Analysis of Deep-Fake Technology Impacting Digital World Credibility: A Comprehensive Literature Review

Mohd Akbar
Dept. Computer Science & Engg.
Integral University, Lucknow, India
Email: Akbar [AT] iul.ac.in

Mohd Suaib
Dept. Computer Science & Engg.
Integral University, Lucknow, India
Email: Suaib [AT] iul.ac.in

Mohd Shahid Hussain
Information Technology Department
University of Technology and Applied Sciences-CAS Ibri, Oman
Email: shahid.ibr [AT] cas.edu.om

Abstract— **Deep-Fake Technique is a new scientific method that uses Artificial-Intelligince to make fake videos with an affect of facial expressions and coordinated movement of lips. This technology is frequently employed in a variety of contexts with various goals. Deep-Fake technology is being used to generate an extremely realistic fake video that can be widely distributed to promote false information or fake news about any celebrity or leader that was not created by them. Because of the widespread use of social media, these fraudulent videos can garner billions of views in under an hour and have a significant impact on our culture. Deep-Fakes are a threat to our celebrities, democracy, religious views, and commerce, according to the findings, but they can be managed through rules and regulations, strong company policy, and general internet user awareness and education. We need to devise a process for examining such video and distinguishing between actual and fraudulent footage.**

Keywords- Deep learning; Encoder; Decoder Generative adversarial networks (GANs). Question Generation, NLP, Intelligent Tutoring System (ITS.

I. INTRODUCTION

Two terms sum up deep fake video technology. 'Deep' means 'deep' and 'false' means 'not genuine.' To put it another way, the film was created by analyzing a relatively similar type of video of a person utilizing deep learning technology for self-leaning. [1, 2]. I was able to produce my own fictional footage of that people after examining these data sets. It is often used by ordinary people to replace their visage with that of a movie star or clip[3]. In conjunction with deep learning Artificial intelligence and machine learning, a growing proportion of Smartphone with high-quality camcorders and easy access to an enormous number of mobile apps for generating and sharing movies and digital photos has promoted a new phenomena of faking videos known as Deep_fake [4]. We discovered in a study that the graph of photo-shoped faked and morphed video climbs dramatically in various social sites such as in digital marking, political marketing, etc which helps the society in a very positive manner and helps them in very different approaches using artificial intelligence. According to the study done by sensity.ai published shows that the content of Deep_fake media is just double every six months as shown in figure 1 till 2020[5].

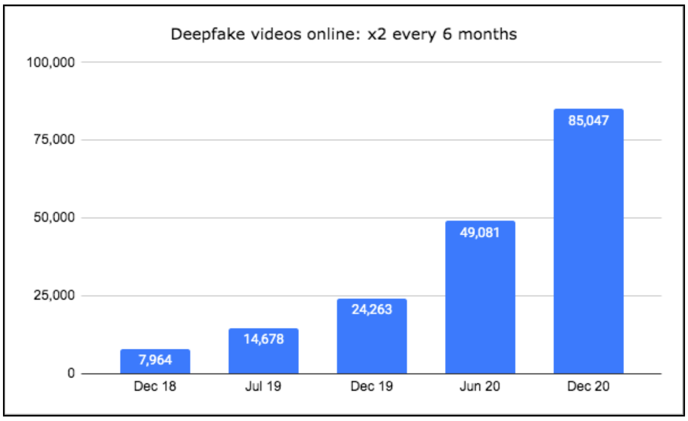
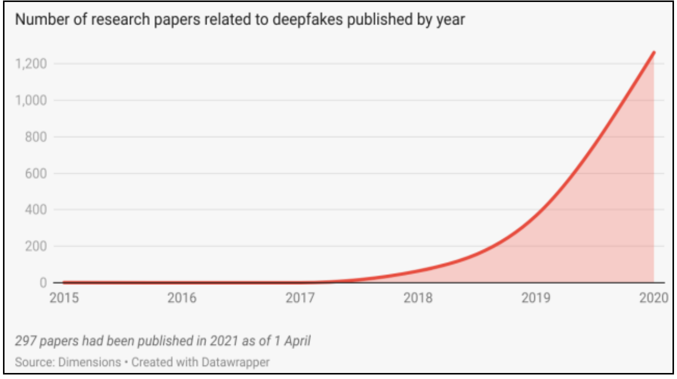


Figure 1: Frequency of deep-fake videos (online)

Another report produced by the World Economic Forum [6.] on the publication of research papers on Deep fake as shown below in figure-2.



297 papers had been published in 2021 as of 1 April

Source: Dimensions • Created with Datawrapper

Figure 2 Rate of research publication on Deep-fake videos

This report by the World Economic Forum [6.] on the publication of research papers on Deep_fake, demonstrates that it's a very hot topic not only in the internet world but also in the research world. These studies demonstrate how quickly technology is being adopted by society in numerous industries.

II. Generation of Deep_fake Matters

There are numerous programmes that can be used to create a Deep fake visual incident without requiring much of domain knowledge. As a result, Deep fake poses a significant threat to applications like Face App and Deep Face Lab. Deep neural networks are used to build Deep fake in these types of applications. Deep fake video can be made in two ways. The first step is to overlay the altered audio on top of the video. The second method is to superimpose a benign image on top of a legitimate image[3][7]. To make a deep_fake, followings are mere few steps to follow.

A. Feature Extraction of Video Frame

Deep fake, as mostly known, is predicated and based on Artificial Intelligent governed approach the deep learning technique and it requires a vast quantity of data known as training data-set. We needed a lot of pictures of the person to make the Deep fake film. All of the frames that face are extracted and aligned. The neural network is used to do the alignment, which is a highly crucial and critical phase. Face swapping is done with an implied constraint of having all faces exactly the same size & dimensions. At the end of the training the machine would be able to convert the face of an input person , say person-1 to face of an another targeted person-2.

B. Training Data Set

The training process, referring to the mechanism that permits a neural-network-system to transform one face into another, incorporates machine learning (ML) technology to all these set and done. It is a lengthy & cumbersome procedure that might take from certain minutes to many hours to perform all these transformation based on training data set and machine learning algorithm.

C. Development of Deep Fake Matter

The final stage in creating Deep fake is to complete the training. It starts with an image, audio or a video, then removes all casings and adjusts all appearances. After that, everyone is switched over to the prepared neurological system. The final step is to solidify the modification over the face in to the next casing once more. It appears to be really basic and straightforward to apply. It is here that the majority of Deep Fake applications fail. Auto encoders are utilised to generate a Deep fake [2-3], as previously stated. The Deep fake matters are created using generative networks and encoder decoder neural-networks, and often referred as Generative Adversarial Networks [9-12].

The basic goal is to accomplish face transposition or replacement. According to the video's purpose, one person's visage is projected onto the face of another. Encoder and decoder are the two components. the encoder-decoder (ED Network) network that will aid in feature extraction by encoding data from the input tier until the the total no. of parameters/variables are reduced. The decoder network, as shown in figure 5, eliminates variables to produce a new output that is remarkably similar to the original[15]. The Deep fake film was created by combining the aligned faces of two individuals, namely, person- and person-2.

Then, using the data provided for face A, encoder EA reconstructs A's face. Similarly to the face of Deep fake, we share the weight of these two encoders EA and EB. However, the decoder is separate. As soon as the optimization is complete. Any image with the face of A can now be encoded using this encoder, but must be decoded using decoder DB.

The principle of making deep-fake can be described as follows: Upper-Top: the training portions with the shared encoder in yellow; Lower-Bottom: the training parts with the shared encoder in yellow, eg; the part where A's (Person-1) images are decoded using B's(Person-2) decoder.

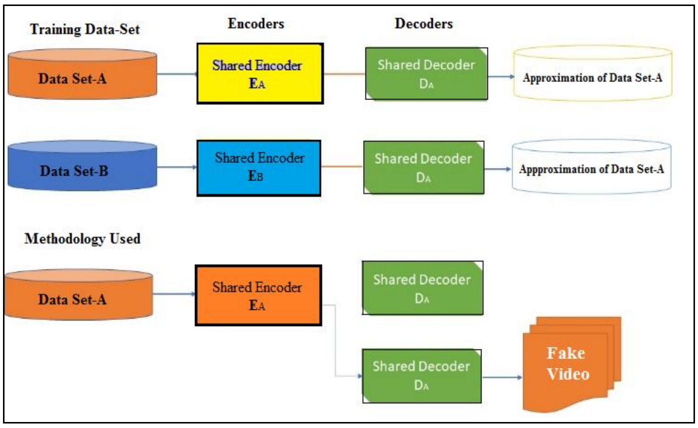


Figure 3: Three Tier Architecture of Deep-fake Creation Process.

D. Tools used in creation of Deep Fake Matter

There are so many tools available in the market that assists people to create deep-fake matters without bothering much of technical know-how.

Table 1.Tools used to create Deep_fake

1	Deep_fake Detection Challenge	http://Deep.fake.detectionchallenge.ai
2	Deep_fake s Web	http://Deep.fake sweb.com
3	Deepware – Deep Fake Detection tool	http://www.deep.ware.ai
4	DF Blue	http://df.blue.com
5	dfaker	http://git.hub.com/dfaker/df
6	Face Crop Jet	http://face.cropjet.com

7	Face Ripper 9000	http://git.hub.com/MotorCityCobra/face_ripper_9000
8	Face Swap Live	http://face.swaplive.com
9	Face Swap Online	http://faces.waponline.com
10	FaceCrop	http://www.luxand.com
11	FaceForensics	http://git.hub.com/ondyari/FaceForensics/
12	Faceit	http://git.hub.com/goberoi/faceit
13	Faceswap	http://faceswap.dev.df
14	Faceswap	http://git.hub.com/dfaker/faceswap
15	Faceware Tech	http://www.face.waretech.com
16	Facial Animation Examples	http://sites.google.com/view/facial-animation/home
17	iClone	http://iclone.reallusion.com
18	iSpeech	http://www.I.speech.org/voice-cloning
19	Lyrebird	http://lyrebird.ai.in
20	MRRMRR	http://mrrmrr.Me.
21	NaturalFront	http://natural.front.com
22	Poser	http://www.poser.software.com.
23	Real-Time Voice Cloning	http://git.hub.com/CorentinJ/Real-Time-Voice-Cloning.
24	Reflect	http://reflect.tech.cs
25	Resemble AI	http://www.resemble.face.ai.

III. Challenges and Threats of Deep Fake

There are numerous examples of Deep fake technology being utilised to threaten civilization in various domains, including political[16-17], socio-economic, and many more. Figure 5 shows that the majority of fake news is tied to politics, while Figure 6 shows that the show clip is more made to avoid fake news. As a result, we may conclude that Deep fake plays a critical part in the development of fake news. The false news information created with deep-fake technology[17] appears to be more authentic and simpler to believe than the video's content. India is a sensitive country.

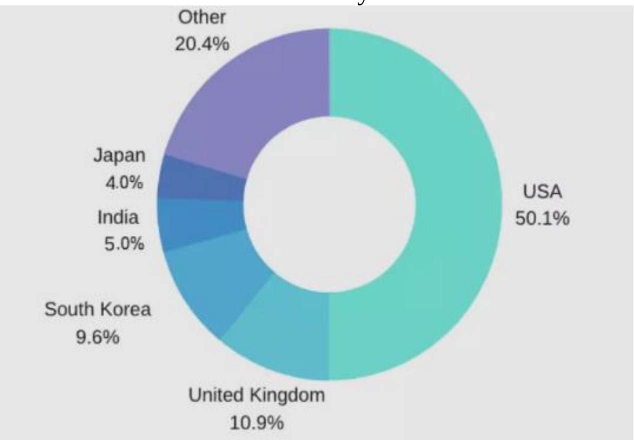


Figure 4 Distribution of detected Deep_fake s by targeted country [18]

According to a survey conducted by sensity.ai [18], India ranks fourth in the world in terms of deep-fake Content development, behind the United States, the United Kingdom, and South Korea (Figure 4).

According to a report published by the NCRB[19] in 2020, communal riots are expected to surge by 96%, with fake news playing a significant role. When false news is developed with Deep fake technology, it appears more authentic. Fake news is extremely hazardous to democracy. Another Indian reporter or human-rights activist whose Deep_fake Obscene and full of nudity clip nevertheless of a pornographic matter [20] video becomes viral to put pressure on the journalist [21] is another example. Apart from that, if any Deep fake of a political leader goes viral just before the election. It has a significant impact on the election results owing to misleading news and determines the country's future.

IV. Statistics of Deep Fake Usage

As the propagation of fake news has accelerated, this technology is now being utilised to spread it. A study [22] was conducted on the topic of fake news on an Indian platform. According to the findings, fake news from, filthy-political-rivalries, finance-Scam, criminality, educational, amusement, skills training, healthcare, sport-&-recreation, global, history, and celebrities accounts for about almost seventy one percent (70.98%) of all fake news, with communalism accounting for twenty two percent (22%) of all fake news (figure 3). Deep fake video is currently being used by Indian political parties to disseminate information quickly. Another example of deep_fake video technique used is by many of India's major political parties prevailing in the nation from time to time.

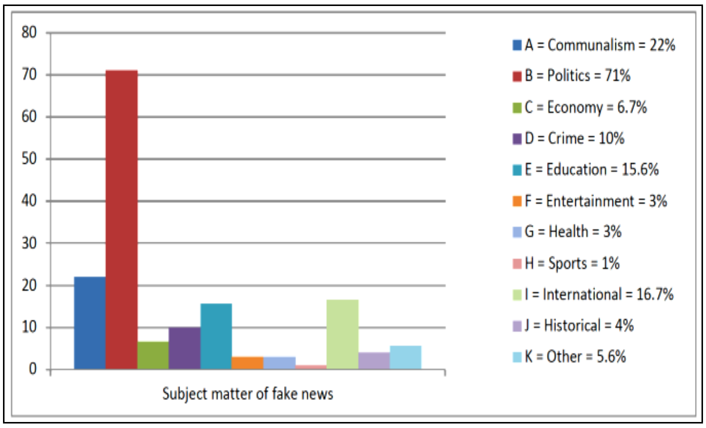


Figure 5 Subject Wise Fake News Stats

When we try to understand the type of media that was utilised to spare phoney news. As seen in Figure 6, over half of all fake news uses video as a medium, compared to textual image, graphical-information, link & attachment bearing text, and textual-images.

The usage of Deep fake technology is playing a very major part in creating fake news of the next level that hardly be authenticated since fake news commonly utilized footage to spare inaccurate information.

Deep fake technology is also employed in the advertising business, in addition to fake news.

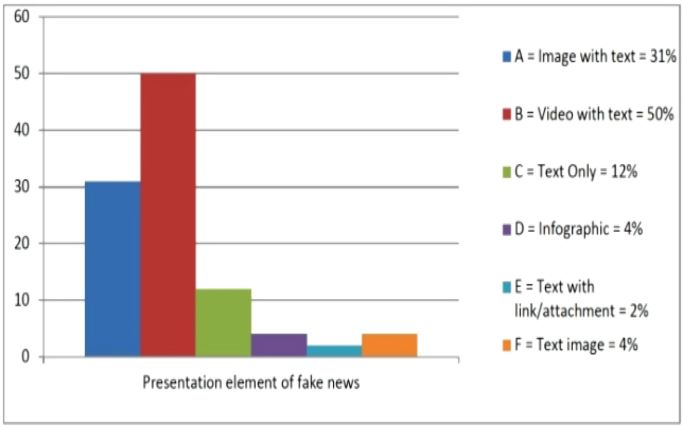


Figure 6 : Category - wise Fake News Stats

Cad-Bury's is the most recent example of digital marketing, which uses deep-learning technology over one of a bollywood star who has recently signed the advertisement contract with the Cad-bury for company's product promotion.

V. TRACINGOUT DEEP FAKE MATTER

Researchers have proposed numerous methods to detect Deep fake [23,25, 26], including the use of PRNU (abbriviated as- photo response non uniformity)alysis in the study of Deep fake utilising senor pattern noise [27]. PRNU is a fingerprints of digital photography that is left in the photos taken by the cameras[28-30]. In picture forensics, the analysis is commonly used[28-32]. Hasan and Salah[33] suggested a model for deep fake detection in block-chain and smart contracts. However, it is a restriction that video sources be traceable. The most recent task of Deep_Fake Tracing on adversarial disruption attempts to befool DNN-based detectors [35-36, 38] has emerged as the invincible challenge which is not only hard to detect but also challenging to trace-out.

VI. CONCLUSION AND FUTURE WORK

Having examined and analyzed these data sets, it is found that people themselves are able to produce their own fictional footage/stories are of others as well. It is often used by ordinary people to replace their visage with that of a movie star or clip[3]. In conjunction with deep learning Artificial intelligence and machine learning, a growing proportion of iphones with high-quality camcorders and easy access to an enormous popularity of Smartphone apps for generating and sharing movies and digital photos has promoted a new phenomena of faking videos known as Deep_fake [1, 4]. We discovered in a study that the graph of photo-shopped faked and morphed video climbs dramatically in various social sites. Detection by Optical Flow Based CNN[43], detection by examining convolutional traces[44], and many others, but these technologies have the drawback of being time consuming and hard to utilise in comparison to the development of Deep_fake video, which is readily available online. We need to create a quick process that can be implemented with little resources. This approach can be used to detect Deep_fake s in their early stages. Apart from this there are the other ways to Control deep-fakes-such as Government's Disciplinary Rules and regulation[45], Rigid business policies with tight action plans, Sensitizing Public against Deep_fake [46] contents through training & awareness programs, Promoting the use, pros & cons of deep-fake methodology to assist in the detection, authentication, and prevention of deep-fakes content widespread around the digital world.

In this study, we attempt to assess the hazards of Deep_fake to society in many scenarios, as well as futuristic democracy. A comparably fast & quicker methodology for detecting Deep_fake and an online portal for detecting such Deep_fake contents can be thout of as future work exploration using factors such as cheek & forehead longitudinal distance in-between, skin-tone & its appearance, eye-brows separation factor, the appearance of facial hair, the appearance of a mole on the face, the blinking of the eyes, the size of the lips, the colour of the lips, and such many other factors involved therein.

REFERENCES

[1] Jafar, M.T., et al. Forensics and analysis of Deep_fake videos. in 2020 11th international conference on information and communication systems (ICICS). 2020. IEEE.

[2] Castillo Camacho, I. and K. Wang, A Comprehensive Review of Deep-Learning-Based Methods for Image Forensics. J Imaging, 2021. 7(4).

[3] Nguyen, T.T., et al., Deep learning for Deep_fake s creation and detection: A survey. arXiv preprint arXiv:1909.11573, 2019.

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

[5] Patel, M., et al. Trans-DF: a transfer learning-based end-to-end Deep_fake detector. in 2020 IEEE 5th international conference on computing communication and automation (ICCCA). 2020. IEEE.

[6] Letzing, J., How to tell reality from a Deep_fake . https://www.weforum.org/agenda/2021/04/are-we-at-a-tipping-point-on-the-use-of-Deep_fake s/, 2021.

[7] Swathi, P. and S. Sk. Deep_fake Creation and Detection: A Survey. in 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA). 2021. IEEE.

[8] Badrinarayanan, V., A. Kendall, and R. Cipolla, Segnet: A deep convolutional encoder-decoder architecture for image segmentation. IEEE transactions on pattern analysis and machine intelligence, 2017. 39(12): p. 2481-2495.

[9] Yang, W., et al., FV-GAN: Finger vein representation using generative adversarial networks. IEEE Transactions on Information Forensics and Security, 2019. 14(9): p. 2512-2524.

[10] Tewari, A., et al., High-fidelity monocular face reconstruction based on an unsupervised model-based face autoencoder. IEEE transactions on pattern analysis and machine intelligence, 2018. 42(2): p. 357-370.

[11] Guo, Y., et al., Fuzzy sparse autoencoder framework for single image per person face recognition. IEEE transactions on cybernetics, 2017. 48(8): p. 2402-2415.

[12] Liu, F., L. Jiao, and X. Tang, Task-oriented GAN for PolSAR image classification and clustering. IEEE transactions on neural networks and learning systems, 2019. 30(9): p. 2707-2719.

[13] Cao, J., et al., 3D aided duet GANs for multi-view face image synthesis. IEEE Transactions on Information Forensics and Security, 2019. 14(8): p. 2028-2042.

[14] Zhang, W., C. Zhao, and Y. Li, A Novel Counterfeit Feature Extraction Technique for Exposing Face-Swap Images Based on Deep Learning and Error Level Analysis. Entropy (Basel), 2020. 22(2).

[15] Güera, D. and E.J. Delp. Deep_fake video detection using recurrent neural networks. in 2018 15th IEEE international conference on advanced video and signal based surveillance (AVSS). 2018. IEEE.

[16] 16. Chesney, B. and D. Citron, Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 2019. 107: p. 1753.

[17] 17. Botha, J. and H. Pieterse. Fake news and Deep_fake s: A dangerous threat for 21st century information security. in ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and publishing limited. 2020.

[18] 18. Hofesmann, E., The State of Deep_fake s in 2020. https://www.skynettoday.com/overviews/state-of-Deep_fake s-2020, 2020.

[19] 19. NCRB Report 2020. https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf, 2021.

[20] 20. Samuel, S., A guy made a Deep_fake app to turn photos of women into nudes. It didn't go well. 2019.

[21] 21. Vurimi Veera Venkata Naga Sai Vamsi, S.S.S., Sodum Sai Mohan Reddy, Sharon S Rose, Sona R Shetty, S Sathvika, Supriya M S, Sahana P Shankar, Deep_fake Detection in Digital Media Forensics. Global Transitions Proceedings, 2022.

[22] Kanozia, R., et al., A study on fake news subject matter, presentation elements, tools of detection, and social media platforms in India. Asian Journal for Public Opinion Research, 2021. 9(1): p. 48-82.

[23] Lyu, S. Deep_fake detection: Current challenges and next steps. in 2020 IEEE international conference on multimedia & expo workshops (ICMEW). 2020. IEEE.

[24] Guarnera, L., et al. Preliminary forensics analysis of Deep_fake images. in 2020 AEIT International Annual Conference (AEIT). 2020. IEEE.

[25] Trinh, L., et al. Interpretable and trustworthy Deep_fake detection via dynamic prototypes. in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision. 2021.

[26] Younus, M.A. and T.M. Hasan. Effective and fast Deep_fake detection method based on haar wavelet transform. in 2020 International Conference on Computer Science and Software Engineering (CSASE). 2020. IEEE.

[27] Koopman, M., A.M. Rodriguez, and Z. Geradts. Detection of Deep_fake video manipulation. in The 20th Irish machine vision and image processing conference (IMVIP). 2018.

[28] Lukas, J., J. Fridrich, and M. Goljan, Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security, 2006. 1(2): p. 205-214.

[29] Rosenfeld, K. and H.T. Sencar. A study of the robustness of PRNU-based camera identification. in Media Forensics and Security. 2009. International Society for Optics and Photonics.

[30] Li, C.-T. and Y. Li, Color-decoupled photo response non-uniformity for digital image forensics. IEEE Transactions on Circuits and Systems for Video Technology, 2011. 22(2): p. 260-271.

[31] Hsu, C.-C. and C.-W. Lin. Unsupervised convolutional neural networks for large-scale image clustering. in 2017 IEEE International Conference on Image Processing (ICIP). 2017. IEEE.

[32] Phan, Q.-T., G. Boato, and F.G. De Natale, Accurate and scalable image clustering based on sparse representation of camera fingerprint. IEEE Transactions on Information Forensics and Security, 2018. 14(7): p. 1902-1916.

[33] Hasan, H.R. and K. Salah, Combating Deep_fake videos using blockchain and smart contracts. Ieee Access, 2019. 7: p. 41596-41606.

[34] Gandhi, A. and S. Jain. Adversarial perturbations fool Deep_fake detectors. in 2020 international joint conference on neural networks (IJCNN). 2020. IEEE.

[35] Hussain, S., et al. Adversarial Deep_fake s: Evaluating vulnerability of Deep_fake detectors to adversarial examples. in Proceedings of the IEEE/CVF winter conference on applications of computer vision. 2021.

[36] Carlini, N. and H. Farid. Evading Deep_fake -image detectors with white-and black-box attacks. in Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops. 2020.

[37] Yang, C., et al. Defending against gan-based Deep_fake attacks via transformation-aware adversarial faces. in 2021 International Joint Conference on Neural Networks (IJCNN). 2021. IEEE.

[38] Yeh, C.-Y., et al. Disrupting image-translation-based Deep_fake algorithms with adversarial attacks. in Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops. 2020.

[39] Christian, J., Experts fear face swapping tech could start an international showdown. The Outline, 2018. 1.

[40] Maddocks, S., 'A Deep_fake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political'deep fakes. Porn Studies, 2020. 7(4): p. 415-423.

[41] Barari, S., C. Lucas, and K. Munger, Political Deep_fake Videos Misinform the Public, But No More than Other Fake Media. OSF Preprints, 2021. 13.

[42] Renaud, L., Will You Believe It When You See It? How and Why the Press Should Prepare for Deep_fake s. Geo. L. Tech. Rev., 2019. 4: p. 241.

[43] Amerini, I., et al. Deep_fake video detection through optical flow based cnn. in Proceedings of the IEEE/CVF international conference on computer vision workshops. 2019.

[44] Guarnera, L., O. Giudice, and S. Battiato. Deep_fake detection by analyzing convolutional traces. in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops. 2020.

[45] Caldera, E., Reject the evidence of your eyes and ears: Deep_fake s and the law of virtual replicants. Seton Hall L. Rev., 2019. 50: p. 177.

[46] Ahmed, M.F.B., et al. Awareness to Deep_fake : A resistance mechanism to Deep_fake . in 2021 International Congress of Advanced Technology and Engineering (ICOTEN). 2021. IEEE.

[47] Manish Agarwal and Prashanth Mannem, "Automatic Gap-fill Question Generation from Text Books", Proceedings of the Sixth Workshop on Innovative Use of NLP for Building Educational Applications, pages 56–64, Portland, Oregon, 24 June 2011.

[48] "Automatic Factual Question Generation from Text" Michael Heilman CMU-LTI-11-004

[49] M Agarwal, R Shah, P Mannem, "Automatic Question Generation using Discourse Cues and Distractor Selection for Cloze Questions" (LTRC), Proceedings of the Sixth Workshop on Innovative Use of NLP for Building Educational Applications, pages 1–9, Portland, Oregon, 24 June 2011.

[50] Y llias Chali Sadid A. Hasan, "Towards Automatic Topical Question Generation" Proceedings of COLING 2012: Technical Papers, pages 475–492, COLING 2012, Mumbai, December 2012.