated and evolving science...constantly and daily. The development of AI has exceeded expectations. A few decades ago, owning hardware or software close to human intelligence seemed impossible and unrealistic. Today, however, there are human supremacy programs in many areas such as video games, information dissemination, manufacturing, decision-making, and medical diagnostic ... etc. This amazing evolution of AI is closely linked to the explosive rise of machine learning, which has become the most popular field of artificial intelligence since 2010 and the most used by the majority of researchers. In this chapter,first we will talk about artificial intelligence , its history, its sub-fields, after that we will talk about machine learning, its types and its applications finally we will be focusing on some of the major algorithms of the machine learning.

2.1 Artificial Intelligence (AI)

2.1.1 What is artificial intelligence?

Artificial intelligence is the capability of a computer system to mimic human cognitive functions such as learning and problem-solving, using math and logic to simulate the reasoning that people use to learn from new information and make decisions. The intangible intelligence is composed of: Reasoning, Learning, Problem Solving, Perception, Linguistic Intelligence. [13]

Advantages and disadvantages of AI

1. Advantages

   The AI has so many advantages, we mention: Reduction in human error that can cause serious problems, its availability because the AI model does not need rest like humans and it takes faster and more precised decisions compared to humans.
2. Disadvantages AI also had some advantages like: Potential for misuse for negative reasons, it can cause dearth of talent of humans.

2.1.2 The history of AI and machine learning

The field has a long history rooted in the U.S military science and statistics, with contributions from philosophy, psychology, mathematics, and cognitive science.
Artificial intelligence was originally designed to make computers more useful and able to think for themselves. Most historians trace the birth of artificial intelligence to a research project in 1956 at Dartmouth College that explored topics such as problem solving and symbolic methods.
In the 1960s, the U.S. Department of Defense began to take an interest in this type of work and put more investments on training computers to mimic human thinking. For example, the U.S. Defense Advanced Research Projects Agency (DARPA) conducted road mapping projects in the 1970s. DARPA began producing intelligent personal assistants as early as 2003, long before Google, Amazon or Microsoft were working on similar projects. This work paves the way for the automated and formalized thinking we see in computers today.[4]
Based on capabilities, AI can be classified into three types: Narrow (Weak) AI, General AI and Super (Strong) AI.

Types of artificial intelligence

- Artificial Narrow Intelligence: have narrow capabilities. These Artificial Intelligence systems are designed to solve one single problem and would be able to execute a single task very well, like recommending a product for an e-commerce user or predicting the weather. And it is the only kind of Artificial Intelligence that exists today.
- Artificial General Intelligence: It's defined as AI which has a human-level of cognitive function, across a wide variety of domains such as language processing, image processing, computational functioning and reasoning and so on.
- Artificial Super Intelligence: An Artificial Super Intelligence (ASI) system are supposed to surpass all human capabilities. This would include decision making, taking rational decisions, and even includes things like making better art and building emotional relationships.

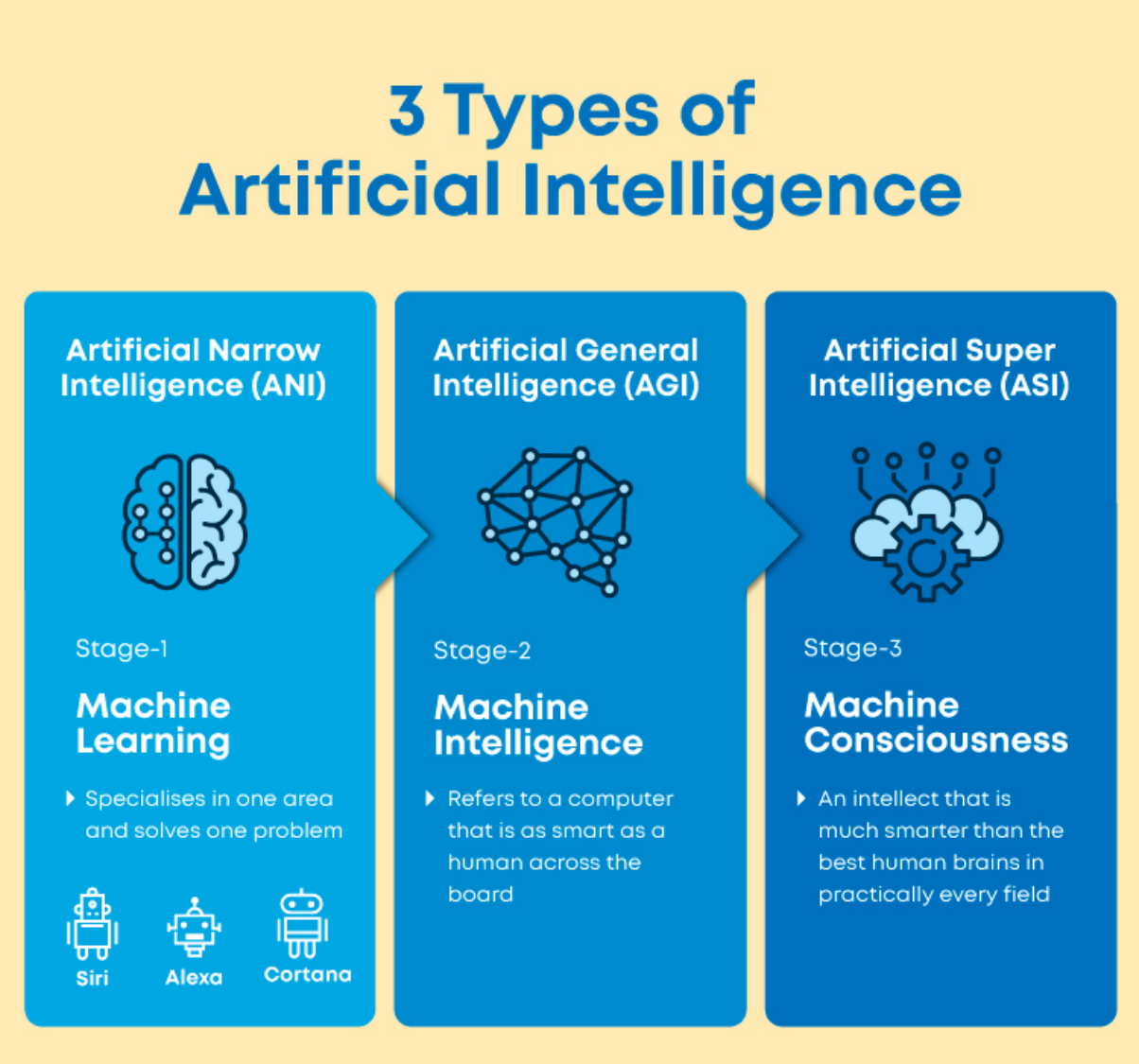

Figure 2.1: The three types of artificial intelligence.
[29]

Currently, we are working with weak AI and general AI. The future of AI is Strong AI for which it is said that it will be more intelligent than humans.

2.1.3 Sub-fields of Artificial Intelligence

As a whole, artificial intelligence contains many sub-fields, including: [59]

- Machine learning (ML)
  automates analytical model building. It uses methods from neural networks, statistics, operations research and physics to find hidden insights in data without being explicitly programmed where to look or what to conclude [32]. we will talk more

about ML in the coming headlines.

- Computer vision

  relies on pattern recognition and deep learning to recognize what's in a picture or video. When machines can process, analyze and understand images, they can capture images or videos in real time and interpret their surroundings. [7]

- Expert System

  It is a knowledge-based system, meaning that it is provided with a database containing and, constantly, collecting all the information needed to access and address a peculiar problem, It emulates the decision-making process performed by a human expert , being mainly provided with an inference engine that is able to process a rule set based on the collected knowledge. [52]

- Data Mining

  Data mining is another subdomain of AI and can be defined as a process that aims to generate knowledge from data and presents findings comprehensively to the user. Generating knowledge in the context of DM can be translated to the discovering of new and non-trivial patterns, relations and trends in data useful to the user.

  DM as a process involves, in essence, the collection and selection of data, the pre-processing of data, data analysis itself including the visualization of results, interpretation of findings, and the application of knowledge. To pre-process and analyze data, ML and statistics methods are deployed in DM. Findings from DM processes can be distinguished in descriptive ones, where knowledge is represented in form of models that depict patterns and relations in data and predictive ones, where knowledge is represented in a prediction of future conditions, trends and relations [54]

- Robotics

  Robotics involves the creation of machines that can perform human movement and mimic human behavior. In a nutshell, the field of robotics is a set of sciences related to artificial intelligence, machine learning, electronics, nanotechnology and many others.

  The discourse focusing on the developments in the field of robotic technologies highlights the implications that robots will have on work and employment; whereas at the other end, there is considerable optimism about the learning and training

opportunities that can create for business and people in organizations.

Research efforts on robotic technologies can be therefore categorized in job replacement, human-robot collaboration, and learning opportunities. [58]

- Natural language processing

  is the ability of computers to analyze, understand and generate human language, including speech. The next stage of NLP is natural language interaction, which allows humans to communicate with computers using normal, everyday language to perform tasks.[4]

2.1.4 Artificial Intelligence and Machine Learning

While artificial intelligence is an all-encompassing science that mimics human skills, machine learning is a specific subset of artificial intelligence that trains machines how to learn.

Artificial Intelligence	Machine learning
Artificial intelligence is a technology which enables a machine to simulate human behavior.	Machine learning is a subset of AI which allows a machine to automatically learn from past data without programming explicitly.
The goal of AI is to make a smart computer system like humans to solve complex problems.	The goal of ML is to allow machines to learn from data so that they can give accurate output.
In AI, we make intelligent systems to perform any task like a human.	In ML, we teach machines with data to perform a particular task and give an accurate result.
AI is working to create an intelligent system which can perform various complex tasks.	Machine learning is working to create machines that can perform only those specific tasks for which they are trained.

The main applications of AI are Siri, customer support using catboats, Expert System, Online game playing, intelligent humanoid robot, etc.	The main applications of machine learning are Online recommender system, Google search algorithms, Facebook auto friend tagging suggestions, etc.
On the basis of capabilities, AI can be divided into three types, which are, Weak AI, General AI, and Strong AI.	Machine learning can also be divided into mainly three types that are Supervised learning, Unsupervised learning, and Reinforcement learning.

Table 2.2: Key differences between Artificial Intelligence and Machine learning. [9]

The relation between AI,ML and Deep Learning

As we have already defined the machine learning, now we explain what is the deep learning:

Deep Learning:

is a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called artificial neural networks. Deep Learning concepts are used to teach machines what comes naturally to us humans. Using Deep Learning, a computer model can be taught to run classification acts taking image, text, or sound as an input. Deep Learning is becoming popular as the models are capable of achieving state of the art accuracy. Large labelled data sets are used to train these models along with the neural network architectures.

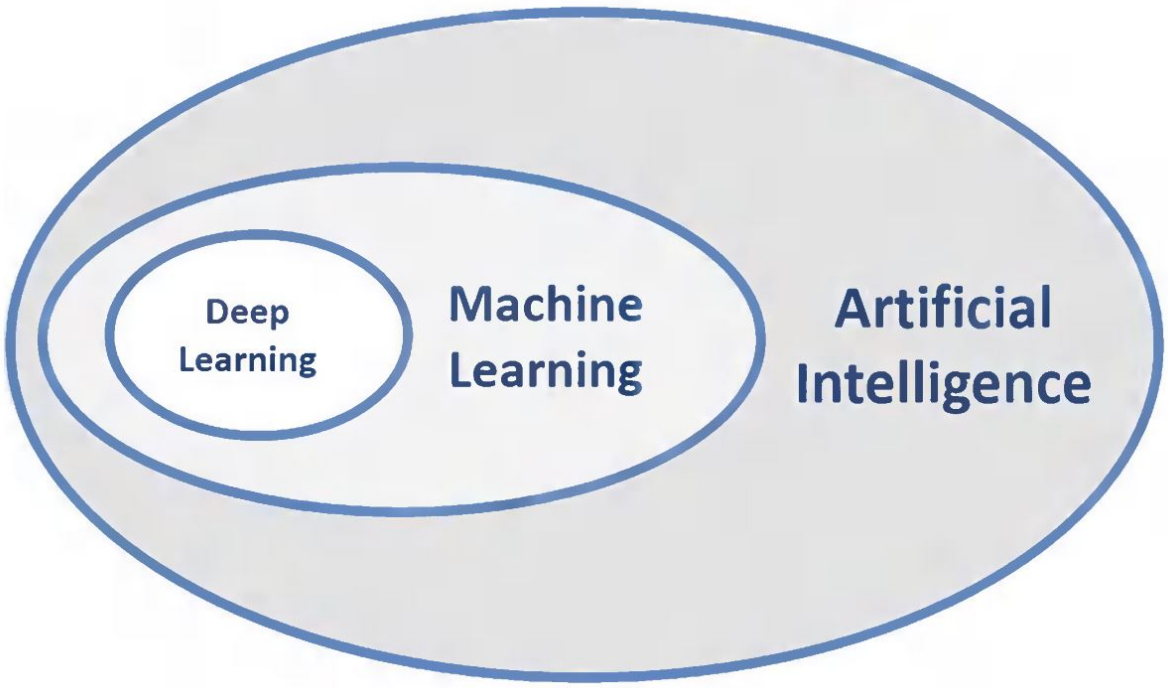

Figure 2.2: The relation between AI , ML and Dl .

[29]

2.2 Machine learning

In this section we give a full definition of the Machine learning, its applications and its sub-fields.

2.2.1 Definition

Machine learning is an application of artificial intelligence (AI) that provides systems with the ability to automatically learn and improve from data without being explicitly programmed. Machine learning-based techniques have been successfully applied in various fields ranging from pattern recognition, computer vision, spacecraft engineering, finance, entertainment, and computational biology to biomedical and medical applications [32].

2.2.2 Applications of machine learning

Machine learning applications are everywhere. Moreover, many people use them every day. We cite a few examples of these applications:

- Virtual personal assistants
- Video surveillance
- Filtering spam emails and malicious programs
- Online fraud detection
- Search engines
- Online customer service
- Object recognition
- Sentiment analysis
- Medical services
- Age / sex identification

The Benefits of Machine Learning

The benefits of Machine Learning are very important, we cite some of them:

- Identification of models and extraction of useful information
- No human intervention required (automation)
- Continuous improvement
- Heterogeneous and multidimensional data processing

2.2.3 Types Machine Learning

Machine learning paradigms differ in their approach. Each paradigm is characterized by the type of inputs and outputs, and the type of task or problem it is supposed to solve.

SUPERVISED MACHINE LEARNING

is based on supervision. It means in the supervised learning technique, we train the machines using the "labelled" data-set, and based on the training, the machine predicts the output. Here, the labelled data specifies that some of the inputs are already mapped to the output. More preciously, we can say; first, we train the machine with the input and corresponding output, and then we ask the machine to predict the output using the test data-set.

The main goal of the supervised learning technique is to map the input variable(x) with the output variable(y). Some real-world applications of supervised learning are Risk Assessment, Fraud Detection, Spam filtering, etc.

1. Classification

   Classification algorithms are used to solve the classification problems in which the output variable is categorical, such as "Yes" or No, Male or Female, Red or Blue, etc. The classification algorithms predict the categories present in the dataset. Some real-world examples of classification algorithms are Spam Detection, Email filtering, etc. Some popular classification algorithms are: Random Forest Algorithm, Decision Tree Algorithm, Logistic Regression Algorithm, Support Vector Machine Algorithm... etc.

2. Regression

   Regression is a supervised learning technique predicting continuous responses (numerical values), regression models are used to predict continuous value like salary, prices and weights, it is one of the most important tools for machine learning and widely used statistics, it makes predictions by learning the relationship between data characteristics and continuous-valued observed results.
   Some popular Regression algorithms are given below: Simple Linear Regression Algorithm, Multivariate Regression Algorithm, Decision Tree Algorithm, Lasso Regression... etc.

advantages and disadvantages of Supervised ML

1. Advantages
   - Since supervised learning work with the labelled dataset so we can have an exact idea about the classes of objects.
   - These algorithms are helpful in predicting the output on the basis of prior experience.
2. Disadvantages
   - These algorithms are not able to solve complex tasks.
   - It may predict the wrong output if the test data is different from the training data.
   - It requires lots of computational time to train the algorithm.

Applications of Supervised Learning

Supervised machine learning is used widely in so many fields, we mention from them:

- Image Segmentation
- Medical Diagnosis
- Fraud Detection
- Spam detection
- Speech Recognition

UNSUPERVISED MACHINE LEARNING

Unsupervised learning algorithms take a set of data that only contains inputs and find structure in the data, such as clustering or clustering of data points. Algorithms therefore learn from test data that has not been labeled, ranked, or categorized. These algorithms identify commonalities in data and react based on the presence or absence of these commonalities in each new piece of data. A central application of unsupervised learning is in the area of density estimation in statistics, although unsupervised learning encompasses other areas involving summarizing and explaining features of data. unsupervised machine learning means essentially clustering.

1. Clustering

   The clustering technique is used when we want to find the inherent groups from the data. It is a way to group the objects into a cluster such that the objects with the most similarities remain in one group and have fewer or no similarities with the objects of other groups. An example of the clustering algorithm is grouping the customers by their purchasing behaviour.
   Some popular Clustering algorithms: K-Means Clustering algorithm, Mean-shift algorithm, DBSCAN Algorithm, Principal Component Analysis, Independent Component Analysis... etc.

2. Association

   Association is an unsupervised learning technique, which finds interesting relations among variables within a large data-set. The goal of this learning algorithm is to find the dependency of one data item on another data item and map those variables

accordingly so that it can generate maximum profit. This algorithm is mainly applied in Market Basket analysis, Web usage mining, continuous production, etc. Some popular Association algorithms are given below: Apriori Algorithm , Eclat, FP-growth algorithm.

advantages and disadvantages of Unsupervised ML

1. Advantages
    - These algorithms can be used for complicated tasks compared to the supervised ones because these algorithms work on the unlabeled data-set.
    - Unsupervised algorithms are preferable for various tasks as getting the unlabeled data-set is easier as compared to the labelled data-set.
2. Disadvantages
    - The output of an unsupervised algorithm can be less accurate as the data-set is not labelled, and algorithms are not trained with the exact output in prior.
    - Working with Unsupervised learning is more difficult as it works with the unlabelled data-set that does not map with the output.

Applications of Unsupervised Learning

- Network Analysis
- Recommendation Systems
- Anomaly Detection
- Singular Value Decomposition

SEMI-SUPERVISED MACHINE LEARNING

In the case of semi-supervised learning algorithms, some data lack training labels, but they can still be used to improve the quality of a model. In weakly supervised learning, training labels are noisy, limited, or imprecise; however, these tags are often cheaper to obtain, resulting in more effective training sets.

advantages and disadvantages of Semi-supervised ML

1. Advantages
    - It is simple and easy to understand the algorithm.

- It is highly efficient.
- It is used to solve drawbacks of Supervised and Unsupervised Learning algorithms.

2. Disadvantages
   - Iterations results may not be stable.
   - We cannot apply these algorithms to network-level data.
   - Accuracy is low.

REINFORCED MACHINE LEARNING

Reinforcement learning is an area of machine learning that concerns how software agents should take action in an environment in order to maximize some notion of cumulative reward. Due to its generality, the field is studied in many other disciplines, such as game theory, control theory, operations research, information theory, simulation-based optimization, multi-systems -agents, statistics and genetic algorithms. Reinforcement learning algorithms do not assume knowledge of an exact mathematical model. They are used when exact patterns are impractical. They are frequently used in autonomous vehicles or to learn how to play a game against a human opponent. Due to its way of working, reinforcement learning is employed in different fields such as Game theory, Operation Research, Information theory, multi-agent systems.
some of its Real-world Use cases are in: Video Games, Resource Management, Robotics, Text Mining.

advantages and disadvantages of Reinforcement ML

1. Advantages
   - It helps in solving complex real-world problems which are difficult to be solved by general techniques.
   - The learning model of RL is similar to the learning of human beings; hence most accurate results can be found.
   - Helps in achieving long term results.
2. Disadvantages
   - RL algorithms are not preferred for simple problems.
   - RL algorithms require huge data and computations.

- Too much reinforcement learning can lead to an overload of states which can weaken the results.

2.3 Some of Machine Learning Algorithms

Here we give example definitions of the most popular machine learning algorithms:[5]

2.3.1 K-nearest neighbor algorithm

K-nearest neighbors (KNN) is to classify a new given unseen data point by looking at the K given data points in the training set that are closest to it in the input or feature space. We use distance metric, such as Euclidean distance to find the K nearest neighbors of the new data point.

2.3.2 Random Forest

Random forest is a Supervised Machine Learning Algorithm that is used widely in Classification and Regression problems. It builds decision trees on different samples and takes their majority vote for classification and average in case of regression.
One of the most important features of the Random Forest Algorithm is that it can handle the data set containing continuous variables as in the case of regression and categorical variables as in the case of classification. It performs better results for classification problems.

2.3.3 K-means

It is a type of unsupervised algorithm which solves the clustering problem. Its procedure follows a simple and easy way to classify a given data set through a certain number of clusters (assume k clusters). Data points inside a cluster are homogeneous and heterogeneous to peer groups.
In K-means, we have clusters and each cluster has its own centroid. Sum of square of difference between centroid and the data points within a cluster constitutes within sum of square value for that cluster. Also, when the sum of square values for all the clusters are added, it becomes total within sum of square value for the cluster solution.

We know that as the number of cluster increases, this value keeps on decreasing but if you plot the result you may see that the sum of squared distance decreases sharply up to some value of k, and then much more slowly after that. Here, we can find the optimum number of cluster.

2.3.4 Support Vector Machine

Support Vector Machine or SVM is one of the most popular Supervised Learning algorithms, which is used for Classification as well as Regression problems. However, primarily, it is used for Classification problems in Machine Learning.
The goal of the SVM algorithm is to create the best line or decision boundary that can segregate n-dimensional space into classes so that we can easily put the new data point in the correct category in the future. This best decision boundary is called a hyperplane.

Conclusion

Machine learning is the present and the future of computing. In addition, most recent technological breakthroughs have been achieved with this tool, which proves its power and efficiency day after day. In this chapter, we have defined artificial intelligence and machine learning and its algorithms such as SVM and Random Forest that we used in our work , we will explain more about them in the next chapter in addition to the model and implementation tools used in our work.

Chapter 3

Methodology and Results

Introduction

As explained in chapter one, the spread of fake news has become one of the daily problems that we face every time we check our social media accounts, causing big troubles to some big companies, famous people and even normal individuals, it became imperative to fight this spread by detecting fake news/ fake news spreaders.Thanks to the artificial intelligence techniques and machine learning algorithms that are already mentioned in chapter two the detection of fake news/ fake news spreaders has become possible and even very accurate , according to some previous works that we will discuss at the end of this chapter where we will present the implementation and development of our model for fake news spreaders detection. We will use classification supervised machine learning algorithms and several programming tools to organize the database of two types, fake articles spreaders and real articles spreaders then train our model.

3.1 Problematic description

3.1.1 Motivations and Problem

Although it is a recurring problem today, the famous "fake news" has always existed. Indeed, false information being sent voluntarily or not is a phenomenon that has been present over the centuries. Being capable of distorting an individual's perception of the world.

We may be exposed to false news at any time, and participate in its dissemination by sharing it on social media or even orally. It is therefore appropriate for everyone to develop their skills and validate information from several sources before it is considered correct.

The questions asked are how can the fake news spreading on social media can be solved? Are there modern ways to detect fake news and their authenticity? or at least minimized? How can the fake news be detected? How can fake news spreaders be detected?

3.1.2 Related works

Some works have already worked on the the 8th International Author Profiling Shared Task at PAN 2020, we will present some of the results of these works in this section.

The participants had to discriminate from Twitter authors whether they are keen to spread fake news or not. The provided data cover the English and Spanish languages. The participants used different features to address the task, mainly: (i) n grams; (ii) stylistics; (iii) personality and emotions. Concerning machine learning algorithms, the most used ones were Support Vector Machines and Logistic Regression, or combinations of both. we notice that the Logistic regression algorithm and SVM in the work [47] gave the same result compared to the average combination result of the same two algorithms among other algorithms in [44] , few participants approached the task with deep learning techniques. In such cases, they used ANN and RF just like [45] that gave a high accuracy. According to the results, traditional approaches obtained higher accuracies than deep learning ones. The team with the highest performance according to the table above is [43] that used SVM and linear SVM.

3.1.3 Solution

To solve the fake news spreaders problem, we used a machine learning based model, using the SVM algorithm in the first experiment and Random Forest algorithm in the second experiment, in the third one we will combine them to have a better result.
Our proposed Ensemble approach for profiling fake news spreaders in Twitter is explained in this section. Architecture for building the Ensemble model using the fake news spreader training set provided by PAN 2020.

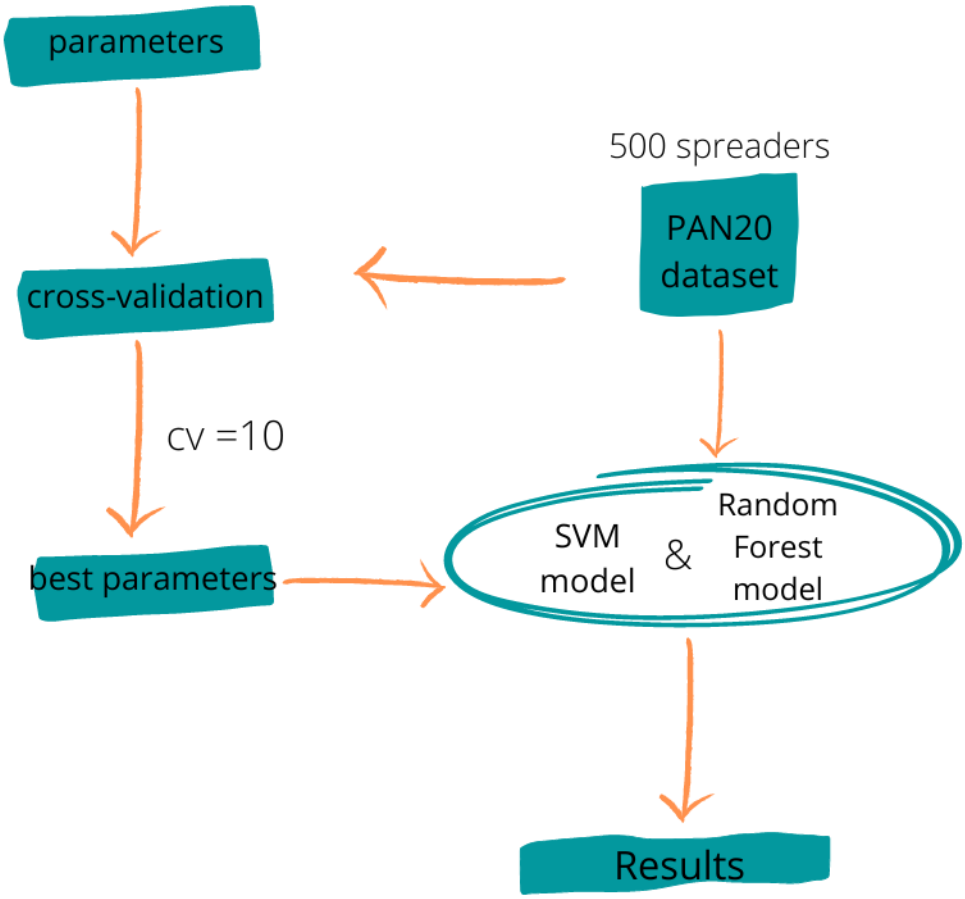

Figure 3.1: the structure of our model

3.2 Method and Implementation Tools

We describe in this section the data-base we used in our work and the implementation tools that we used to have the results we had.

3.2.1 Data-set Description

The PAN-AP-20 presents the statistics of the corpus that consists of 500 authors for two languages, English and Spanish. For each author, retrieved via the Twitter API her last 100 Tweets. The corpus for each language is balanced, with 250 authors for each class (fake and real news spreaders). [18].

The goal is to decide if a new author is a spreader of fake news or not. Formally, we are given a decision problem which states:

Given an author A who tweets in language L (in our case it's only English) and from the collection of tweets C, given a subset of tweets C A (of an author A), CA = t1; t2; ... ; t100 the authors are labelled:(0 a non fake-news spreader; 1 a fake-news spreader)
We used the Cross-Validation (CV) to have the best parameters and for a better splitting. We used the 10 folds validation after extracting the best parameters , this means that the training was done one 9/10 of the folds and the testing was done on the remaining 1/10 of the folds.
the table bellow describes our data-set.

Language	Fake news spreaders	Non-Fake news spreaders	Total
English	250 fake news spreaders	250 non fake news spreaders	500
Spanish	250 fake news spreaders	250 non fake news spreaders	500

Table 3.1: the PAN CLEF 2020 Data-set used in this work .

In this project, we only took the English part and we worked on it.

3.2.2 Implementation Tools

In order to make this work, we used so many tools which we explain in this part.

- Google colab

  Colab is a free Jupyter notebook environment that runs entirely in the cloud. Most importantly, it does not require a setup, also the notebooks created can be simultaneously edited by the team members. Colab supports many popular machine learning libraries.[30]

- Python

  Python is an interpreted, object-oriented, high-level programming language with dynamic semantics. Its high-level built in data structures, combined with dynamic typing and dynamic binding, make it very attractive for Rapid Application Development, also for use as a scripting or glue language to connect existing components together. Python is simple, easy to learn syntax emphasizes readability and therefore reduces the cost of program maintenance. It also supports modules and packages, which encourages program modularity and code reuse..[33]

- Sklearn

  Scikit-learn is a key library for the Python programming language that is typically used in machine learning projects. Scikit-learn is focused on machine learning tools including mathematical, statistical and general purpose algorithms that form the basis for many machine learning technologies. As a free tool, Scikit-learn is very important in many different types of algorithm development for machine learning and related technologies. [19]

3.2.3 Training

The following section includes description of the proposed method with the corresponding intermediate steps.

Pre processing

First, the tweets from each author are concatenated, and only the printable characters are kept, which means no non-printable characters are preserved. Data pre-processing includes the following steps:

- From the original data punctuation is removed
- All characters are lower case
- URL and hashtags are removed
- Stop-words are removed
- Emojies removed
- Stemming

Classifier selection

Classification model we aimed for this task are the Random Forest and the Support Vector Machines. we give definitions and more details about each one of them.

SVM Definition

A support vector machine (SVM) is a supervised machine learning model that uses classification algorithms for two-group classification problems,in our case its the fake news spreaders and truth news spreaders. After giving an SVM model sets of labeled training data for each category (1 for fake news spreaders and 0 for the others), they're able to

categorize new text. It is very suitable for text classification problems, where it's common to have access to a data-set of at most a couple of thousands of tagged samples.[2]

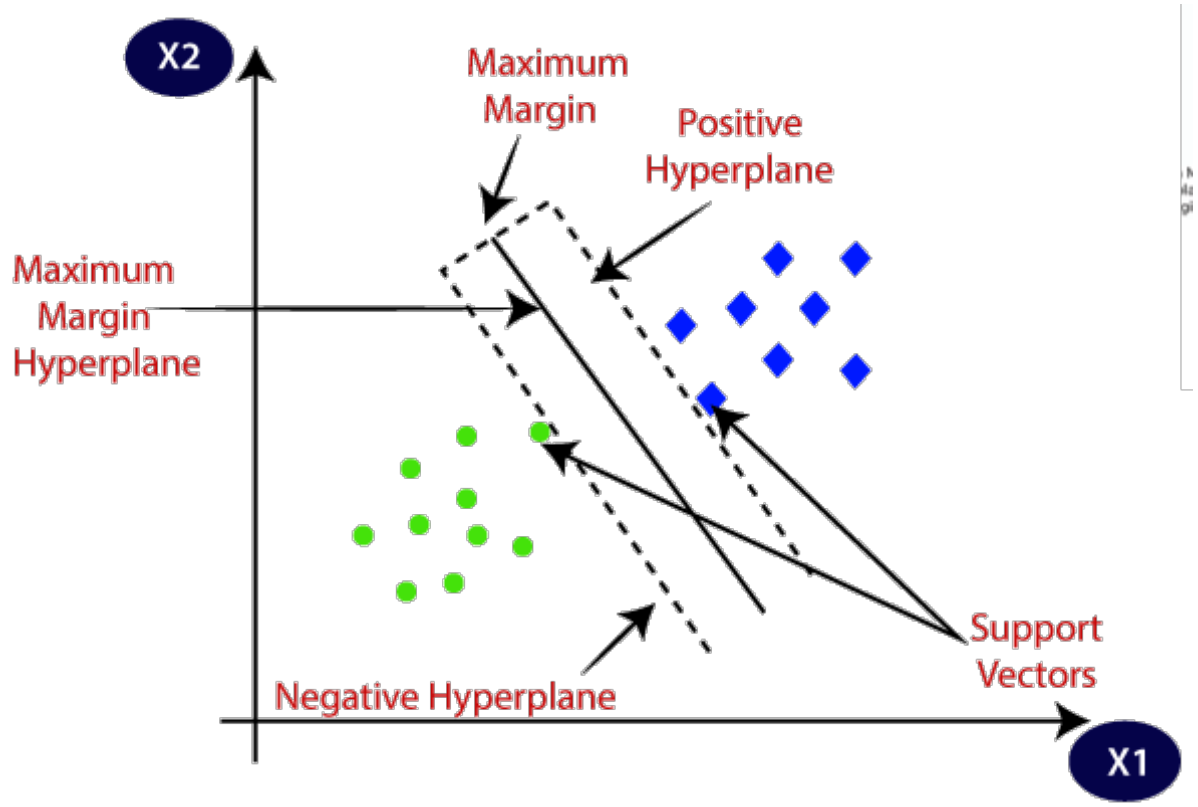

Figure 3.2: SVM Algorithm

The working mechanism of SVM

SVM is about selecting the best hyper-plane: the hyper-plane as a definition is the lines/decision boundaries to segregate the classes in n-dimensional space. Now the best hyper-plane is the one that gives the best decision boundary that helps to classify the data points. [21]

One reasonable choice as the best hyperplane is the one that represents the largest separation or margin between the two classes.[2] The dimensions of the hyperplane depend on the features present in the data-set, which means if there are 2 features (as shown in image), then hyperplane will be a straight line. And if there are 3 features, then hyperplane will be a 2-dimension plane.

We always create a hyperplane that has a maximum margin, which means the maximum distance between the data points.[23]

SVM Kernel

The SVM kernel is a function that takes low dimensional input space and transforms it into higher-dimensional space, in other words it converts not separable problem to separable problem. It is mostly useful in non-linear separation problems. Simply put the kernel, it does some extremely complex data transformations then finds out the process to separate the data based on the labels or outputs defined.[16] In this project we used the linear kernel

Why use SVM?

Well SVM it capable of doing both classification and regression. But we will focus on using SVM for classification because that was our goal from using it. Because our data is Linearly separable,in other words it can be separated using a single Line. And that is one of the most common kernels to be used for such problems.
Mostly used when there are a Large number of Features in a particular Data Set. One of the examples where there are a lot of features, is Text Classification, as each alphabet is a new feature. So we mostly use Linear Kernel in Text Classification.[6]

Types of SVM

SVM can be of two types:

- Linear SVM Linear SVM is used for linearly separable data, which means if a data-set can be classified into two classes by using a single straight line, then such data is termed as linearly separable data, and classifier is used called as Linear SVM classifier.Which is the one used for this project.
- Non-linear SVM Non-Linear SVM is used for non-linearly separated data, which means if a data-set cannot be classified by using a straight line, then such data is termed as non-linear data and classifier used is called as Non-linear SVM classifier.

SVM Application

SVM can be used in so many different domains the need classification or regression such as:

- Protein Structure Prediction
- Intrusion Detection

- Handwriting Recognition
- Detecting Steganography in digital images
- Breast Cancer Diagnosis
- Almost all the applications where ANN is used

[22]

Advantages

We talk more about some of the advantages that lead us to use this machine learning algorithm:

- Effective in high dimensional cases
- SVM's are very good when we have no idea on the data.
- Works well with even unstructured and semi structured data like text, Images and trees.
- The kernel trick is real strength of SVM. With an appropriate kernel function, we can solve any complex problem.
- It scales relatively well to high dimensional data.
- SVM models have generalization in practice, the risk of over-fitting is less in SVM.

Disadvantages

And just like anything else, SVMs also have some disadvantages, we mention:

- Choosing a "good" kernel function is not easy.
- Long training time for large data-sets.
- Difficult to understand and interpret the final model, variable weights and individual impact.
- Since the final model is not so easy to see, we can not do small calibrations to the model hence its tough to incorporate our business logic.

Now, we explain the second machine learning algorithm that we used in this work too.

Random Forest Definition

Random Forest is a popular machine learning algorithm that belongs to the supervised learning technique. It can be used for both Classification and Regression problems in ML. It is based on the concept of ensemble learning, which is a process of combining

multiple classifiers to solve a complex problem and to improve the performance of the model.

As the name suggests, "Random Forest is a classifier that contains a number of decision trees on various subsets of the given data-set and takes the average to improve the predictive accuracy of that data-set." Instead of relying on one decision tree, the random forest takes the prediction from each tree and based on the majority votes of predictions, and it predicts the final output. The greater number of trees in the forest leads to higher accuracy and prevents the problem of overfitting. The below diagram explains the working of the Random Forest algorithm:

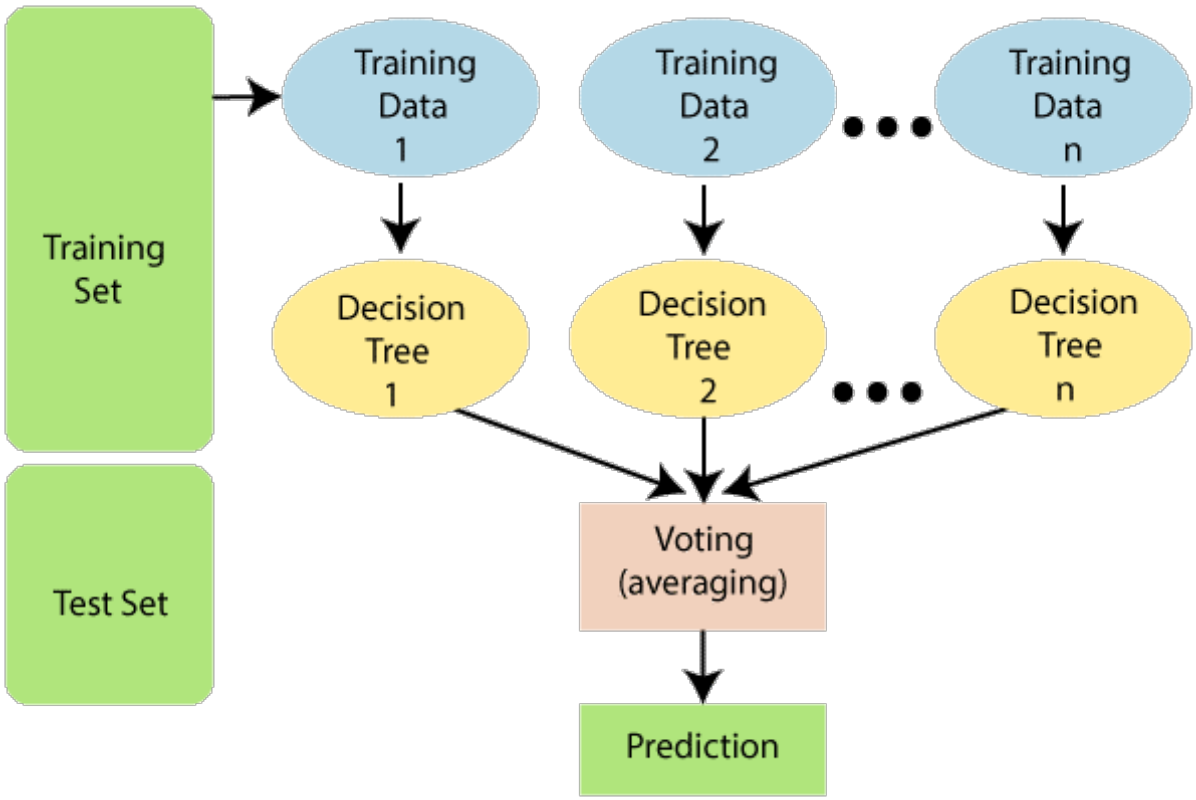

Figure 3.3: Random Forest Algorithm

Random Forest uses two methods

1. Bagging– It creates a different training subset from sample training data with replacement and the final output is based on majority voting. For example, Random Forest. Which is the technique that we used in our project.
2. Boosting– It combines weak learners into strong learners by creating sequential models such that the final model has the highest accuracy. For example, ADA

BOOST, XG BOOST [25].

Why use Random Forest?

Below are some points that explain why we used the Random Forest algorithm to solve the problem we had:

- It takes less training time as compared to other algorithms.
- It predicts output with high accuracy, even for the large data-set it runs efficiently.
- It can also maintain accuracy when a large proportion of data is missing.

The working mechanism of Random Forest algorithm

Random Forest works in two-phase first is to create the random forest by combining N decision tree, and second is to make predictions for each tree created in the first phase. The Working process can be explained in the below steps:

1. Step-1: Select random K data points from the training set.
2. Step-2: Build the decision trees associated with the selected data points (Subsets).
3. Step-3: Choose the number N for decision trees that you want to build.
4. Step-4: Repeat Step 1 and 2.
5. Step-5: For new data points, find the predictions of each decision tree, and assign the new data points to the category that wins the majority votes.

Applications of Random Forest

There are mainly four sectors where Random forest mostly used:

- Banking: Banking sector mostly uses this algorithm for the identification of loan risk.
- Medicine: With the help of this algorithm, disease trends and risks of the disease can be identified.
- Land Use: We can identify the areas of similar land use by this algorithm.
- Marketing: Marketing trends can be identified using this algorithm.

Advantages of Random Forest

Some of the positive points about Random Forest that motivated us to use it:

- Random Forest is capable of performing both Classification and Regression tasks.

- It is capable of handling large data-sets with high dimensionality.
- It enhances the accuracy of the model and prevents the overfitting issue.

Disadvantages of Random Forest

The Random Forest also has some weak points:

- Although random forest can be used for both classification and regression tasks, it is not more suitable for Regression tasks[14].

In this part we explain in details the three experiments we have done to solve the fake news spreaders problem.

Experiment 1: SVM

We used scikit-learn python library for our experiments and training N-grams models. Experimental searches have been done for tuning N-grams and TF-IDF parameters using 10 fold cross-validation. - N-grams, it converts a collection of text documents to a matrix of token counts as a term frequency(TF) representation.
– N-grams with TF-IDF weighting, it works by determining the relative frequency of words in a specific document compared to the inverse proportion of that word over the entire document corpus. Words that are common in documents tend to have higher TF-IDF numbers than others. TF-IDF matrix representation of documents presents fingerprinted features for documents. We used a pipline to grid search over parameters of all estimators in the pipeline at once. the grid search best parameters: the n-grame range we used is (1,6), the min-tf=8 ,svm-classifier= kernel(linear)

Experiment 2: Random Forest

in the Random Forest algorithm, we used the random forest classifier with the following parameters that we obtained using the Grid Search too:ngram-range=(1,2) , min-df=8 ,n-estimator=100, min-samples-leaf=1 .[20] and We used a pipline to grid search over parameters of all estimators in the pipeline

Experiment 3: SVM and Random Forest Combined

as a final step we combine the SVM classifier and the Random Forest classifier using an estimator . we used the voting.classifier to combine the two methods:

VotingClassifier(estimators=[('svm', classifierSVC), ('RF', classifierRF),],voting='soft', weights=[4,1]).

Further definitions

Here we define more some of the tools we used in the devoleppement of this work.

- GridSearchCV

  Grid search is a tuning technique that attempts to compute the optimum values of hyperparameters. It is an exhaustive search that is performed on a the specific parameter values of a model. The model is also known as an estimator.[31]

- Cross Validation

  Cross-validation is a technique that is used for the assessment of how the results of statistical analysis generalize to an independent data set. Cross-validation is largely used in settings where the target is prediction and it is necessary to estimate the accuracy of the performance of a predictive model. The prime reason for the use of cross-validation rather than conventional validation is that there is not enough data available for partitioning them into separate training and test sets (as in conventional validation). This results in a loss of testing and modeling capability.[7]

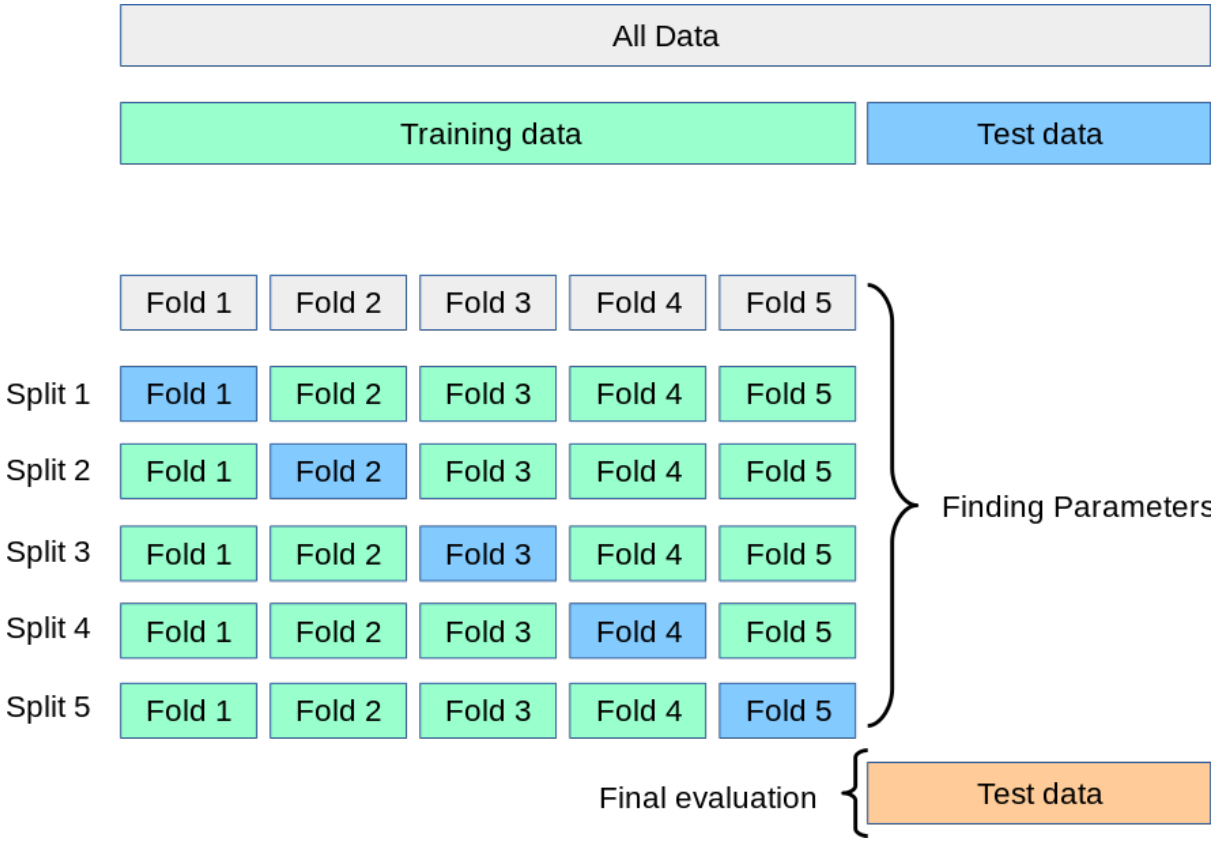

Figure 3.4: Cross-Validation example

[3]

- Tf-idf

  TF-IDF (term frequency-inverse document frequency) is a statistical measure that evaluates how relevant a word is to a document in a collection of documents.

  This is done by multiplying two metrics: how many times a word appears in a document, and the inverse document frequency of the word across a set of documents.[26]

- N-gram

  An N-Gram is a connected string of N items from a sample of text or speech. The N-Gram could be comprised of large blocks of words, or smaller sets of syllables. N-Grams are used as the basis for functioning N-Gram models, which are instrumental in natural language processing as a way of predicting upcoming text or speech. [28]

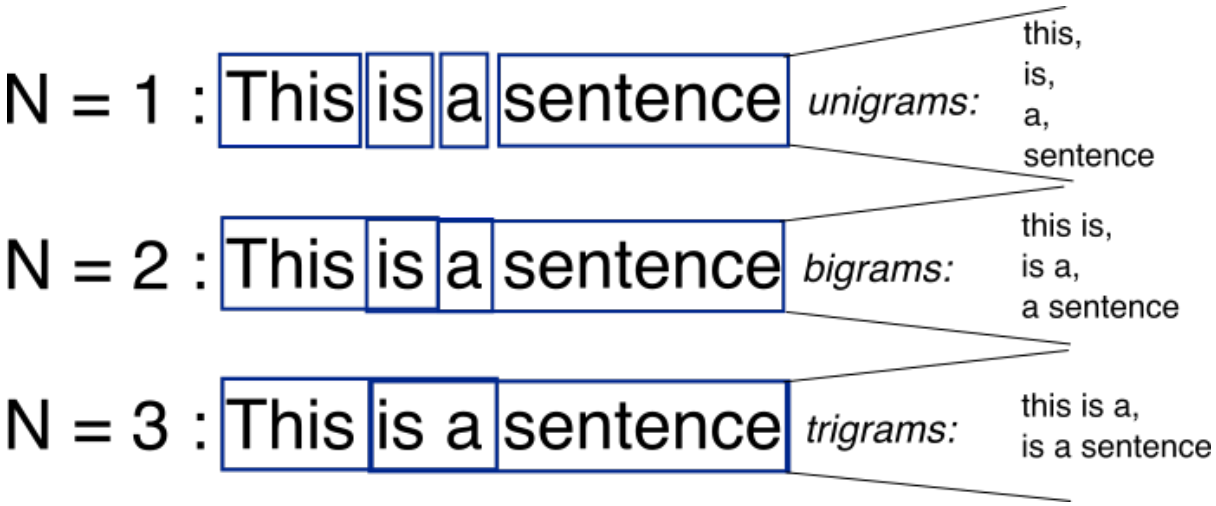

Figure 3.5: n-gram model

[28]

3.3 Results and Discussion

3.3.1 Results

We constructed two approaches one that was based on Support Vector Machine (SVM) classifier and the second was modeled with Random Forest (RF) as classifier. The array of experiments conducted yielded the final results of our work in Table 3.2.

Method	Accuracy
SVM	0.72
Random Forest	0.70
SVM+RF ensembled	0.74

Table 3.2: Experimental Results.

Thus we focused more on the combination of SVM and Random Forest because it gave the highest accuracy amongst the other methods.

3.3.2 Comparison

Some of the results of the related works we mentioned before that worked on the same topic and the same data-set are shown in the table below:

Research	Methods	Results
Detecting fake news spreaders in social network via linguistic and personality features[56]	N grams , SVM, sentiment analysis	Spanish training: 0.7 testing: 0.76 English training : 0.73 Testing: 0.71 Psycholinguistic: English: 0.72/ Spanish: 0.80
Multi aspect classification ensemble approach for profiling fake news spreaders on twitter [45]	Random forest, ANN	Accuracy:85.20
Fake news spreaders profiling through behavioural analysis [38]	Random forest, KNN, decision tree, SVC	English:0.67 Spanish:0.71 Average:0.69
Analyzing User Profiles for Detection of Fake News Spreaders on Twitter [44]	Logistic Regression, K-Neighbors, Random Forest, Decision Tree, and SVM	training: 0.68 Test : 0.64
Ensemble model for profiling fake news spreaders on Twitter[55]	Linear SVC, logistic regression, n grams	English:0.73 Spanish:0.67
Multilingual Detection of Fake News Spreaders via Sparse Matrix Factorization [47]	LR and SVM	English LR: 0.71 SVM: 0.70 Spanish LR: 0.79 SVM: 0.79

Profiling fake news spreaders using characters and words N-grams [43]	SVM and linear SVM	English SVM 81.33 Linear SVM 86.28 Spanish SVM 80.99 Linear SVM 81.83

Table 3.4: Some related works about profiling Fake News Spreaders that used the same data-set.

3.3.3 Discussion

In this table, we have presented some of the results of the 8th International Author Profiling Shared Task at PAN 2020, hosted at CLEF 2020. The participants had to discriminate from Twitter authors whether they are keen to spread fake news or not. The provided data cover the English and Spanish languages. The participants used different features to address the task, mainly: (i) n grams; (ii) stylistics; (iii) personality and emotions. The team with the highest performance according to the table above is [43] that used SVM and linear SVM.The results we obtained are almost similar to [47] even though we worked on English tweets only . Looking at the results and the error analysis, we can conclude that: it is possible to automatically identify potential Fake News Spreaders in Twitter with high precision, even when only textual features are used.

Conclusion

In this section we described the practical side of this work, we defined the main problem and the real motives for making this whole project, then we went more in details with the architecture of our model that contains 3 algorithms SVM, Random Forest and the combination of the SVM and Random Forest together.we also exposed the results we got out of the combination and last we discussed some related works results and compared them to the results we obtained.

General Conclusion

Online social media have drastically transformed how information is shared and assimilated by individuals and communities, fake news and rumors are often spread on online social networks to deceive users and promote certain views.[45][48]. We may be exposed to false information or fake news at any time, and participate in its dissemination by sharing it on social networks or even orally. It is therefore appropriate for everyone to develop their skills and validate information from several sources before it is considered correct. Historically, this problem is not new, but social media platforms have led to an exponential increase in this phenomenon in recent years. The increasing threat of fake news creating and spreading is very serious and it is high time to take also serious ways to fight it [57].

The objective of of our work was to distinguish authors who have disseminated fake news from those who have never done so. For this task, we used a machine learning based model using the Support Vector Machine and the Random Forest algorithms. The data-set used is PAN CLEF 2020 which is a collection of sample messages from known fake news spreaders and truth-tellers, gathered from the Twitter platform using around 50000 twits half of them are fake news spreaders. [18]

We got inspired by some previous works [51, 49, 42, 35, 37] which have worked on the same problem using the same data-set but solving it using different artificial intelligence techniques.

This thesis started with a general introduction and ends with a general conclusion was composed of three chapters. In the first chapter we talked about false information generally, fake news specifically and the fight against fake news.

In the second chapter we talked about artificial intelligence and machine learning and their applications and advantages.

In the last chapter we explained the model we used and the implementation tools used

in this work and finally the obtained results.

We had obtained satisfying results using the supervised machine learning approaches (Support Vector Machine and Random Forest). We worked on three experiments; first one using SVM algorithm only, second one; using Random Forest algorithm only; and the third one was combining the first two algorithm. At the end, from our results and from the previous works we conclude that it is possible to detect fake news spreaders with a good accuracy using machine learning algorithms. Thus we can fight this phenomenon using technological approaches, especially on social media platforms.

Just like any other works, this one is not without faults and shortcomings, we wish to use the deep learning methods in the future.

Bibliography

[1] 10 Examples of Fake News from History. https://www.thesocialhistorian.com/fake-news/. Accessed: 2022-06-1.

[2] 1.4. Support Vector Machines. https://scikit-learn.org/stable/modules/svm.html. Accessed: 2022-05-13.

[3] 3.1. Cross-validation: evaluating estimator performance. https://scikit-learn.org/stable/modules/cross$_v$*alidation.html. Accessed* : 2022 − 06 − 1.

[4] Artificial intelligence, machine learning, deep learning and beyond. https://www.sas.com/es$_c$*o/insights/articles/big* − *data/artificial* − *intelligence* − *machine*−*learning*−*deep*−*learning*−*and*−*beyond.html. Accessed* : 2022−05−30.

[5] Commonly used Machine Learning Algorithms (with Python and R Codes). https://www.analyticsvidhya.com/blog/2017/09/common-machine-learning-algorithms/. Accessed: 2022-05-30.

[6] Creating linear kernel SVM in Python. https://www.geeksforgeeks.org/creating-linear-kernel-svm-in-python/. Accessed: 2022-06-1.

[7] Cross-Validation. https://www.techopedia.com/definition/32064/cross-validation. Accessed: 2022-06-1.

[8] Definition of disinformation. https://www.merriam-webster.com/dictionary/disinformation. Accessed: 2022-05-21.

[9] Difference between Artificial intelligence and Machine learning. https://www.javatpoint.com/difference-between-artificial-intelligence-and-machine-learning. Accessed: 2022-06-10.

[10] Fact check: Fake news thrives amid Russia-Ukraine war. https://www.dw.com/en/fact-check-fake-news-thrives-amid-russia-ukraine-war/a-61477502. Accessed: 2022-06-11.

[11] False information definition. https://www.lawinsider.com/dictionary/false-information. Accessed: 2022-05-30.

[12] From "brute" to "thug:" the demonization and criminalization of unarmed Black male victims in America. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5004736/. Accessed: 2022-06-13.

[13] Introduction to Artificial Intelligence. https://becominghuman.ai/introduction-to-artificial-intelligence-5fba0148ec99. Accessed: 2022-05-30.

[14] Introduction to Random Forest in Machine Learning. https://www.section.io/engineering-education/introduction-to-random-forest-in-machine-learning/. Accessed: 2022-05-21.

[15] Misinformation, Disinformation and Mal-Information . https://www.mediadefence.org/ereader/publications/introductory-modules-on-digital-rights-and-freedom-of-expression-online/module-8-false-news-misinformation-and-propaganda/misinformation-disinformation-and-mal-information/. Accessed: 2022-05-21.

[16] ML - Support Vector Machine(SVM). https://www.tutorialspoint.com/machine-learning- with- python/machine-learning -with- python- classification- algorithms-support-vector$_m achine.htm. Accessed : 2022 - 05 - 13$.

[17] November 1, 1755: The Earthquake of Lisbon: Wrath of God or Natural Disaster? . https://blogs.scientificamerican.com/history-of-geology/november-1-1755-the-earthquake-of-lisbon-wraith-of-god-or-natural-disaster/. Accessed: 2022-06-13.

[18] Profiling Fake News Spreaders on Twitter 2020. https://pan.webis.de/clef20/pan20-web/author-profiling.html. Accessed: 2022-06-1.

[19] Scikit-Learn. https://www.techopedia.com/definition/33860/scikit-learn. Accessed: 2022-06-10.

[20] sklearn.ensemble.RandomForestClassifier. https://scikit-learn.org/stable/modules/generated/sklearn.ensemble.RandomForestClassifier.html. Accessed: 2022-05-21.

[21] Support Vector Machine Algorithm. https://www.geeksforgeeks.org/support-vector-machine-algorithm/. Accessed: 2022-05-13.

[22] Support Vector Machine (SVM) Introduction — Machine Learning. https://pub.towardsai.net/support-vector-machine-svm-introduction-machine-learning-8c56b7da63f1. Accessed: 2022-05-13.

[23] Support Vector Machines (SVM) Algorithm Explained. https://monkeylearn.com/blog/introduction-to-support-vector-machines-svm/. Accessed: 2022-05-13.

[24] The Long and Brutal History of Fake News . https://www.politico.com/magazine/story/2016/12/fake-news-history-long-violent-214535/. Accessed: 2022-06-14.

[25] Understanding Random Forest. https://www.analyticsvidhya.com/blog/2021/06/understanding-random-forest/. Accessed: 2022-05-21.

[26] Understanding TF-ID: A Simple Introduction. https://monkeylearn.com/blog/what-is-tf-idf/. Accessed: 2022-06-1.

[27] U.S. Diplomacy and Yellow Journalism, 1895–1898. https://history.state.gov/milestones/1866-1898/yellow-journalism. Accessed: 2022-06-13.

[28] What is an N-Gram? https://deepai.org/machine-learning-glossary-and-terms/n-gram. Accessed: 2022-06-1.

[29] What is Artificial Intelligence? How does AI work, Types, Trends and Future of it? . https://www.mygreatlearning.com/blog/what-is-artificial-intelligence/. Accessed: 2022-05-13.

[30] What is Google Colab? https://blog.educationecosystem.com/what-is-google-colab/. Accessed: 2022-06-10.

[31] What Is Grid Search? https://medium.com/fintechexplained/what-is-grid-search-c01fe886ef0a. Accessed: 2022-06-1.

[32] What Is Machine Learning: Definition, Types, Applications And Examples. https://www.potentiaco.com/what-is-machine-learning-definition-types-applications-and-examples/. Accessed: 2022-05-30.

[33] What is Python? Executive Summary. https://www.python.org/doc/essays/blurb/. Accessed: 2022-06-10.

[34] Jonathan Albright. Welcome to the era of fake news. *Media and Communication*, 5(2):87–89, 2017.

[35] Janek Bevendorff, Bilal Ghanem, Anastasia Giachanou, Mike Kestemont, Enrique Manjavacas, Ilia Markov, Maximilian Mayerl, Martin Potthast, Francisco Rangel, Paolo Rosso, et al. Overview of pan 2020: Authorship verification, celebrity profiling, profiling fake news spreaders on twitter, and style change detection. In *International Conference of the Cross-Language Evaluation Forum for European Languages*, pages 372–383. Springer, 2020.

[36] Alessandro Bondielli and Francesco Marcelloni. A survey on fake news and rumour detection techniques. *Information Sciences*, 497:38–55, 2019.

[37] Jakab Buda and Flora Bolonyai. An ensemble model using n-grams and statistical features to identify fake news spreaders on twitter. In *CLEF (Working Notes)*, 2020.

[38] Matteo Cardaioli, Stefano Cecconello, Mauro Conti, Luca Pajola, and Federico Turrin. Fake news spreaders profiling through behavioural analysis. In *CLEF (Working Notes)*, 2020.

[39] Elinor Carmi, Simeon J Yates, Eleanor Lockley, and Alicja Pawluczuk. Data citizenship: Rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review*, 9(2):1–22, 2020.

[40] Ivan De Martino, Rocco D'Apolito, Alexander S McLawhorn, Keith A Fehring, Peter K Sculco, and Giorgio Gasparini. Social media for patients: benefits and drawbacks. *Current reviews in musculoskeletal medicine*, 10(1):141–145, 2017.

[41] The Lancet Infectious Diseases. The covid-19 infodemic. *The Lancet. Infectious Diseases*, 20(8):875, 2020.

[42] Xinhuan Duan, Elham Naghizade, Damiano Spina, and Xiuzhen Zhang. Rmit at pan-clef 2020: Profiling fake news spreaders on twitter. In *CLEF (Working Notes)*, 2020.

[43] Daniel Yacob Espinosa, Helena Gómez-Adorno, and Grigori Sidorov. Profiling fake news spreaders using character and words n-grams. In *CLEF (Working Notes)*, 2020.

[44] María S Espinosa, Roberto Centeno, and Álvaro Rodrigo. Analyzing user profiles for detection of fake news spreaders on twitter. In *CLEF (Working Notes)*, 2020.

[45] Clemens Hörtenhuemer and Eva Zangerle. A multi-aspect classification ensemble approach for profiling fake news spreaders on twitter. In *CLEF (Working Notes)*, 2020.

[46] Simon Kemp. Digital in 2020: global digital overview. *We are Social, Hootsuite, jan*, 2020.

[47] Boshko Koloski, Senja Pollak, and Blaz Skrlj. Multilingual detection of fake news spreaders via sparse matrix factorization. In *CLEF (Working Notes)*, 2020.

[48] David M. J. Lazer, Matthew A. Baum, Yochai Benkler, Adam J. Berinsky, Kelly M. Greenhill, Filippo Menczer, Miriam J. Metzger, Brendan Nyhan, Gordon Pennycook, David Rothschild, Michael Schudson, Steven A. Sloman, Cass R. Sunstein, Emily A. Thorson, Duncan J. Watts, and Jonathan L. Zittrain. The science of fake news. *Science*, 359(6380):1094–1096, 2018.

[49] Juan Pizarro. Using n-grams to detect fake news spreaders on twitter. In *CLEF (Working Notes)*, 2020.

[50] Julie Posetti and Alice Matthews. A short guide to the history of 'fake news' and disinformation. *International Center for Journalists*, 7(2018):2018–07, 2018.

[51] Francisco Rangel, Anastasia Giachanou, Bilal Hisham Hasan Ghanem, and Paolo Rosso. Overview of the 8th author profiling task at pan 2020: Profiling fake news spreaders on twitter. In *CEUR Workshop Proceedings*, volume 2696, pages 1–18. Sun SITE Central Europe, 2020.

[52] Aurora Saibene, Michela Assale, and Marta Giltri. Expert systems: definitions, advantages and issues in medical field applications. *Expert Systems with Applications*, 177:114900, 2021.

[53] Karen SANTOS-D'AMORIM and Májory K Fernandes de Oliveira MIRANDA. Misinformation, disinformation, and malinformation: Clarifying the definitions and examples in disinfodemic times. *Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação*, 26, 2021.

[54] Günther Schuh, Gunther Reinhart, Jan-Philipp Prote, Frederick Sauermann, Julia Horsthofer, Florian Oppolzer, and Dino Knoll. Data mining definitions and applications for the management of production complexity. *Procedia CIRP*, 81:874–879, 2019.

[55] HL Shashirekha, MD Anusha, and Nitin S Prakash. Ensemble model for profiling fake news spreaders on twitter. In *CLEF (Working Notes)*, 2020.

[56] Anu Shrestha, Francesca Spezzano, and Abishai Joy. Detecting fake news spreaders in social networks via linguistic and personality features. In *Working Notes of CLEF 2020-Conference and Labs of the Evaluation Forum*, 2020.

[57] Shalini Talwar, Amandeep Dhir, Puneet Kaur, Nida Zafar, and Melfi Alrasheedy. Why do people share fake news? associations between the dark side of social media use and fake news sharing behavior. *Journal of Retailing and Consumer Services*, 51:72–82, 2019.

[58] Demetris Vrontis, Michael Christofi, Vijay Pereira, Shlomo Tarba, Anna Makrides, and Eleni Trichina. Artificial intelligence, robotics, advanced technologies and human resource management: a systematic review. *The International Journal of Human Resource Management*, 33(6):1237–1266, 2022.

[59] Ming-Hwa Wang. Artificial intelligence and subfields. *Santa Clara University, Department of Computer Engineering*, 2017.

[60] Claire Wardle, Hossein Derakhshan, et al. Thinking about 'information disorder': formats of misinformation, disinformation, and mal-information. *Ireton, Cherilyn;*

Posetti, Julie. Journalism,'fake news'& disinformation. Paris: Unesco, pages 43–54, 2018.

[61] Savvas Zannettou, Michael Sirivianos, Jeremy Blackburn, and Nicolas Kourtellis. The web of false information: Rumors, fake news, hoaxes, clickbait, and various other shenanigans. *Journal of Data and Information Quality (JDIQ)*, 11(3):1–37, 2019.

[62] Xichen Zhang and Ali A Ghorbani. An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management*, 57(2):102025, 2020.