TOP THREE ADVANCEMENTS IN ARTIFICIAL INTELLIGENCE

ASSIGNMENT – 4

IFT 598 – AI IN CYBER SECURITY

Arizona State University

Manohar Akula – 1223335191

Sep 2022

Abstract:

The field of artificial intelligence [1] has made significant strides in nearly all of its traditional sub-areas in the last five years, including vision, speech recognition and generation, natural language processing (understanding and generation), image and video generation, multi-agent systems, planning, decision-making, and the integration of vision and motor control for robotics. Furthermore, ground-breaking applications were developed in a number of fields, including as gaming, medical diagnostics, logistics systems, autonomous driving, language translation, and interactive personal support. Examples of several significant advancements are provided in the following sections.

Today, more people are utilizing AI to enhance their conference call backdrops, dictate to their phone, get recommendations for shopping, news, or entertainment, and so much more. Machine learning, particularly deep learning (including generative adversarial networks or GANs) and reinforcement learning driven by large-scale data and computational resources, is the primary technology underpinning the majority of the most obvious advancements. Deep networks can now create artificial content, such as counterfeit photographs that pass for the genuine thing, thanks to the significant advancement of GANs. GANs are made up of two interconnected parts: a discriminator that separates the output of the generator from naturally occurring material, and a generator that generates realistic content. Both parties gain knowledge from one another, improving in their respective jobs over time. One of the real-world applications is GAN-based medical picture augmentation, which automatically creates false images to increase the data set required to train networks to make diagnoses. Over the past ten years, awareness of deep learning's amazing ability has progressively increased. Recent research have started to provide light on why and under what circumstances deep learning is effective. Machine-learning technologies have emerged from academia into the real world in a variety of ways during the past 10 years that are both exciting and unsettling. The top three advances in Artificial Intelligence for societal benefit are as follows: Natural Language Processing, Machine Learning, Artificial Intelligence.

1. Natural Language Processing (NLP):

Development:

The field of artificial intelligence known as "Natural Language Processing" (NLP) aims to help computers comprehend, analyze, and use human languages. By leveraging human language, NLP enables computers to converse with people. The capacity for computers to read text, hear voice, and understand it is provided by natural language processing. In order to bridge the communication gap between humans and computers, NLP depends on a number of academic fields, including computational linguistics and computer science. In general, NLP aims to comprehend the links between language's shorter, more fundamental units, known as tokens (words, periods, etc.).

In 1957, Noam Chomsky released his book Syntactic Structures. In it, he overturned earlier theories about language, coming to the radical conclusion that a language's sentence structure needed to be altered in order for a computer to grasp it.

John McCarthy published the computer language LISP (Locator/Identifier Separation Protocol), which is still in use today, in 1958. In order to mimic a psychiatrist utilizing reflection techniques, ELIZA, a "typewritten" remark and answer mechanism, was created in 1964.

The NRC and ALPAC stopped supporting research on machine translation and natural language processing in 1966, starting the first AI and NLP pause.

Natural Language Processing and Artificial Intelligence research needed approximately fourteen years (until1980) to recover from the broken expectations generated by ardent enthusiasts.

Impact on Society:

Yoshio Bengio and his colleagues presented the first neural "language" model in 2001, utilizing a feed-forward neural network. The feed-forward neural network is an artificial neural network that does not employ connections to generate a cycle. In this form of network, data flows solely in one way, from input nodes to hidden nodes and finally to output nodes. The feed-forward neural network is distinct from recurrent neural networks in that it lacks cycles and loops.

Risks and Challenges:

NLP is a strong technology with several advantages, yet there are certain limitations and issues with Natural Language Processing:

- Contextual words and phrases, as well as homonyms - The same words and phrases can have distinct meanings depending on the context of a statement, and many terms, particularly in English, have the same pronunciation but completely different meanings.
- Ambiguity - In NLP, ambiguity refers to statements and phrases that have two or more different meanings. Lexical ambiguity occurs when a word can be employed as a verb, noun, or adjective.
- Text and speech errors - Text analysis might be hampered by misspelled or misused terms. Autocorrect and grammatical correction software can handle frequent errors, but they don't always comprehend the writer's purpose.
- Domain-specific jargon - Various firms and sectors frequently employ extremely distinct jargon. A healthcare NLP processing paradigm, for example, would be significantly different from one used to handle legal texts. There are already a lot of analytic tools that have been trained for certain disciplines, but very narrow companies may need to design or train their own models.

Initial Trends:

In 2011, Apple's Siri was recognized as one of the world's first successful NLP/AI assistants utilized by mainstream customers. The Automated Speech Recognition mechanism of Siri converts the owner's speech into digitally interpreted ideas. The Voice-Command system then matches such concepts to established commands, resulting in particular activities being initiated. For example, if Siri asks, "Do you want to hear your balance?" it will comprehend and act on a "Yes" or "No" response[2].

Current Trends:

In many current real-world applications, natural language processing is the driving force behind machine intelligence. Here are a couple such examples:

- Spam detection: You might not think of spam detection as an NLP solution, yet the top spam detection solutions examine emails for language that commonly indicates spam or phishing.
- Machine translation: Google Translate is an example of NLP technology at action. True machine translation entails more than simply substituting words in one language with ones in another.
- Chatbots and virtual agents: Virtual assistants like Apple's Siri and Amazon's Alexa employ speech recognition and natural language generation to reply with appropriate action or helpful comments.
- Social media sentiment analysis: Natural language processing (NLP) has evolved into an essential commercial tool for identifying hidden data insights from social media channels.
- Text summarizing: Text summarization use NLP approaches to digest massive amounts of digital text and provide summaries and synopses for indexes, research databases, and busy readers who do not have time to read complete text.

Implementations Benefiting the Society:

Fake News and Cyberbullying Detection[3]:

NLP has evolved into an indispensable tool for reducing the time and human effort required to detect and prevent the spread of fake news and disinformation. With so much incorrect information about Covid-19 circulating this year, we've already seen some fascinating attempts to automatic fake news identification (using transformers, no less), and we'll undoubtedly see more of it in 2022.

Another application of NLP for good is the identification of cyberbullying. Classifiers are being developed to detect the usage of rude, insulting, or hateful words on social media.

Given the ongoing discussion over whether or not social media information should be controlled, these NLP applications may become even more important.

Multilingual NLP:

To date, most NLP advances have been focused on English. However, businesses such as Google and Facebook are increasingly providing pre-trained multilingual models that outperform monolingual models.

Multilingual models were unheard of before to 2019, when Facebook launched XLM-R and, more recently, M2M-100, the first multilingual machine translation model capable of translating 100 languages without relying on English data.

Open-source libraries are following in the footsteps of Google and Facebook, with recent breakthroughs in language-agnostic sentence embeddings, zero-shot learning, and the availability

of multilingual embeddings, thus we may anticipate to see an increasing trend in multilingual NLP models this year.

2.Computer Vision:

Development:

Computer vision [4] is a branch of artificial intelligence (AI) that allows computers and systems to derive meaningful information from digital photos, videos, and other visual inputs and then act or recommend on that information. If artificial intelligence allows computers to think, computer vision allows them to see, watch, and comprehend. Computer vision functions similarly to human vision, with the exception that humans have an advantage. Human vision has the benefit of lifetimes of context to learn how to discern objects apart, how far away they are, if they are moving, and if there is something wrong with a picture.

For almost 60 years, scientists and engineers have been attempting to create methods for robots to perceive and analyze visual input. Experiments began in 1959, when neurophysiologists gave a cat a series of pictures in an attempt to correlate a reaction in its brain. They noticed that it responded initially to hard edges or lines, which implied that picture processing begins with basic forms such as straight edges.

In 1974, optical character recognition (OCR) technology was introduced, which could recognize text printed in any font or typeface.

David Marr, a neurologist, proved that vision works hierarchically in 1982 and presented techniques enabling robots to recognize edges, corners, curves, and other fundamental structures.

By 2000, the focus of research had shifted to object identification, and by 2001, the first real-time face recognition applications were available. The ImageNet data collection became released in 2010. It contains millions of annotated photos from a thousand object classes and serves as the foundation for today's CNNs and deep learning models. A team from the University of Toronto entered a CNN into an image recognition competition in 2012. AlexNet, the model, drastically lowered the error rate for picture recognition.

Impact on Society:

As computer vision grows more prevalent, it is beginning to transform society and the entire planet. This technology is used to boost human capacity in autonomous cars and other sectors. Current generation technology may provide the required level of precision and speed at the edge by utilizing techniques such as 3-D reconstruction.

Computer vision is already improving our lives without our knowledge. Face ID technology was initially used to unlock phones, but it has now been embraced by mobile applications for services such as investing and banking accounts, which demand a high level of security. As technology continues to automate traditional manufacturing and industrial procedures, computer vision will be and already is critical to the development of the Fourth Industrial Revolution [5].

Risks and Challenges:

Computer vision enables artificial intelligence systems to recognize faces, objects, places, and motions; yet this technology creates a number of ethical and privacy problems. Fraud, prejudice, inaccuracy, and a lack of informed consent are examples of these[6]:

- Fraud: Hackers and fraudsters have used masks and photographs to fool face recognition equipment to claim benefits or get access to a site using another person's identity.
- Bias: In law enforcement and other settings, Black and Asian faces receive considerably more incorrect identifications than white faces, increasing the likelihood of erroneous arrest. It is also considerably more likely to identify elderly persons and little children than middle-aged adults, which skews the findings and influences investigations.
- Inaccuracy: Extraneous signals, or data noise, can contribute to inaccuracy and inaccurate diagnoses in healthcare and illness detection. One CV method was discovered to predict health depending solely on the type of X-ray equipment utilized. It erroneously linked portable X-ray equipment to a specific ailment.
- Ethical Consent Violations: Without consent, researchers accumulate massive data sets of face photographs, and this data, along with data scraped from the web, is frequently used to develop military and commercial surveillance algorithms. Users are unaware that the personal information they share on the internet is later utilized as training data for surveillance apps all around the world.

Initial Trends:

The first digital image scanner, introduced in 1959, converted photos into grids of numbers that computers could identify. A few years later, a debate moderated by Lawrence "Larry" Roberts — widely regarded as the inventor of the internet as well as the father of computer vision — looked into the possibility of extracting 3-D geometrical information from 2-D perspective views of blocks. Many academics quickly recognized the need to discover techniques to identify pictures in the actual environment, and research began to focus on low-level vision tasks such as segmentation and detection. Multiple frameworks arose, such as techniques of capturing and/or recording items and recognition-by-components, which stated the human eye can recognize objects by breaking them down into their primary components. Kunihiko Fukushima produced the predecessor thirty years later.

Current Trends:

Computer vision has seen a significant increase in popularity. It is now the foundation of an autonomous future in many industries, including transportation, healthcare, agriculture, retail, manufacturing, and others. Tesla said in May that it will phase out radar in favor of Tesla Vision, a camera-based autopilot technology. Nanox is planning to buy Zebra Medical Vision, a healthcare-focused computer vision firm, for computer vision technologies that identify bone, liver, lung, and cardiovascular problems. It may be used in retail to give insight into consumer behavior, which merchants can then utilize to develop even better customer experiences.

Historically, computer vision has been unable to achieve the degree of speed and precision required to function in certain situations, such as self-checkout systems in retail locations, which is what my firm focused in.

Here are some examples of well-known computer vision tasks:

- Image classification detects and classifies images (a dog, an apple, a person's face). More specifically, it can correctly predict that a given picture belongs to a specific class. A social media company, for example, might want to use it to automatically identify and separate objectionable images uploaded by users.
- Picture classification may be used to identify a certain class of image and then detect and tabulate its existence in an image or video. Detecting defects on a manufacturing line or spotting machines in need of repair are two examples.
- Object tracking is the process of following or tracking an object after it has been discovered. This activity is frequently carried out either sequential photos or real-time video streams. Autonomous vehicles, for example, must not only identify and detect items like people, other automobiles, and road infrastructure, but they must also track them in motion in order to prevent crashes and follow traffic regulations.

Implementations Benefiting the Society:

Retail and ecommerce:

- Reducing human contacts in businesses to improve safety, provide a digital shopping experience, and save labor expenses
- Personalizing the client experience to boost engagement and make upselling and cross-selling techniques more effective
- Using next-generation in-store analytics to avoid stockouts, improve shop layout designs, and optimize staff scheduling

Healthcare:

- Improving patient identification to avoid wrong-person treatments
- Providing more accurate diagnoses using medical imaging analysis
- Providing support in surgical training and real-world procedures to improve results
- Patients' rehabilitation help

Education:

- Understanding students' learning patterns to promote personalisation and improve learning experiences
- Automating classroom surveillance to discourage test cheating
- Assessing students' papers to lessen the strain on educators

Agriculture:

- Accurately identifying pests and weeds in order to maximize chemical application

- Monitoring crop growth and the environment to maximize yields and deliver higher quality in response to increased customer demands
- Automating livestock management to decrease flock and herd losses and eliminate the need for feet in the field

3. Machine Learning:

Development:

Machine learning is a subfield of artificial intelligence (AI) [7]and computer science that utilizes data and algorithms to mimic how people learn, progressively improving its accuracy.

IBM has a long history of using machine learning. Arthur Samuel, one of its own, is credited with coining the phrase "machine learning" with his study on the game of checkers. In 1962, the self-proclaimed checkers master, Robert Nealey, played the game on an IBM 7094 computer and lost to the computer. This achievement appears minor in comparison to what can be done now, yet it is regarded a key milestone in the field of artificial intelligence.

At the Cornell Aeronautical Laboratory in 1957, Frank Rosenblatt coupled Donald Hebb's idea of brain cell interaction with Arthur Samuel's machine learning work to build the perceptron.

The closest neighbor method was developed in 1967, marking the beginning of rudimentary pattern recognition. This technique was used for route mapping and was one of the first algorithms used to solve the problem of identifying the most efficient path for traveling salespeople.

Rather than algorithms, artificial intelligence research in the late 1970s and early 1980s concentrated on logical, knowledge-based techniques.

Long short-term memory (LSTM), a neural network model proposed by Jürgen Schmidhuber and Sepp Hochreiter in 1997, is currently used for much of the voice recognition training.

The Facial Recognition Grand Challenge, a program of the National Institute of Standards and Technology, assessed popular face recognition algorithms in 2006.

Impact on Society:

Machine learning is revolutionizing the world by reshaping industries such as healthcare, education, transportation, food, entertainment, and various assembly lines, among others. It will have an influence on practically every element of people's life, including homes, automobiles, shopping, food ordering, and so on. Internet of Things (IoT) and cloud computing are both increasing the use of ML to make items and devices "smart" for themselves. ML offers potential value to companies trying to leverage big data for customer satisfaction. The underlying pattern buried in the data can be quite beneficial to company [8].

Risks and Challenges:

Machine learning technology has surely made our lives simpler as it has advanced. However, the use of machine learning in business has created a variety of ethical questions concerning AI technology. Some examples are:

Singularity in technology

- While this subject has received a great deal of public interest, many experts remain unconcerned about AI exceeding human intellect in the near future. Strong AI or superintelligence are other terms for technological singularity.
- Although superintelligence is not imminent in society, the concept poses some intriguing challenges when we examine the usage of autonomous technologies such as self-driving automobiles. It's ridiculous to believe that a driverless automobile will never be involved in an accident, but who is accountable and liable in those cases?

The influence of AI on jobs:

- While much of the public's anxiety about artificial intelligence is around job losses, this fear should probably be reframed. With each disruptive new technology, we witness a shift in market demand for certain employment types.

Privacy:

- Data privacy, data protection, and data security are frequently mentioned in conjunction with privacy. These issues have allowed politicians to make significant advances in recent years.

Initial Trends:

People began frequently engaging with AI in the 1990s, most notably when search engines based on sophisticated new algorithms were widely available [9].

The Mazda Cosmo Eunos was an underappreciated breakthrough. Yes, a vehicle is one of the most underappreciated advancements in machine learning. It was the first automobile to incorporate GPS navigation, and it was only available with automatic gearbox, which is nearly unheard of in sports cars nowadays. It also had a one-of-a-kind rotary engine that made it quieter than any automobile until electric vehicles arrived decades later. The automation provided by GPS, a touchscreen, and an automatic gearbox felt futuristic in 1990, just as self-driving cars do now. Our relationship with smart automobiles has always captivated us.

Current Trends:

Real-world Machine Learning Applications Here are a few instances of machine learning that you could encounter daily:

- Speech recognition: Speech recognition is a skill that employs natural language processing (NLP) to convert human speech into a written format. It is also known as automated speech recognition (ASR), computer speech recognition, or speech-to-text.
- Customer service: Online chatbots are replacing human agents across the consumer experience, altering how we think about customer involvement on websites and social media platforms. Chatbots answer commonly asked inquiries (FAQs) regarding issues such as shipping, or can give individualized advice to consumers, such as cross-selling items or recommending sizes.

- Recommendation engines: AI algorithms can assist find data trends that can be leveraged to generate more successful cross-selling tactics by using historical consumption behavior data. Online businesses employ this method to give appropriate product recommendations to customers throughout the checkout process.
- Automated stock trading: AI-driven high-frequency trading platforms, designed to optimize stock portfolios, execute hundreds or even millions of deals each day without human interaction.

Implementations Benefiting the Society:

Predictions While Driving:

Traffic Predictions: We've all used GPS navigation services. While we do this, our current locations and speeds are kept at a central server for traffic management. This information is then utilized to create a map of current traffic. While this aids in traffic prevention and congestion analysis, the fundamental issue is that there are fewer automobiles equipped with GPS. In such cases, machine learning assists in estimating the areas where congestion might be identified based on everyday encounters.

Surveillance Videos:

AI is currently used in video surveillance systems, allowing them to detect crime before it occurs. They monitor strange behavior such as people standing stationary for an extended period of time, tripping, or dozing on benches, among other things. As a result, the system may inform human attendants, which can eventually assist to avert disasters. When such acts are reported and verified, they assist to enhance surveillance services. This occurs as a result of machine learning working in the background.

Filtering of email spam and malware:

Email clients employ a variety of spam screening methods. Machine learning is used to ensure that these spam filters are constantly updated. When rule-based spam filtering is used, it fails to follow the latest spammer techniques. Spam filtering approaches enabled by ML include Multi-Layer Perceptron and C 4.5 Decision Tree Induction.

Detecting Online Fraud:

Machine learning is shown its ability to make cyberspace safer, with one example being the detection of financial crime online. Paypal, for example, use ML to combat money laundering. The organization employs a combination of techniques that allows them to examine millions of transactions and discern between genuine and illicit transactions between buyers and sellers.

References:

[1]. https://ai100.stanford.edu

[2]. https://www.dataversity.net/a-brief-history-of-natural-language-processing-nlp/

[3].https://www.ibm.com/cloud/learn/natural-language-processing

[4]. https://www.ibm.com/topics/computer-vision

[5].https://www.forbes.com/sites/forbestechcouncil/2021/10/14/the-evolution-of-computer-vision-and-its-impact-on-real-world-applications/?sh=59151b3c6abd

[6]. https://innodata.com/ethical-issues-in-computer-vision-and-strategies-for-success/

[7]. https://www.dataversity.net/a-brief-history-of-machine-learning/

[8]. https://www.datasciencecentral.com/how-machine-learning-is-changing-the-world/

[9].https://towardsdatascience.com/10-overlooked-machine-learning-advances-in-the-last-10-decades-2e9fe9f2f073