Literature Review

Course: MSc Computer Science

Module: Research Methods and Professional Practice

Assignment: Literature Review

Date: Sunday 17th April 2022

Student ID: 126853

1 – Introduction:

Deep Learning is a Machine Learning method used for classification of images, text and other data based on a training model that has been pre-sorted and classified either algorithmically or with human intervention. The modern topic of Deep Learning was first demonstrated in the 1970's by Japanese computer scientist Kunihiko Fukushima, who developed a basic Artificial Neural Network to automatically identify specific visual patterns (Foote, 2022).

Within this Literature Review, I will be evaluating a series of online publications focusing on how the necessity for Deep Learning techniques for object classification have changed over time. In particular, focusing on the use cases and commercially available products utilising such techniques, demonstrating how these have become more commonplace in the present time in sectors such as social media and vehicular automation. As both Machine Learning and Deep Learning are extremely broad techniques, this review will predominantly focus on the object classification aspects, whilst referring to other Machine Learning techniques where appropriate.

Research for this review will be sourced from a series of publicly available resources including Google Scholar, IEEE Explore, PrePrint publications, the Essex Library, News Articles and information from industry sources. Where possible, this will be organised in a coherent and chronological fashion to show how the studied techniques have evolved over time. Limitations of the available research and techniques will be highlighted where appropriate throughout the main body of this document.

2 – Literature Review:

2.1 – History of Deep Learning:

Deep Learning is a specific aspect of Machine Learning designed to algorithmically mimic human behaviour by a process of continual learning. The foundations for this topic were first laid out in the late 1800's (Wang & Raj, 2017), but modern Deep Learning techniques were inspired in the 1970's by Japanese computer scientist, Kunihiko Fukushima (Foote, 2022) who had used a basic Artificial Neural Network in order to accurately detect stimulus patterns despite a shift in position or distortion of shape/size (Fukushima, 1980). Since this demonstration, Deep Learning has been continually evolving and has since developed numerous practical applications within vehicular automation and online search engines, both of which have been touched upon in the following sections of this review.

Companies such as Google and Facebook have recently begun releasing software which only existed in a research environment, to reduce the barriers to developers and organisations utilising Deep Learning techniques. The two most commonly of which are TensorFlow and pyTorch, both of which are freely available and well documented, ensuring simple access to deep learning. Although, both of which require large training datasets (Sometimes running into the millions of images) which need to be provided and pre-labelled, such as those available in the free COCO dataset. Despite the models being trained on extremely large datasets, there is still room for error. Wang & Raj (2017) have demonstrated that in a series of cases, mis-classifications with their ResNet model were caused by the annotators' labelling preferences as opposed to the model and techniques themselves.

A 2018 study by Liang et al. suggests that China were planning to implement mass citizen identification with smart cameras using Deep Learning as part of their Social Credit System, which had aimed to include over 1.4 billion people by 2020 (Liang et al., 2018). Although I have been unable to locate further publications confirming whether this had been implemented, it would be the largest use of deep learning for human identification to date. Although ethically wrong, this project demonstrates that there is room in society for deep learning models for crime prevention and citizen monitoring. One such case could be the implementation of deep learning models in motorway cameras to detect those that are unaware of their surroundings or otherwise inhibited due to alcohol or drug usage based on their driving behaviour.

2.2 – Case Study – Captcha (People, Plant & Animal Detection):

Alan Turing proposed a method aptly named the “Turing Test” which was a concept for differentiating between the actions of a computer (via Artificial Intelligence) and a human (St George & Gillis, n.d.). In recent years, this theory has been implemented into a commercial product labelled as CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) which operates both, as a practical security method for websites, as well as provides the facility to gain a solution to a currently unsolved Artificial Intelligence problem (von Ahn, et al., 2003).

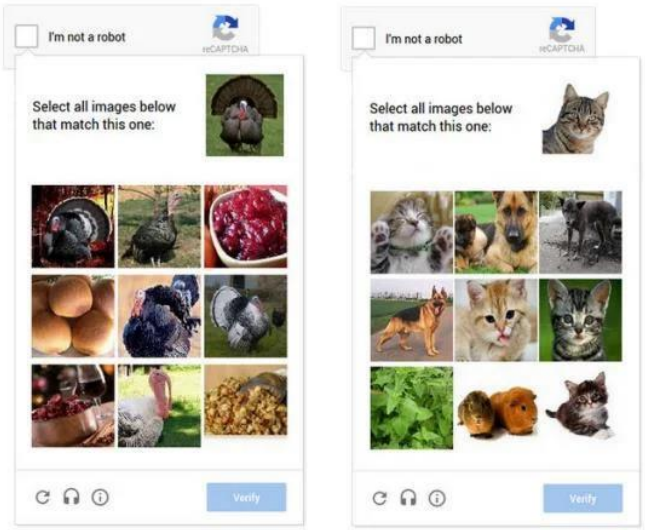

Figure 1: Google reCAPTCHA for animal classification (Lopez, 2014).

To most users of the internet, CAPTCHA-based systems are seen as a slightly frustrating barrier to completing a simple online task such as filling in a form or completing an e-commerce checkout process. Such systems are marketed to webste providers as being a low-cost solution to provide bot mitigation services and fraud detection (Google, n.d.). Security researchers have discovered that Google uses a series of unpublished additional metrics in conjunction with the AI-training tool, including mouse movements, linked Google accounts and IP addresses (Akrout et al., 2019).

Within industry, it is widely believed that Google are using their reCAPTCHA product to train incredibly large Deep Learning models which can be used to improve the results available within their search engine (O'Malley, 2018). During recent years, these models have been made available in the Google Images product, which will recognise objects within an image and will perform both, a word-based and a

visually-similar image based search. Although there is little research to support this theory, my preliminary testing shows that this is effective at detecting types of animals and their specific breeds when part of the image is not obscured or has been mislabelled on other websites on the internet.

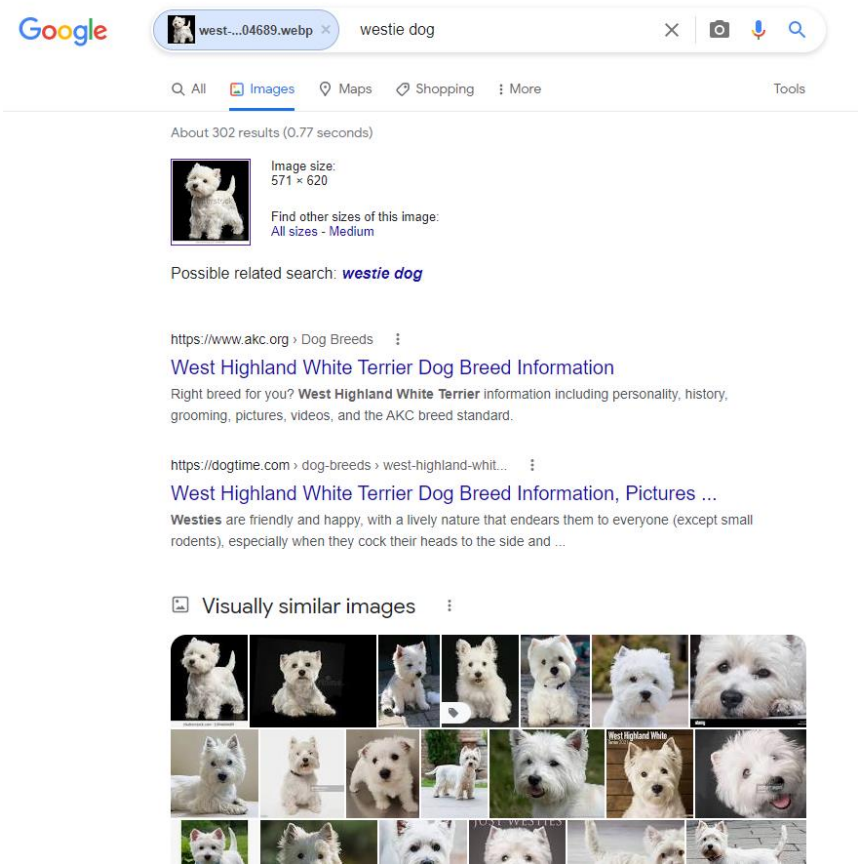

Figure 2: Correctly analysed search results for a photo of a dog (West Highland Terrier).

2.3 – Case Study - Tesla Autopilot (People & Animal Detection):

In September 2014, car manufacturer Tesla, begun installing hardware standard within their vehicles that supported the driver assistance tool that was named “Autopilot” (Evannex, 2020). The Tesla Autopilot programme used a series of on-

board technologies such as ultrasonic sensors, 3D mapping, radar as well as on-board cameras to identify visual cues such as road markings or stationary humans (Ingle & Phute, 2016). In order to perform meaningful actions based upon the visual aspects surrounding the car, Tesla have chosen to use a powerful deep learning model on all of their vehicles onboard computers, which is remotely trained based upon human-classified data from over 1 million vehicles worldwide (Tesla, n.d.).

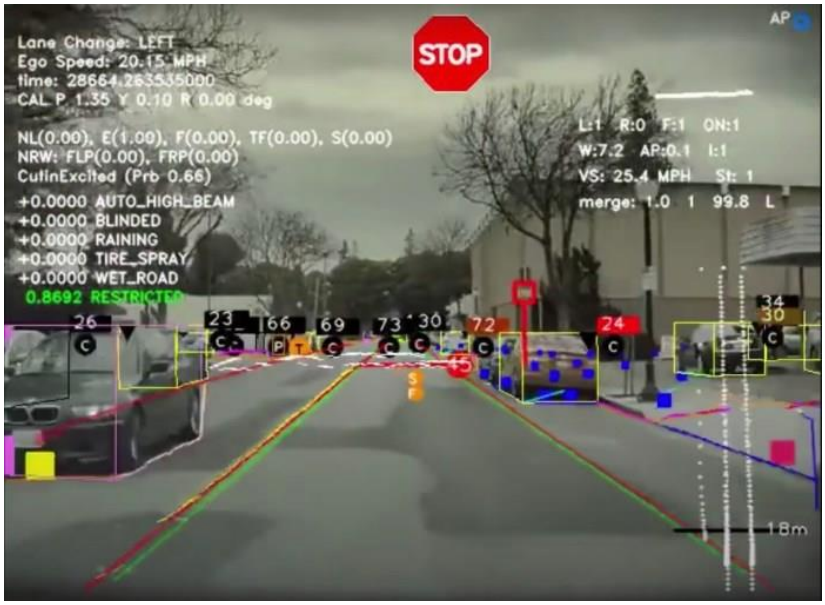

Figure 3: Visualisation of Tesla Autopilot system, showing detected objects such as signs and vehicles (Tesla, n.d.)

A 2016 study by Dikmen & Burns shows that based upon a sample of 121 participants, 90.1% of Tesla owners have actively used the autopilot programme in the past, with 62.4% of those users reporting at least one unexpected action whilst in the autopilot mode. Although this research doesn't elaborate on what those specific failures related to in terms of technology, it can be assumed that a percentage of those could have been down to mis-classification of people or animals located in the path of the vehicle. This shows that despite the fact that the Tesla Deep Learning

models are trained on an incredibly large dataset, the fast paced nature and unpredictability of vehicle driving can sometimes exceed the capabilities of Deep Learning models and hardware at the present moment in time.

3 – Limitations of Deep Learning techniques:

Although Deep Learning is becoming far more prevalent within society, there are still a large number of significant barriers to developing or using such models. The sections below aim to highlight some of the major limitations and how these may be overcome in a practical situation.

3.1 – Large volumes of data required for meaningful results:

In order for a Deep Learning algorithm to be effective, a large amount of pre-labelled training data needs to be provided. This can take a significant amount of man-hours to achieve, during which the algorithm is likely to be ineffective and yield incorrect results.

3.2 – Computationally expensive:

Training deep learning algorithms is a very computationally expensive task, with resource limitations often being the barrier to what can be achieved (Thompson et al., 2020). These limitations have slowly been reduced over recent years with more efficient GPU’s and specialised hardware being released on the market.

3.3 – Shortage of skilled engineers:

At present, there is a far higher demand for skilled Machine Learning Engineers than are currently available in the sector. Job listing site Indeed (2019) states that between 2015 and 2018 within the US there was a 344% growth in job listings, accounting for 179 per million. This is likely to act as a barrier for businesses expanding within the deep learning and image recognition sectors.

3.4 – Inability to distinguish Deep Learning behaviour:

Since 2014, Generative Adversarial Networks (GAN) have become more common, with the intention of one Machine Learning algorithm to be able to create a fictional model that cannot be automatically distinguished by another Machine Learning algorithm, and in some cases, humans. One such example is the online website, ThisPersonDoesNotExist, which uses a GAN to generate photo-realistic images which are indistinguishable from those of an actual human.

Figure 4: A photo generated by a Generative Adverserial Network to simulate a facial photo.

4 – Conclusion:

The research and examples available online demonstrate that Deep Learning techniques in general have massively evolved since their first inception, and have become more commercialised with the readily available access to powerful computing components. Cases such as Tesla have demonstrated that crowdsourced data from millions of vehicles can be trained using manually labelled snapshots to accurately identify other vehicles, animals and people that may be in the path of their

semi-autonomous vehicles. I do, however, believe that there should be larger studies into the ethical and moral applications of where this can be used in society, particularly in cases such as the proposed Social Credit System in China that would use Deep Learning and smart cameras to identify individuals and analyse their behaviour.

During my research into the uses of Deep Learning tools in Image recognition, I have identified a series of gaps in the currently available literature, which include:

- Deep Learning is a constantly evolving topic, therefore information available can become outdated/surpassed fairly quickly with new technological and software based innovations.
- A large amount of the research has been published by the research arms of large companies such as Facebook and Google, with limited research papers and other academic material being available to support their point of view.
- A large amount of the commercially available products for human identification are related to governmental projects, therefore there are no publications due to its commercially sensitive nature. Some examples include the usage of services provided by Clearview AI in the Ukraine-Russia conflict, as well as within the US.

Despite the limitations identified and listed above, I still believe that the Deep Learning aspect of Machine Learning has incredible potential. For example, cases such as Fraud detection could see this as a massive enhancement, with some tools being able to identify visual differences as well as voice/vocabulary differences in a financial setting.

5 - References:

Akrout, I., Feriani, A., Akrout, M. (2019) *Hacking Google reCAPTCHA v3 using Reinforcement Learning*. Available from: https://arxiv.org/pdf/1903.01003.pdf [Accessed 18th April 2022].

Dikemn, M. Burns, C. (2016) 'Autonomous Driving in the Real World: Experiences with Tesla Autopilot and Summon' Automotive'UI 16: *Proceedings of the 8th International Conference on Automotive User Interfaces and Interactive Vehicular Applications*. Michigan, October 2016. New York: Association for Computing Machinery. 225-228.

Evannex. (2020) The Ultimate Tesla Autopilot Guide: How Has It Evolved Over The Years. Available from: https://insideevs.com/news/443886/tesla-autopilot-evolution-history-ultimate-guide/ [Accessed 17th April 2022].

Foote, K. (2022) A Brief History of Deep Learning. Available from: https://www.dataversity.net/brief-history-deep-learning/ [Accessed 17th April 2022].

Fukushima, K. (1980) Neocognitron: A Self-organizing Neural Network Model for a Mechanism of Pattern Recognition Unaffected by Shift in Position. *Biological Cybernetics* 36(4):193-202. Available from: https://www.rctn.org/bruno/public/papers/Fukushima1980.pdf [Accessed 18th April 2022].

Google. (n.d.) reCAPTCHA. Available from: https://www.google.com/recaptcha/about/ [Accessed 18th April 2022].

Indeed. (2019) The Best Jobs in the U.S. in 2019. Available from: https://www.indeed.com/lead/best-jobs-2019 [Accessed 18th April 2022].

Ingle, S., Phute, M. (2016) Tesla Autopilot : Semi Autonomous Driving, an Uptick for Future Autonomy. *International Research Journal of Engineering and Technology* 3(9): 369-372. Available from: https://www.academia.edu/download/54330579/IRJET-V3I969.pdf [Accessed 17th April 2022].

Liang, F., Das, V., Kostyuk, N., M. Hussain, M. (2018) Constructing a Data-Driven Society: China's Social Credit System as a State Surveillance Infrastructure. *Policy & Internet* 10(4):415-453. DOI: https://doi.org/10.1002/poi3.183

Lopez, T. (2014) Spam-Bots, Beware! Google Beefs Up CAPTCHA. Available from: https://slate.com/technology/2014/12/new-no-captcha-recaptcha-from-google-is-much-easier-for-humans.html [Accessed 17th April 2022].

O'Malley, J. (2018) Captcha if you can: how you've been training AI for years without realising it. Available from: https://www.techradar.com/uk/news/captcha-if-you-can-how-youve-been-training-ai-for-years-without-realising-it [Accessed 18th April 2022].

St. George, B., Gillis, A. (n.d.) A guide to artificial intelligence in the enterprise. Available from: https://www.techtarget.com/searchenterpriseai/definition/Turing-test [Accessed 17th April 2022].

Tesla (n.d.) Artificial Intelligence & Autopilot. Available from: https://www.tesla.com/en_GB/AI [Accessed 17th April 2022].

Thompson, N., Greenewald, K., Lee, K., Manso, G. (2020) The Computational Limits of Deep Learning. Available from: https://arxiv.org/pdf/2007.05558.pdf

von Ahn, L., Blum, M., J. Hopper, N., Langford, J. (2003) 'CAPTCHA: Using Hard AI Problems for Security' *International conference on the theory and applications of cryptographic techniques*. Berlin, May 2003. Heidelberg: Springer. 294-311.

Wang, H., Raj, B. (2017) *On the Origin of Deep Learning*. Available from: https://arxiv.org/pdf/1702.07800.pdf [Accessed 18th April 2022].