International Journal of Engineering and Management Research
e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-3 (June 2022)
www.ijemr.net
https://doi.org/10.31033/ijemr.12.3.10

Impact of Deepfake Technology on Digital World Authenticity: A Review

Sarfraj Ahmed[1] and Dr. Mohd Akbar Shaun[2]
[1]PG Scholar, Department of Computer Science, Integral University Lucknow, INDIA
[2]Assistant Professor, Department of Computer Science, Integral University Lucknow, INDIA

[1]Corresponding Author: sarfrajiiet@gmail.com

ABSTRACT

Deep fake technology is an emerging technology that creates fake videos by using artificial intelligence (AI) with the facial expression and lips sing effect. Deep fake technology is widely used in different scenarios with different objectives. Deep fake technology is used to make a highly realistic fake video that can be widely used to spread the wrong information or fake news by regarding any celebrity or political leader which is not created by them. Due to the high impact of social media, these fake videos can reach millions of views within an hour and create a negative impact on our society. This technology can be used by criminals to threaten society by making such deep fake (AI) videos. The results suggest that deepfakes are a threat to our celebrities, political system, religious beliefs, and business, they can be controlled by rules and regulations, strict corporate policy and awareness, education, and training to the common internet users. We need to develop a technology that can examine such types of video and be able to differentiate between real and fake video. Government agency also needs to create some policy to regulate such technology so that monitoring and controlling the use of this AI technology can be managed.

***Keywords*--** Encoder, Decoder, Deep Learning, Generative Adversarial Networks (GANs)

I. INTRODUCTION

Deepfake video technology is made of two words Deep means 'In-depth' and fake means 'not real' in other words we can say that the video is made by using the analysis of the relatively same type of video of a person with the deep learning technology for self-leaning[1, 2]. After analyzing these data sets able to create my own fake video of that person. It is widely use by common people to swap there face with movie hero or clip[3]. The spread of smartphones with high-quality digital cameras in combination with easy access to a myriad of software apps for recording, editing, and sharing videos and digital images in combination with deep learning AI platforms has spawned a new phenomenon of faking videos known as Deepfake[1, 4]. In a study, we find that the graph of deepfake video increases very drastically in various spaces of society 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 deepfake media is just double every six months as shown in figure 1 till 2020[5].

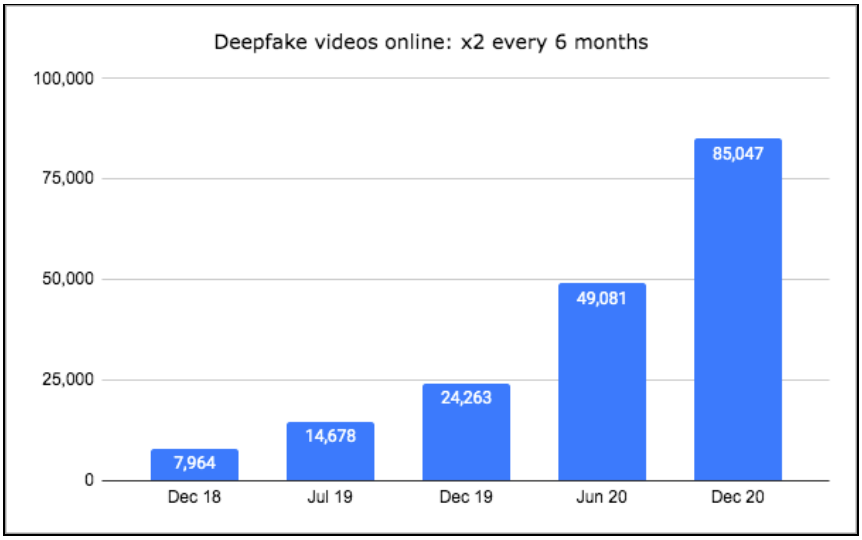

Figure 1: Rate of online deepfake video

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-3 (June 2022)
https://doi.org/10.31033/ijemr.12.3.10

There is one more report published by world Economics forum[6] regarding research paper publication on deepfake figure 2 shows that it's really very emerging topic not only digital world but also in research world. These above studies show that how fast this technology is used by the society in various fields.

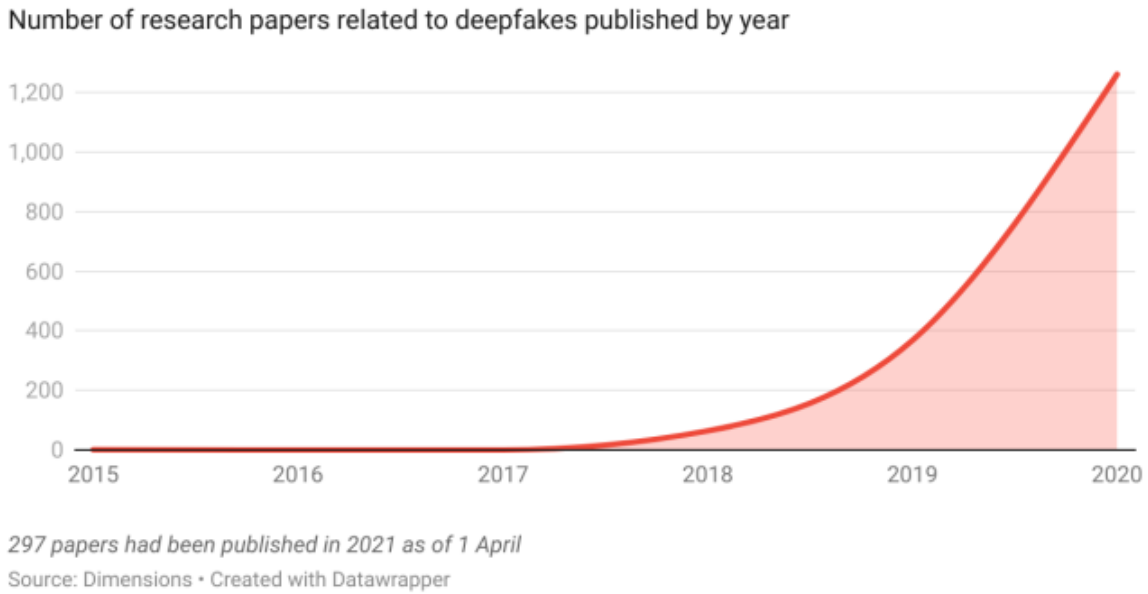

Figure 2: Rate of Deepfake research paper published

II. CREATION OF DEEPFAKE

There are many applications which you can use to create deepfake video event without having too much knowledge of the domain. This make deepfake a big threat to society application such as Face App, Deep Face Lab etc. These types of applications use deep neural network to create Deepfake. There are two ways to create deep fake video. First one is to superimpose the fake audio to the video. And second one is by superimposing benign image into legitimate one[3, 7].

$$\min_G \max_D V(D,G)$$

$$V(D,G) = \mathbb{E}_{x\sim p_{data}(x)}[\log D(x)] + \mathbb{E}_{z\sim p_z(z)}[\log(1-D(G(z))]$$

where,
G = Encoder, D = Decoder, Pdata(x) = distribution of real data, P(z) = distribution of generator, x = sample from Pdata(x), z = sample from P(z), D(x) = Discriminator network, G(z) = Generator network

There are mainly three steps to create deep fake.

1. Extraction: As we know that deepfake based on deep learning technology and it required large amount of data set. To create deepfake video we required large amount of picture of that person. In extraction all the frame that face and do alignment of them. The alignment is very important and critical phase which done using neural network. We do face swapping and for this all the face size should be same.

2. Training: Training is done by using machine learning technology it alludes to the procedure which permits a neural network system to change over a face into other. It is a time taking process which take some few hours and done only once at the time of preparation. When the training finished it can able to change over a face from individual A to individual B

3. Creation: As the training finished it is the last step to create deepfake. It is start with a video or an image, all casings are removed and all appearances are adjusted. At that point, everyone is changed over-utilizing the prepared neural system. The last advance is to consolidate the change over the face once again into the first casing. Its sounds like very simple and easy to implement.it is really where most Deep fake applications turn out badly. As already been told that autoencoders are used to create a deepfake[3].

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-3 (June 2022)
https://doi.org/10.31033/ijemr.12.3.10

The algorithm which is used to create Deepfake are generative network and encoder-decoder neural network i.e. generative adversarial networks (GANs)[8-14]. The main objective of this is to implement face transpose or replace. The face of one person to the face of other person as per as intention of the video. There are two components are encoder and decoder. the encoder network that will help to achieve a dimensional reduction by encoding the data starting from the input layer until it reduces the number of variables. The second one is the decoder network which reduces variables to create a new output very similar to the original[15] as illustrated in figure 5. The deepfake video generated by collecting the aligned face of two person i.e face of person A and face of person B. After that encoder EA is to reconstruct the face of A using data set of face A. In the same manner the face of deepfake we use the weight of these two encoder EA and EB by sharing. But decoder is separated. As soon as optimization has been done. Now any image having face of A can be encode by sharing this encoder but decoded by decoder DB.

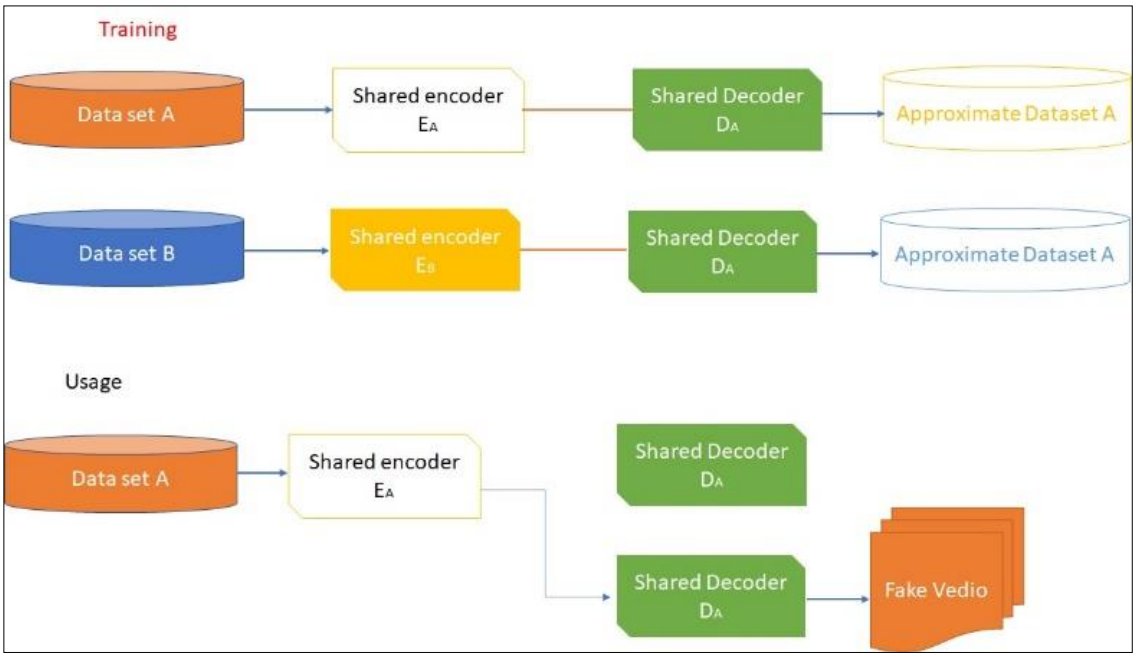

Figure 3: Deepfake principle. Top: the training parts with the shared encoder in yellow **Bottom:** the usage part where images of A are decoded with the decoder of B

Table 1: Tools used to create Deepfake

1	AE Face Tools	http://videohive.net/item/ae-face-tools/24958166
2	CrazyTalk	http://www.reallusion.com/crazytalk
3	DeepFaceLab	http://github.com/iperov/DeepFaceLab
4	Deepfake Detection Challenge	http://deepfakedetectionchallenge.ai
5	Deepfakes Web	http://deepfakesweb.com
6	Deepware – Deep Fake Detection tool	http://www.deepware.ai
7	DF Blue	http://dfblue.com
8	dfaker	http://github.com/dfaker/df
9	Face Crop Jet	http://facecropjet.com
10	Face Ripper 9000	http://github.com/MotorCityCobra/face_ripper_9000
11	Face Swap Live	http://faceswaplive.com
12	Face Swap Online	http://faceswaponline.com
13	FaceCrop	http://www.luxand.com/facecrop

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-3 (June 2022)
https://doi.org/10.31033/ijemr.12.3.10

14	FaceForensics	http://github.com/ondyari/FaceForensics/
15	Faceit	http://github.com/goberoi/faceit
16	Faceswap	http://faceswap.dev
17	Faceswap	http://github.com/dfaker/faceswap
18	Faceware Tech	http://www.facewaretech.com
19	Facial Animation Examples	http://sites.google.com/view/facial-animation/home
20	iClone	http://iclone.reallusion.com
21	iSpeech	http://www.Ispeech.org/voice-cloning
22	Lyrebird	http://lyrebird.ai
23	MRRMRR	http://mrrmrr. Me
24	NaturalFront	http://naturalfront.com
25	Poser	http://www.posersoftware.com
26	Real-Time Voice Cloning	http://github.com/CorentinJ/Real-Time-Voice-Cloning
27	Reflect	http://reflect.tech
28	Resemble AI	http://www.resemble.ai
29	Samsung AI System	http://arxiv. org/abs/190508233 & video
30	Speech Driven Animation	http://github.com/DinoMan/speech-driven-animation
31	The Deepfake Algorithm	http://github.com/deepfakes/faceswap

III. DEEPFAKE THREATS

There are many examples of deepfake technology used to threat the society in different fields such as political[16], social, economic, and many fields of society. As we see in figure 5 most of the fake news is related to politics and in figure 6 its show video is more created to spared fake news. Hence, we can say that deepfake play very important role in the field of fake news creation. The fake news content which is made by using deepfake technology[17] is look alike more authentic and easier to believe to the content of the video. As India is a emotional country. A study done by sensity.ai [18] shows in Figure 4 that India is in top 4 country in the world after USA, U.K and South Korea in the creation of deepfake Content.

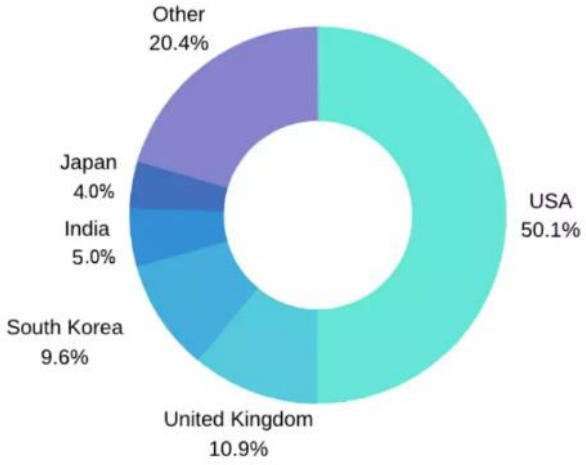

Figure 4 Distribution of detected deepfakes by targeted country (source)

As per as report publish in NCRB[19] report publish in 2020 the communal riots increase 96% and fake news play very important role in this. Fake news look alike more authentic when it was created with deepfake technology Fake news is really very dangerous for democracy. There is one more example of Indian journalist/human rights activist whose deepfake pornographic[20] video goes viral to create pressure on the journalist [21]. Apart from this if any deepfake of political leader just before the election and goes virial. It really effects the result of the election due to false news and decide the future of the country.

e-ISSN: 2250-0758 | p-ISSN: 2394-6962
Volume-12, Issue-3 (June 2022)
https://doi.org/10.31033/ijemr.12.3.10

As the fake news increased very rapidly this technology is also used to spreading fake news. A study [22] done on fake news subject matter on Indian platform. In that study we find that fake news out of communalism, politics, economy, crime, education, entertainment, education, health, sports, international, historical, politics is very almost 71% and communalism is at second highest 22% of all fake news as shown in figure 3. Deepfake video is now use by political party of India for speeding information. There is one more example of use of deep fake video technology is used by one of major political party of India.

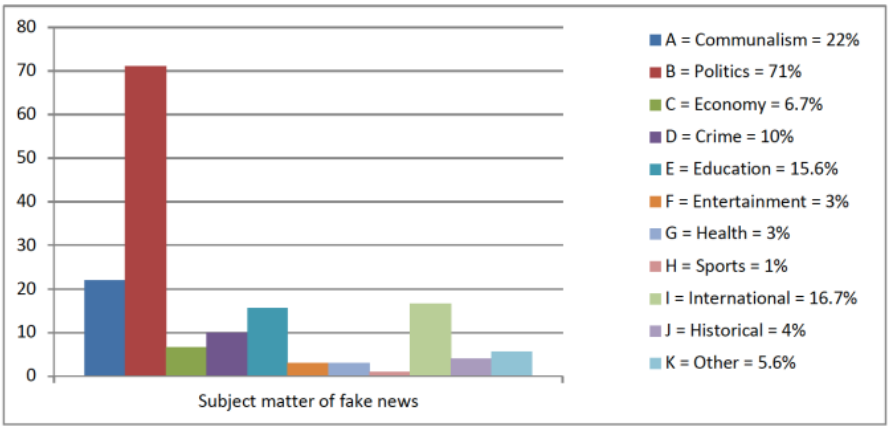

Figure 5: fake news subject wise

When we try knowing that the type media used to spared fake news. We come to know that the almost 50% of fake news contain video as media as compare to image text, info graphics, text with link/attachment, text image as figure 6. The fake news widely used video to spared wrong information it is the reason that use of deepfake technology is play a very big role to create fake news of next level which cannot be easily authenticate.

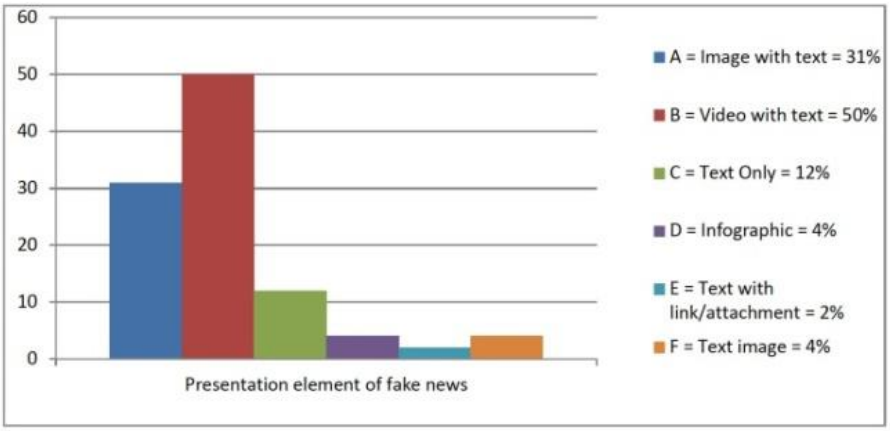

Figure 6: Fake news presentation wise

Apart from the fake news deepfake technology also used in advertising industry. The latest example of digital marketing is by Cadburys which use deep learning over a bollywood star.

IV. DETECTION OF DEEPFAKE

There are various method suggest by researcher to detect deepfake[1, 23-26] such as the use of photo response non uniformity (PRNU) analysis was proposed [27] in the analysis of deepfake using senor pattern noise to analysis. PRNU is approx to no considered as the fingerprint of digital cameras left in the images by the cameras[28-30]. The analysis is widely used in image forensics[28-32]. There is model proposed by Hasan and Salah[33] for deep fake detection blockchain and smart contracts. But it Limitation that video sources should be traceable. The latest work on adversarial perturbation attacks to fool DNN-based detectors[34-38] by deepfake detection task become more difficult to trace

V. DISCUSSION AND CONCLUSION

Deep fake really a upcoming thread to the future of digital world trust. Incoming day it is big question that what we are seeing in digital world we have to believe it or not. Deep fake is widely used pornography for blackmailing[39] the Press[40], politics[41] and Social activist[42].Apart from this it is also used to manipulate election which is serious threat to democracy. To control this damage before it happens. we need to develop a mechanism to detect deepfake video authenticity in minimum amount of possible time. So that any deepfake video gone viral people able to detect it in online process and check the authenticity. There are many technology available for deepfake such as Detection Using Recurrent Neural Networks[15], Detection through Optical Flow Based CNN[43], detection by analyzing convolutional traces[44] and many more but there is limitation in these technology that it will time taking and highly complex to use as compare as creation of deepfake video is easily available online. we need develop an fast methodology which can easily implement with minimum resource. This methodology can be use for primary detection of deepfake
Apart from this there are the other ways to Control deepfakes:

Strict Government Rules and regulation[45], Strict corporate policies with Strict action, Introducing Public awareness training program on deepfake[46], and Encourage deepfake methodology that helps deepfake detection, content authentication, and deepfake prevention.

FUTURE WORK

In this paper we try to analyze the threats of deepfake to the society in different scenario of the society and the future of democracy. In Future work we need to develop a fast methodology to detect deepfake and also develop an online portal for the detection of deepfake using point in mind such as distance of cheek and forehead, appearance of skin, distance between eye brows, facial hair appearance, mole on face, blinking of eyes, size of lips, color of lips and many more point in which we will work to detect deepfake.

REFERENCES

[1] Jafar, M.T., et al. (2020). Forensics and analysis of deepfake videos. In: *11th international conference on information and communication systems (ICICS)*.
[2] Castillo Camacho, I. & K. Wang. (2021). A comprehensive review of deep-learning-based methods for image forensics. *J. Imaging, 7*(4).
[3] Nguyen, T.T., et al. (2019). *Deep learning for deepfakes creation and detection: A survey.* arXiv preprint arXiv:1909.11573.
[4] Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11).
[5] Patel, M., et al. (2020). Trans-DF: a transfer learning-based end-to-end deepfake detector. In: *IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*.
[6] Letzing, J. (2021). *How to tell reality from a deepfake.* Available at: https://www.weforum.org/agenda/2021/04/are-we-at-a-tipping-point-on-the-use-of-deepfakes/.
[7] Swathi, P. & S. Sk. (2021). DeepFake Creation and Detection: A Survey. In: *Third International Conference on Inventive Research in Computing Applications*.
[8] Badrinarayanan, V., A. Kendall & R. Cipolla. (2017). Segnet: A deep convolutional encoder-decoder architecture for image segmentation. *IEEE transactions on pattern analysis and machine intelligence, 39*(12), pp. 2481-2495.
[9] Yang, W., et al. (2019). FV-GAN: Finger vein representation using generative adversarial networks. *IEEE Transactions on Information Forensics and Security, 14*(9), pp. 2512-2524.
[10] Tewari, A., et al. (2018). High-fidelity monocular face reconstruction based on an unsupervised model-based face autoencoder. *IEEE transactions on pattern analysis and machine intelligence, 42*(2), pp. 357-370.
[11] Guo, Y., et al. (2017). Fuzzy sparse autoencoder framework for single image per person face recognition. *IEEE Transactions on Cybernetics, 48*(8), pp. 2402-2415.
[12] Liu, F., L. Jiao & X. Tang. (2019). Task-oriented GAN for PolSAR image classification and clustering. *IEEE Transactions on Neural Networks and Learning Systems, 30*(9), pp. 2707-2719.
[13] Cao, J., et al. (2019). 3D aided duet GANs for multi-view face image synthesis. *IEEE Transactions on Information Forensics and Security, 14*(8), pp. 2028-2042.
[14] Zhang, W., C. Zhao & Y. Li. (2020). A novel counterfeit feature extraction technique for exposing face-swap images based on deep learning and error level analysis. *Entropy (Basel), 22*(2).
[15] Güera, D. & E.J. Delp. (2018). Deepfake video detection using recurrent neural networks. In: *15th IEEE International Conference on Advanced Video and Signal based Surveillance (AVSS)*.
[16] Chesney, B. & D. Citron. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev., 107*, 1753.
[17] Botha, J. & H. Pieterse. (2020). Fake news and deepfakes: A dangerous threat for 21st century information security. In: *15th International Conference on Cyber*

Warfare and Security. Academic Conferences and Publishing Limited.
[18] Hofesmann, E. (2020). *The state of deepfakes in 2020*. Available at: https://www.skynettoday.com/overviews/state-of-deepfakes-2020.
[19] NCRB Report. (2020). Available at: https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf.
[20] Samuel, S. (2019). *A guy made a deepfake app to turn photos of women into nudes. It didn't go well*.
[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. (2022). Deepfake detection in digital media forensics. *Global Transitions Proceedings*.
[22] Kanozia, R., et al. (2021). A study on fake news subject matter, presentation elements, tools of detection, and social media platforms in India. *Asian Journal for Public Opinion Research, 9*(1), 48-82.
[23] Lyu, S. (2020). Deepfake detection: Current challenges and next steps. In: *IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*.
[24] Guarnera, L., et al. (2020). Preliminary forensics analysis of deepfake images. In: *AEIT International Annual Conference (AEIT)*.
[25] Trinh, L., et al. (2021). Interpretable and trustworthy deepfake detection via dynamic prototypes. In: *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*.
[26] Younus, M.A. & T.M. Hasan. (2020). Effective and fast deepfake detection method based on haar wavelet transform. In: *International Conference on Computer Science and Software Engineering (CSASE)*.
[27] Koopman, M., A.M. Rodriguez & Z. Geradts. (2018). Detection of deepfake video manipulation. In: *The 20th Irish Machine Vision and Image Processing Conference*.
[28] Lukas, J., J. Fridrich & M. Goljan. (2006). Digital camera identification from sensor pattern noise. *IEEE Transactions on Information Forensics and Security, 1*(2), pp. 205-214.
[29] Rosenfeld, K. & H.T. Sencar. (2009). A study of the robustness of PRNU-based camera identification. In: *International Society for Optics and Photonics*.
[30] Li, C.-T. & Y. Li. (2011). Color-decoupled photo response non-uniformity for digital image forensics. *IEEE Transactions on Circuits and Systems for Video Technology, 22*(2), pp. 260-271.
[31] Hsu, C.-C. & C.-W. Lin. (2017). Unsupervised convolutional neural networks for large-scale image clustering. In: *IEEE International Conference on Image Processing (ICIP)*.
[32] Phan, Q.-T., G. Boato & F.G. De Natale. (2018). Accurate and scalable image clustering based on sparse representation of camera fingerprint. *IEEE Transactions on Information Forensics and Security, 14*(7), pp. 1902-1916.
[33] Hasan, H.R. & K. Salah. (2019). Combating deepfake videos using blockchain and smart contracts. *IEEE Access, 7*, pp. 41596-41606.
[34] Gandhi, A. & S. Jain. (2020). Adversarial perturbations fool deepfake detectors. In: *International Joint Conference on Neural Networks (IJCNN)*.
[35] Hussain, S., et al. (2021). Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. In: *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision*.
[36] Carlini, N. & H. Farid. (2020). Evading deepfake-image detectors with white-and black-box attacks. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*.
[37] Yang, C., et al. (2021). Defending against gan-based deepfake attacks via transformation-aware adversarial faces. In: *International Joint Conference on Neural Networks (IJCNN)*.
[38] Yeh, C.-Y., et al. (2020). Disrupting image-translation-based deepfake algorithms with adversarial attacks. In: *Proceedings of the IEEE/CVF Winter Conference on Applications of Computer Vision Workshops*.
[39] Christian, J. (2018). Experts fear face swapping tech could start an international showdown. *The Outline, 1*.
[40] Maddocks, S. (2020). A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political'deep fakes. *Porn Studies, 7*(4), 415-423.
[41] Barari, S., C. Lucas, & K. Munger. (2021). Political deepfake videos misinform the public, but no more than other fake media. *OSF Preprints, 13*.
[42] Renaud, L. (2019). Will you believe it when you see it? how and why the press should prepare for deepfakes. *Geo. L. Tech. Rev., 4*, 241.
[43] Amerini, I., et al. (2019). Deepfake video detection through optical flow based cnn. In: *Proceedings of the IEEE/CVF International Conference on Computer Vision Workshops*.
[44] Guarnera, L., O. Giudice & S. Battiato. (2020). Deepfake detection by analyzing convolutional traces. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*.
[45] Caldera, E. (2019). Reject the evidence of your eyes and ears: deepfakes and the law of virtual replicants. *Seton Hall L. Rev., 50*, 177.
[46] Ahmed, M.F.B., et al. (2021). Awareness to Deepfake: A resistance mechanism to Deepfake. In: *International Congress of Advanced Technology and Engineering (ICOTEN)*.