Artificial Intelligence in Deepfake Technologies Based on Supply Chain Strategy

[1]Khalid Alattas, [2]Magdy Bayoumi
[1]College of Computer Science and Engineering, University of Jeddah, Jeddah, Saudi Arabia, kaalattas@uj.edu.sa.
[2]Department of Electrical and Computer Engineering, University of Louisiana at Lafayette, Lafayette, LA 70503, USA
magdy.bayoumi@louisiana.edu.

Abstract It is highly impossible to differentiate between verified and fake media news and updates with modern emerging technology. The creation of deeper fake photos and videos which use artificial intelligence (AI), that shows someone saying and doing things that never did in reality, is one of the recent innovations that contribute to it. Concentrated depths will easily hit millions of citizens and affect adversely our culture, along with their accessibility and pace of social networking. This paper analyses a variety of widely accessible internet news stories, while literature on this subject is scarce, in order to explore the depths, and who creates them, how deep technological advantages and risks are, which example of deepfake occur and how the depths are to be gauged. We will use qualitative research methodology to gather the available information and based on the findings, in the end, we will conclude the discussions along with recommendations.

Keywords: *Deepfake, intelligent Technology, supply chain management, blockchain*

1. Introduction

Deepfakes are fake videos or audio recordings that sound as if they were the real thing. For decades, such capabilities have existed. However, it used to take whole studios with experts a year to create these effects. Deep technology new computer graphics or machine learning systems can now synthesize images and videos much faster. Deepfakes mean manipulated videos or other digital representations produced by advanced artificial intelligence, which produce real images and sounds. Such videos "get more and more sophisticated and accessible," writes John Villasenor, a non-resident senior governance fellow in the Washington-based Center for Technology Innovation, the Brookings Institution [1-3]. "Deepfakes raises a series of challenging political, technical and legal issues." Indeed, anyone with a computer and internet access can produce in-depth content that can be used for fun and other purposes technically.

Altough manipulations of visual and auditory media are as old as media themselves, the recent entrance of deepfakes has marked a turning point in the creation of fake content. Powered by the latest technological advances in artificial intelligence and machine learning, deepfakes offer automated procedures to create fake content that is harder and harder for human observers to detect. Thanks to digital technologies, today it is much easier to establish the authenticity of a work. There are databases where you can check authors' signatures, and millions of images that can be viewed with a few clicks. Selling a fake is more difficult.

International Journal of Supply Chain Management
IJSCM, ISSN: 2050-7399 (Online), 2051-3771 (Print)

Deepfake technology can seamlessly stitch anybody in the world into a video or photo in which they have never participated [4, 5]. The video of Hader is a profoundly skilled device, a technology invented in 2014 by Ian Goodfellow, an Apple Ph.D. student. The deepest technology is based on generative networks of opponents (GANs). GANs allow algorithms to move beyond data classification to images generation or creation. This occurs when two GANs try to fool one another into thinking that an image is "real." A experienced GAN can create a video clip of a person using just one image. Today everyone can upload deep fake software in their spare time and create convincing fake videos [6]. So far, deepfakes are limited to hobbyists who put their faces on the bodies of porn stars and make politicians speak funny stuff.

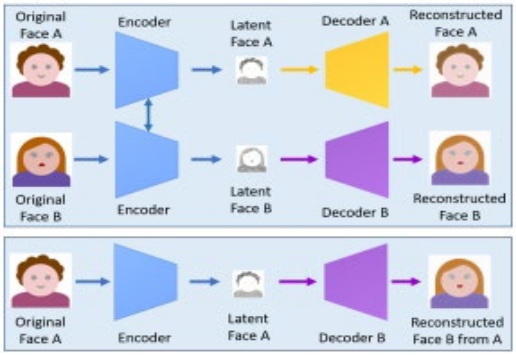

Figure 1: illustrates the process of deepfaking:

2. Literature Review

False news has been a threat to human society, public discourse, and democracy in recent years. Fake news relates to fictional content in the style of news intended to trick the public. False information can quickly spread through social media, affecting millions of users [7]. On YouTube, one of five web users will receive their news, on Facebook alone. This increase of popularity highlights the fact that new technologies are capable to make video manipulation convincing, thus confirming the authenticity of news and media content. Given the ease of gathering and distributing information through social media platforms, the knowledge which has affected informed decision-making, among several other things, becomes more and more difficult [8]. Indeed, we are currently living in a post truth system dominated by a conflict of electronic propaganda and lies, and false information led by malicious actors engaged in falsified public opinion information campaigns.

Deepfake is a technique for manipulation or tampering which enables a user to interact with any other actor or person, often an actor, actress or other celebration. The look and sound of fake videos, audio or pictures is made authentic [9]. The system creates a model of someone who speaks or does anything using large datasets with

records, videos, or photographs. The use of hundreds or thousands of photos of the target is used as a dataset to manipulate this. Image and video manipulation technology, such as deepfake, depends on artificial intelligence techniques, a field that aims to understand human thought and behavior processes [10-12]. Machine learning is specifically used to help a system learn from available data. It is an artificial intelligence part. Deepfake is popular for two reasons: firstly, due to the ability to produce photorealistic data results, in particular, photos, but also videos given sufficient computer time, and secondly, because the layman can easily access and use this technique because it is available in large numbers. Reddit released an application called FakeApp that leads users through the fundamental steps of the deep algorithm [13]. Through this application a deep image or video can even be created, as mentioned by [14], with a limited knowledge of machine learning and programming. Deepfakes are usually performed to a person to take revenge, upload a pornographic video of a famous person, or make a person to chuck by showing a changed or manipulated video or photograph. In addition, as Stover mentions, deepfakes are also used to create fake political videos to create false news [15]. In short, the deep fake in today's society has become a major problem.

The term "deep learning" and "fake" is related to a type of artificial understanding. Deepfakes are deep learning videos that are just proven false [16]. Deep learning is a "AI subset" that refers to algorithms that can learn and decide for themselves. However, the risk is that the technique can be used to convince people that something else is true. Deepfakes is a product for AI applications mixing, combining, deleting, and overlaying photos and video clips to construct composite, real videos [17]. For example, Deep Technology may, without the permission of the person with his or her own image or voice, create a humorous pornographic or political video for a person who says something. The fundamental factor that changes the game is its size, scale, and sophistication because almost all can generate fake, nearly inconsistent videos from authentic media with a computer [18]. While early instances of the deep-faced are orders, actresses, comics and animators whose faces will be transformed into porn images, deep-fakes will possibly be gradually used to bully porn, intimidate videos, false courtship footage, political sabotage, jihadist messaging, chase, consumer theft and false news.

The difference between true and false media is becoming more complicated with emerging modern technology. One of the most recent innovations that add to this topic is the creation of hyper-realistic videos utilizing artificial intelligence. Deep belief will affect millions of citizens easily and have a detrimental influence on our culture through the reach and pace of social networking. While there are few studies on this subject, this analysis analyses the profound challenges, the benefits, and risks of depressional Technology, Deeper defects and how to cope with deeper defects in many news articles that are accessible publicly online. While the findings indicate that deepfakes pose a major challenge to society, the legislative and regulatory structures, organizational strategies and voluntary initiatives, education and education, the implementation of in-depth analysis, verification of information and deep-seated prevention technologies are addressable [19]. The survey presents a comprehensive analysis of essential trends and gives entrepreneurs the chance to tackle false news and media falsification on Internet protection and AI sector.

3. Methodology

This research applies to news stories on deepfakes and the emergent empirical literature. An order to perform empirical research of how the media discussed profound issues a total of 20 papers from different publications were gathered. Deepfake, written in English and released in 2018-2019, were the subject of all posts [20]. They were identified using "deep" keywords, "deep false" and the corresponding plural forms from Google News. Upon locating an post, a similar quest has been conducted using the search option for the news web site to locate further articles about the same media outlet. From general daily news, to industry or technological news based on the chosen news media. This dataset contains 2 to 16 news stories for any news organization on the deepfakes. The papers have been coded with a short identifier for quotes purposes. Then, they have been evaluated by content review to deep faults and to figure out what the advantages and threats of deep fabric technology are. The news stories, their publishers, news organizations and dates of publishing are present; due to room constraints, the item titles are shortened.

4. Results

Deepfakes represent a serious issue and threat to society, the political system, and our business because:

- They put pressure on journalists who fight to filter real news,
- They are threatened by the dissemination of propaganda and election interference.
- They are hampered by the public's confidence in government information; and
- They raise cyber security problems for people and organizations.

The journalistic business would most certainly have to confront a major problem of customer confidence because of fundamental difficulties. Deepfakes pose a greater challenge than 'traditional' false news, since it is more challenging to see, and people prefer to assume that the fake is genuine [11]. The technology makes it possible to create obviously legitimate news videos which jeopardize the credibility of journalism and the media. Winning the battle to get video evidence from an event would also provide a news media organization with strategic benefit, although risk improves if it is a false one. In 2019, Reuters noticed 30 fake videos on the case, mostly old videos from other events posted with new subtitles, as a result of the conflict between India and Pakistan [17]. Distributed video images, such as a true demonstration march or a violent skirmish, is a growing concern and gradually gets deepened. It is implied that it happens anywhere else. Reuters discovered an eyewitness video on school killings in the town of Christchurch, New Zealand, which appeared to demonstrate when the police fired a gunman. They soon figured out to be another crime in the United States, though, and the perpetrator was not assassinated in the Christchurch shooting.

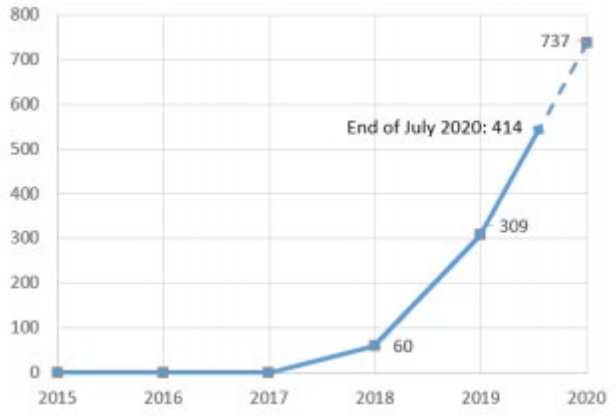

Figure 2: The graph above shows the number of published papers on deepfakes taken by Google

The curve shows a significant increase in the number of papers indicating the importance of the topic and its application in society. White surfaces are the concern of the intelligence services by promoting liberal propaganda and distorting campaigns in the name of domestic security. U.S. security officials have cautioned regularly of the danger of foreign interference in American affairs, especially before the elections. In today's wars of misinformation, inserting language in someone's mouth on a viral video is a strong tool since such modifying Videos will quickly skew the perception of citizens. A foreign intelligence service may create a deep-seated video of a leader who uses a racist image or takes a coat of arms, a political nominee who confesses to involvement in the crime, or informs a government of a possible conflict, an official in a seemingly compromises circumstance or who supports a hidden conspiracy plot, or soldiers performing war crimes such as murdering civilians. While such fake videos may lead to civil turmoil, upheavals and votes, some nation states may even choose for impossible foreign policy, contributing to world wars. eepfakes are likely to mess with digital literacy and citizens' confidence in knowledge supplied by government, since false videos display politicians who claim something that never happened call people in question [7]. Indeed, the spam created by AI and fake notifications, which build on bigoted text, fake videos, and a multitude of complot theories, is now becoming increasingly affected. However, deep-faced individuals may not be most destructive in their own eyes but more how frequent interaction with disinformation causes people to believe too much content, even footage, is actually unconfident, culminating in a phenomenon called "information apocalypse" or "reality apathy."

Another challenge imposed by deepfakes is cyber-security concerns. The business sector has also demonstrated an interest in safeguarding itself from viral manipulation, for example by showing a leading boss who talks of derogatory or misogynistic slurs, by reporting a falsified acquisition, creating misleading statements of financial loss or disappointment, or presenting them as a crime. In comparison, in-depth product releases for brand sabotage, extortion, or shame management could be used [5]. Deep technology often allows an employee to, for example, order an employee to make an immediate cash transfer or to include classified details in real-time digital personalization.

Table 1: The summary of the well-known and notable deepfake tools being used

Tools	Links	Key Features
Faceswap	https://github.com/deepfakes/faceswap	- Using two encoder-decoder pairs. - Parameters of the encoder are shared.
Faceswap-GAN	https://github.com/shaoanlu/faceswap-GAN	Adversarial loss and perceptual loss (VGGface) are added to an auto-encoder architecture.
Few-Shot Face Translation GAN	https://github.com/shaoanlu/fewshot-face-translation-GAN	- Use a pre-trained face recognition model to extract latent embeddings for GAN processing. - Incorporate semantic priors obtained by modules from FUNIT and SPADE
DeepFaceLab	https://github.com/iperov/DeepFaceLab	- Expand from the Faceswap method with new models, e.g. H64, H128, LIAEF128, SAE - Support multiple face extraction modes, e.g. S3FD, MTCNN, dlib, or manual
DFaker	https://github.com/dfaker/df	- DSSIM loss function is used to reconstruct face. - Implemented based on Keras library.
DeepFake_tf	https://github.com/StromWine/DeepFake_tf	Similar to DFaker but implemented based on tensorflow.
Deepfakes web β	https://deepfakesweb.com/	Commercial website for face swapping using deep learning algorithms.

In addition, deep technology can establish a fake persona, and turn an adult's face into a kid's or younger face in live-stream footage, creating questions regarding the implementation of child predators' technology. Finally, deepfakes can help distribute harmful scripts. Researchers have recently learned that a deepfakes website used machines on its guests to mine cryptocurrencies. This suggests that deep hobbyists will become objects of 'crypto jacking,' since they undoubtedly have potent machines.

5. Recommendation and Future Research

Ironically, the only solution for now could be artificial intelligence. Fake videos are detected utilizing artificial intelligence, but many of the current recognition systems are seriously weak: they function well on popular individuals because they can practice publicly accessible pictures over hours [18]. The results suggest that while deepfakes are a significant threat to our society, political system and business, they can be combatted via legislation and regulation, corporate policies and voluntary action, education and training, as well as the development of technology for deepfake detection, content authentication, and deepfake prevention. Technology companies are already focused on identification technologies to identify fakes once they emerge. The root of the media is another tactic. Digital watermarks are not foolproof, however an

online blockchain blocking scheme could archive photographs, photos and audio in a manner that would guarantee that they would still verify their origin and any manipulation.

6. Conclusion

The research studied and assessed many recent media publications on profound faults to better appreciate the deep faults, the advantages and risks of deep faults technologies, explanations of and how to tackle existing profound faults [11]. The study showed that deepfakes are digitally manipulated hyper realistic images that show characters who say and do stuff that never exist. Deepfakes are built with AI, namely the Generative Adversarial Networks (GANs) which pit discriminatory and generative algorithms against each other to boost their output with each repeat. These fakes are also highly viral and appear to propagate rapidly through social networking sites, making them a successful tool for misinformation. In so doing, the study found that deepfakes are hyper-realistic videos digitally manipulated to depict people saying and doing things that never happened. The outcomes of this analysis make many additions to the emerging array of deep-fake academic literature. According to our research, profound challenges are a big danger to culture, the democratic structure and industries because they compel media to root out false news in real life, endanger national security by distributing election misinformation, impair citizens' trust in government knowledge and create cyber safety concerns for individuals and organizations. In this respect, the research primarily confirms the conclusions of previous studies and, concurrently, describes these risks by using actual and future applications of deep defects.

References

[1] Antinori, A., 2019, October. Terrorism and deepfake: from hybrid warfare to posttruth warfare in a hybrid world. In ECIAIR 2019 European Conference on the Impact of Artificial Intelligence and Robotics (p. 23). Academic Conferences and publishing limited.

[2] Bazarkina, D. and Pashentsev, E., 2019. Artificial Intelligence and New Threats to International Psychological Security. Artificial Intelligence.

[3] Caporusso, N., 2020, July. Deepfakes for the Good: A Beneficial Application of Contentious Artificial Intelligence Technology. In International Conference on Applied Human Factors and Ergonomics (pp. 235-241). Springer, Cham.

[4] Chesney, R. and Citron, D., 2019. Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Aff., 98, p.147.

[5] Fletcher, J., 2018. Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance. Theatre Journal, 70(4), pp.455-471.

[6] Floridi, L., 2018. Artificial intelligence, deepfakes and a future of ectypes. Philosophy & Technology, 31(3), pp.317-321.

[7] Hasan, H.R. and Salah, K., 2019. Combating deepfake videos using blockchain and smart contracts. Ieee Access, 7, pp.41596-41606.

[8] Jones, V.A., 2020. Artificial Intelligence Enabled Deepfake Technology: The Emergence of a New Threat (Doctoral dissertation, Utica College).

[9] Karnouskos, S., 2020. Artificial Intelligence in Digital Media: The Era of Deepfakes. IEEE Transactions on Technology and Society, 1(3), pp.138-147.

[10] Kaur, S., Kumar, P. and Kumaraguru, P., 2020. Deepfakes: temporal sequential analysis to detect face-swapped video clips using convolutional long short-term memory. Journal of Electronic Imaging, 29(3), p.033013.

[11] Kietzmann, J., Lee, L.W., McCarthy, I.P. and Kietzmann, T.C., 2020. Deepfakes: Trick or treat?. Business Horizons, 63(2), pp.135-146.

[12] Kirchengast, T., 2020. Deepfakes and image manipulation: criminalisation and control. Information & Communications Technology Law, 29(3), pp.308-323.

[13] Kwok, A.O., and Koh, S.G., 2020. Deepfake: a social construction of technology perspective. Current Issues in Tourism, pp.1-5.

[14] Maras, M.H. and Alexandrou, A., 2019. Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. The International Journal of Evidence & Proof, 23(3), pp.255-262.

[15] Nazar, S. and Bustam, M.R., 2020, July. Artificial Intelligence and New Level of Fake News. In IOP Conference Series: Materials Science and Engineering (Vol. 879, No. 1, p. 012006). IOP Publishing.

[16] Pantserev, K.A., 2020. The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability. In Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity (pp. 37-55). Springer, Cham.

[17] Paris, B. and Donovan, J., 2019. Deepfakes and Cheap Fakes. United States of America: Data & Society.

[18] Siau, K. and Wang, W., 2020. Artificial Intelligence (AI) Ethics: Ethics of AI and Ethical AI. Journal of Database Management (JDM), 31(2), pp.74-87.

[19] Watney, M.M., 2020, June. Artificial Intelligence and its' Legal Risk to Cybersecurity. In European Conference on Cyber Warfare and Security (pp. 398-405). Academic Conferences International Limited.

[20] Westerlund, M., 2019. The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11).