Fahd M. Saleem

Professor Mahmood

IT-104-214 (Fall 2018)

27 September 2018

Deep learning / Deep fakes Research

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://oai.gmu.edu/mason-honor-code/ and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site."

Envision humanity in disbelief as reality becomes indistinguishable by the human eye, as what's false is soon believed true. Leading to a future with false Innovation ultimately contributing to rising automation being superbly superior. This fate is our current reality as described in countless newspapers, reports, magazines, interviews, and even blogs. Throughout history, industrialization & innovation is what lead to societal growth, an increase which generally holds a positive connotation is inevitably leading to reality's demise through deep fakes. To adequately understand deep fakes, we must first understand deep learning, in which artificial intelligence is exposed to information to evaluate. We commonly see the process of deep learning in many fun and interactive social media apps such as Snap Chat, which allows for face swapping, and the application of elaborate yet realistic filters. However, this process can lead to deep fakes, where AI knowledge is used to impose a person's face onto another person with distinctly identical results usually for malicious intent. Throughout recent years this technology has been used for misinformation & mass manipulation leading to various legal, ethical & security concerns.

The roots of deep fakes technology rely similarly on any other, according to "Phil's Stock World: Detecting 'deepfake' videos in the blink of an eye" the algorithm of deep fakes is similar to Googles translate service. Essentially AI uses machine learning to analyze hundreds to thousands of images of a person usually a celebrity. The images are synthesized onto another person's face down to the various analogous movements & angles making it appear as the source is the target person (Stock, 2018). In essence, the more source information provided to the AI, the better the quality of the superimposed digital impression. Assumedly it can lead to many cons associated with the technology but stores excellent capabilities as well. Deep learning in addition to computer-generated imagery or more commonly known as CGI, offers a preeminent potential for film & television. London's "The Economist" magazine by the title of "What if AI made actors immortal?: Performance anxiety" offers excellent insight into the potential uses for deep learning technology as a whole. Deep learning technology although already advance has the potential to carry on actors lives through film even after their death. Imagine an actor able to star in countless films at once. The magazine then goes on to say that different ages of the actors could be portrayed in various films. The real-world application of deep learning offers the legacy of beloved actors to live on for decades to come.

However deep learning poses various social as well as ethical concerns to individuals of many backgrounds from celebrities, to political figures, and even the general public. This was notably prevalent during the 2018 campaign season where deep fakes started to take over online, creating the genre of "fake news" which many now associate with deep fakes. During campaign seasons, political figures are especially at risk by deep fakes. Along with the social concern, it compromises the security of political figures, using their own words against them making it nearly impossible to differentiate between the deep fakes & legitimate video. The use of deep fakes is mainly used to discredit, which is predominately done through making it seem as the specific individual has said or done something they normally wouldn't consider doing inevitably leading to public backlash as the evidence was nearly impossible to distinguish as real or fake without the use of deep learning itself. "Phil's Stock World: Detecting 'deepfake' videos in the blink of an eye" article also provides the flaws in the algorithm of deep fakes. Despite its immense realism, deep fakes cannot perfect the replication of a human blink due. This can only be noticed by deep learning machines conditioned to look out for discrepancies within blink intervals which are a lot less frequent in deep fakes (Stock,2018).

Furthermore, many celebrities are at risk due to the harsh nature of the origins of deep fakes raising many ethical concerns. The eminence of deep fakes was first made apparent through pornographic content. Initially, the first user to post content regarding deep fakes was a Reddit user who goes by the online alias of “Deepfakes,” ultimately the username gave the name to this genre of realistically misleading content (Weekend Edition Saturday, 2018). Without permission faces of celebrities were digitally stitched onto adult films thus creating an entirely new category within the industry (The Economist, 2018). Celebrities, unlike the average consumer, have thousands of images of themselves online making them more prone to be a subject of deep fake videos. As a result, celebrities are astonished by the fact they never performed in such films, and this raises legal concerns allowing them to possibly sue for misappropriation of their image (Weekend Edition Saturday, 2018). Although celebrities are most vulnerable, that doesn’t mean any one individual is safe. In fact, in an interview done by “Weekend Edition Saturday states that its hypothetically possible for any individual to be a victim of deep fakes, assuming enough images or videos are found it’s entirely possible. As a result, the typical person could possibly be seen as doing something they dint or even be framed for a crime they did not commit. Questions of such are what’s soon to be true, as indicated by the various hints that deep fakes are continually advancing. Thus, making the intriguing technology of deep fakes even more accessible to produce among online vigilantes.

In addition, within the research, it was prevalent that due to the constant advancements, the accessibility to produce such material is relatively easy. Without the need for a powerful PC, even common devices are capable of producing video modifications in ideal standards varying in quality (The Economist, 2018). As a result, even free to use programs allow for video modifications. The free available programs, as well as tools, eventually could lead to the increased rise in deep fakes. Comparatively prices for professional video editing software with advanced AI capabilities will soon become cheaper as time progresses. This overall contributes to the social problems caused by the technology of deep fakes. These social problems, however, are not just caused by the manipulated video, but by audio as well immensely increasing the realistic appeal of the deep fakes. In conjunction with face swapped videos and manipulated audio, online communities & the public are oblivious to the fact that some of these videos are considerably fake. This entire issue not only further contributes to the social problems concerned with the issue of deep fakes but creates a sense of misinformation among the general public.

Speaking the general public within the congressional publication “House Oversight and Government Reform Subcommittee on Information Technology Hearing” A Testimony by Jack Clark, Director, of OpenAI conveys that reforms regarding ethical formalities are needed when working with AI to ensure safety among information. He goes to provide the example that deep fakes have caused significant upheaval in recent times. Clark explains “… at MIT of President Trump's face being mapped onto the face of President Obama n2, and vice versa” (Clark, 2018). The example demonstration shown in the quote provided not only shows the negative aspect it can have on politics but that indeed anyone is at risk even the presidents. Despite this being a huge concern, Clark evokes a sense of hope through specific reforms still being able to be made. Through the creation of ethical norms, AI can be regulated, including the creation of deep fakes. Ultimately this ensures the lack of fake news to come & safety among the use of AI, also it will immensely minimize the potential of conflict & harm. In order to make this reform work as designated, it must be proceeded by governmental reforms to complete this issue.

In conclusion, its predominately shown that deep fakes have been used for malicious intent, despite the positives it so actively can be manipulated for unethical purposes. Its commonly shown to be used for harm to an individual, usually a political figure or celebrity from Donald Trump to Obama. Due to the harmful misuse, deep fakes are generally associated with a negative connotation. Deep fakes throughout recent years have led to mass misinformation and have led everyone to continually question the validity of the source no matter how realistic it may seem. Throughout the examination of the research, It can be concluded that in its recent upcoming it still poses a threat and has not been effectively handled despite any reform actions taking place. If no further action is taken the utilization of social media might end abruptly as videos, photos become impossible to distinguish between authentic or false. According to “What if AI made actors immortal?: Performance anxiety” Its highly possible, for example even Gal Gadot a famous Israeli actor was depicted in a deep fake adult film which she had no connection with, but through the extensive images of her online, AI was primarily able to analyze all her facial movements and positions to compile a realistic-looking video accurately. As stated before the more images the AI has to interpret the better the output quality of the final deep fake video. Finally, Consumers should take away and be made aware of the direct consequences of having vulnerable images, videos, & audio online.

References & Bibliography:

1) HOW ARTIFICIAL INTELLIGENCE CAN DETECT - AND CREATE - FAKE NEWS. (2018, Aug 04). US Fed News Service, Including US State News Retrieved September 10, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/2082561464?accountid=14541

This newspaper covers in through detail how AI through deep fakes can assist in the creation of fake news. It also goes to elaborate on how to differentiate between the information of deep fake videos to conclude its authenticity. The source is reliable due to it being published by the United States Federal news service, going to show further how huge the issue is on a country-wide scale. In summary, it contributes to my research by exemplifying the adverse effect of deep fakes. Also, through the negative effects such as fake news, and how it can be combated in attempts to resolve the bigger issue at hand of deep fakes.

2)Foer, F. (2018, 05). REALITY'S END. The Atlantic Monthly, 321, 15-18. Retrieved September 10, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/2080197716?accountid=14541

This source is a reputable magazine publication from well-known author Franklin Foer. Receiving his education from the prestigious Columbia University, Foer currently is residing as a staff writer for The Atlantic. Throughout his magazine publication, the central idea of how advances in deep learning are making deep fakes indistinguishable. Thus, contributing to reality’s ultimate demise from the abundance of fake news & deep fakes. Much of the publication conveys how manipulated video results in conflict between what’s authentic or not and provides examples to back up the claim showing its reliability as a source.

3)House oversight and government reform subcommittee on information technology hearing. (2018). (). Washington: Federal Information & News Dispatch, Inc. Retrieved from Research Library Retrieved September 10, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/2026918302?accountid=14541

The reviewed report focuses directly on the many beneficial uses of AI. It also regards back to the issue of deep fakes showing its impact on society specifically in the political field. It also provides a counter-argument showing that it offers many benefits. For example, by stating changes that could be applied for the AI deep learning to be reliable yet safe. Much of the article provides textual features to enhance the credibility of the source through textual elements. Logos, for example, is one textual feature prevalent through much of the report, its use ultimately betters the reliability of the source as a whole.

4)What if AI made actors immortal? (2018, Jul 05). The Economist (Online), Retrieved September 10, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/2064401228?accountid=14541

Uniquely this magazine by London's well known "The Economist," exemplifies the potential benefits of deep fakes in the film entertainment industry. In summary, it shows how deep fakes can be used to make the work of actors live on, showing its positive use. The opposing negatives it shows through stating the cons of the technology helps build the credibility of the source. This is because acknowledging both points of views shows the cause is not biased and therefore reliable to both audiences. It also provides intricate use of factual appeal to build on the ethos or credibility of the magazine publication.

5)Phil's stock world: Detecting 'deepfake' videos in the blink of an eye (2018). . Chatham: Newstex. Retrieved September 10, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/2095624709?accountid=14541

This weblog provides a captivating method to detect deep fakes. It briefly introduces the topic of deep fakes giving a straightforward stance on the issue. Throughout much of the blog, it talks about how machines can be used to detect the issue. It extensively shows the vulnerabilities deep fakes have interpreting blinks and as a result do not blink as often as real individuals will. Through these finding, AI machines can be used against Deep fakes in attempts to solve the issue. The blog overall relies much on the ethos of the writer, but also occasionally goes to use facts & evidence to further his claim.

6)In an era of fake news, advancing face-swap apps blur more lines (2018). . Washington, D.C.: NPR. Retrieved September 10, 2018 from https://search-proquest-com.mutex.gmu.edu/docview/1993644892?accountid=14541

This reasonably short interview consists of the reputable editor Samantha Cole being interviewed on the issue of deep fakes. She goes on to say how it affects the regular citizen and how they are put at risk. Risk of being put into an in-depth deep fake video, through the use of social media which leaves everyday people vulnerable. Cole overall offers excellent brief insight into the dark world of deep fakes. She also provides an alternative approach to tackle the issue. Cole recommends an extreme solution as to not putting pictures on social media as well as a more probable solution to reform laws protecting individuals. Her knowledgeable responses made in the interview together show a sense of credibility of the source, further making her argument more compelling.