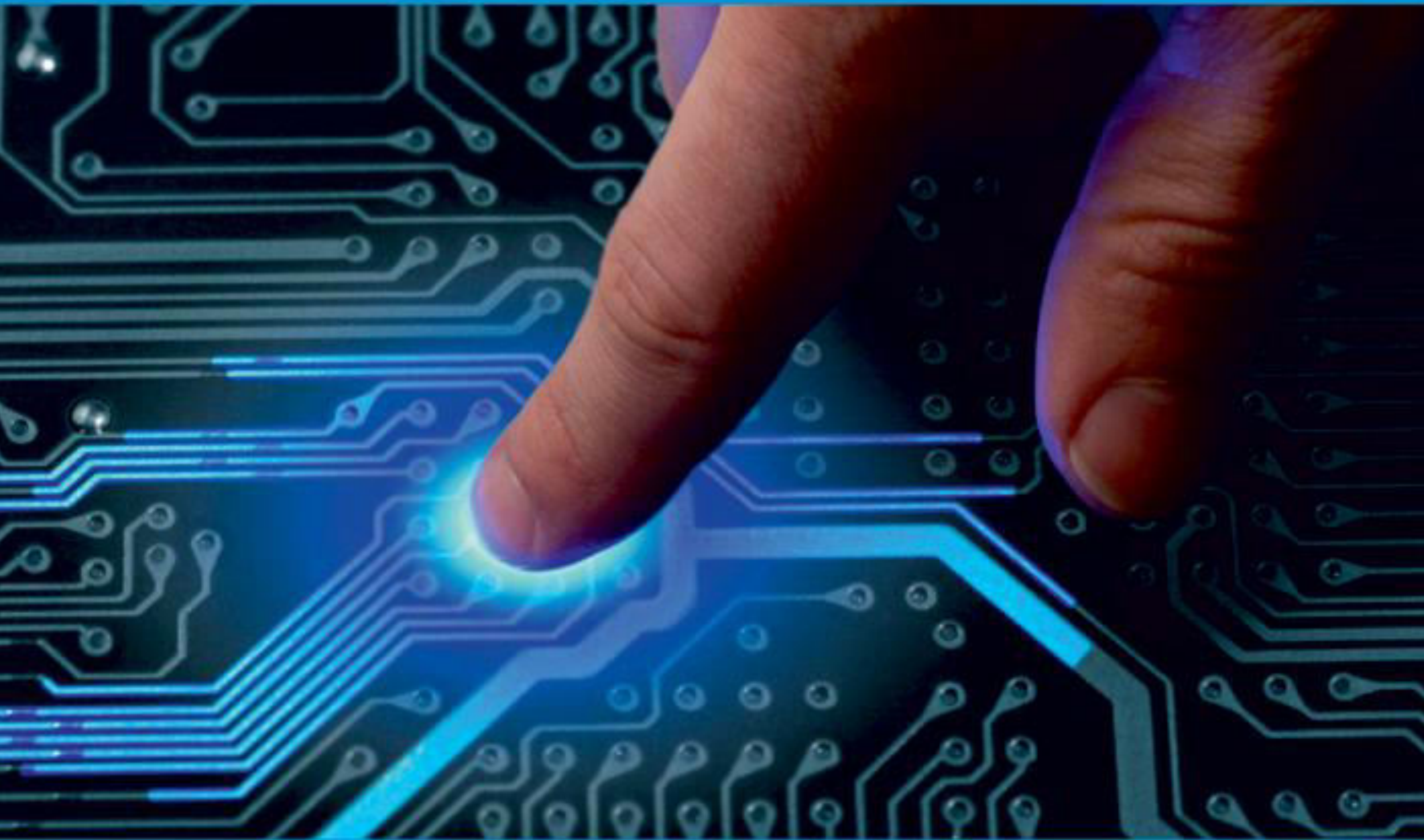
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 6, June 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

The Rise of Deepfake Technology

Omkar Vitthal Kharade, Swati Chopade

P. G Student, Department of MCA (Master of Computer Applications), VJTI Engineering college, Matunga, Mumbai, India

Professor and HOD, Department of MCA (Master of Computer Applications), VJTI Engineering college, Matunga, Mumbai, India

ABSTRACT: This paper explores the fascinating world of deepfakes, highlighting both their creative potential and their potential for misuse. We trace the journey from early autoencoder models to sophisticated GAN models like StyleGAN, explaining how these technologies work and their remarkable advancements. Key milestones include the improvements in realism and control over the generated content. We delve into the practical workflow using Google Colab and the Roop library, and discuss various detection methods like neural network, biometric, and video detection to tackle the challenges posed by deepfakes. The paper also examines the social impacts, such as trust issues, opinion manipulation, cybercrimes, and psychological effects, and reviews efforts to counter these through technological progress, government action, and public awareness. By using the example of Tom Cruise deepfakes on TikTok, we illustrate the ethical dilemmas, artistic possibilities, and social repercussions of deepfake media today.

KEYWORDS:: Deepfakes, Generative Adversarial Networks, GANs, Synthetic media, StyleGAN, Artificial Intelligence, Deepfake techniques, Machine learning, Deepfake detection, Roop library, Google colab, Computer security, Government Regulations, Public perception, Sociology, Ethical consequences, Realism in position, Biometric detection, Video detection, Credibility, Opinion manipulation, Psychological effect, Government actions, Awareness campaigns.

I. INTRODUCTION

Popularly known as deepfakes, Deepfakes are deep learning plus fake and it's Near natural videos that replicate a particular person to do something they never did. Deepfakes are thus in a position to replicate mannerisms specific to facial movements, the tone of voice, and even body postures as deepfakes take their time undergoing various data sets to learn how to swap faces in videos. More specifically, the deepfakes rely on the rate at which the fake information is disseminated; they are, therefore, founded on people's disposition toward information received from friends and acquaintances on social media. Perhaps, this tendency when people take the information received as complete truth if it confirms their position, to a large extent, contributes to the creation of deepfakes. Components and open source software are also now easily procurable thus it was made possible to produce 'cheap fakes' with little technical skills, but the content can be reeled convincingly.

It stemmed from Generative Adversarial Networks (GANs); a generator and a discriminator produce believable media content. Like in the case of GANs, the performance of the model is increased with the help of the shared data set and generating new samples to mislead the discriminator. These networks are able to get representations close to some individuals without copying their icons and are progressing toward controlling face, body, and voice with less input info. Other enhancements have even gone a notch higher to allow the creation of videos out of single pictures for instance the selfies.

Therefore, the deepfake is relevant in the contemporary society through various facets due to the aforesaid potentials and ramifications. Among the social consequences of fake news is that it is rapidly penetrating society, especially due to deep fakes, which means that videos or voices can be successfully impersonated and used to present ''false'' information to people, change their attitude and decrease trust in society. Likely, deepfakes present a threat to the credibility of elections especially when the fake content is developed in a way that affects the politicians, other influential personalities or institutions with an intention of influencing the mass in the process of the election.

In the media and entertainment industry, deepfake technology has both positive and negative implications. While it can be used creatively, it also poses risks such as creating fake celebrity videos or altering movie scenes, impacting

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

reputations and intellectual property rights. Cybersecurity is another critical area affected by deepfakes, as they can be used for identity theft or to create convincing fake videos for phishing attacks, compromising personal or organizational security. Privacy concerns are also paramount, with deepfakes having the potential to violate privacy rights by superimposing individuals' faces onto explicit or compromising content without their consent, posing significant threats to personal privacy and reputation.

The legal and ethical challenges posed by deepfakes are complex. Determining responsibility for their creation and distribution, regulating their use, and addressing their impact on rights such as freedom of speech and expression are areas of concern. The interaction between technology and society is also challenged by the rise of deepfake technology, necessitating a balance between technological advancement and responsible usage to mitigate potential harm.

Understanding the relevance of deepfakes in today's world is crucial for prompting discussions about ethical considerations, regulation, technological advancements, and the development of countermeasures to address the challenges they present. The impact of deepfake technology spans various sectors, underscoring the need for awareness, preparedness, and proactive measures to mitigate its negative consequences.

II. PROBLEM STATEMENT

The advancement of deepfake technology presents important challenges. Deepfakes, which use AI to create hyper-realistic fake videos and images, threaten to erode trust in media, manipulate public opinion, and compromise cybersecurity. They can be used for identity fraud, financial scams, and unauthorized access to sensitive information, posing severe risks to individuals and organizations. Additionally, deepfakes can cause psychological harm by fostering skepticism and anxiety, and they present complex regulatory and ethical challenges. This research aims to explore the impacts of deepfakes and propose measures for effective detection, regulation, and public education to mitigate their negative effects.

III. LITERATURE SURVEY

Korshunov Pavel and Marcel Sebastien in [1] (2019) introduces a groundbreaking database comprising 620 Deepfake videos across 16 pairs of subjects sourced from the VidTIMIT database. These videos were generated in two versions using different GAN models—64 × 64 and 128 × 128—to demonstrate the vulnerability of cutting-edge VGG and Facenet-based face recognition algorithms. The findings revealed that these algorithms struggle to differentiate Deepfake videos from originals, exhibiting up to a 95.00% equal error rate. Additionally, the study evaluated various baseline face swap detection methods, uncovering limitations in lip-sync-based approaches but showing promise in image quality-based measures coupled with SVM classifiers, achieving an 8.97% equal error rate in detecting high-quality Deepfake videos. However, the paper warns of the continuous evolution in face-swapping techniques, indicating that future Deepfake videos may pose increased challenges for existing detection algorithms. This raises the need for new databases and more robust detection methods to counter these advancements, suggesting the potential emergence of an ongoing competition or "arms race" between Deepfake creation methods and detection algorithms.

Westerlund Mika in [2] (2019) analyzed 84 recent news articles on deepfakes revealed their AI-generated, hyper-realistic nature used for creating misleading content that spreads rapidly on social media. Deepfakes pose threats to society, politics, and businesses by eroding trust, manipulating information, and potentially compromising security. Various actors, from governments to trolls, create these videos for diverse reasons like propaganda, monetary gain, or entertainment. However, legitimate uses exist in industries like entertainment, healthcare, and education. Combating deepfakes demands a multi-pronged approach involving legislation, corporate policies, education, and technology, although challenges persist due to the rapid evolution of this technology. Awareness, media literacy, and collaborative efforts among entities are crucial. Leveraging AI-based detection tools, digital watermarks, and blockchain may aid in countering deepfake sophistication. Despite limitations, this study consolidates news-based insights, contributing significantly to understanding and tackling deepfake challenges in today's digital era.

Katarya Rahul And Lal Anushka in [3] (2020) As deepfake technology advances, the challenge of detecting these highly convincing fake contents escalates, demanding immediate and cautious responses. Organizations can consider implementing encrypted digital stamps to authenticate digital media, aiming to distinguish between genuine and generated content. To prevent the widespread dissemination of deepfakes, social media platforms must proactively develop tools for moderation, detection, and prevention, possibly introducing deliberate confusion in digital photos

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

uploaded online. However, countering deepfakes requires continuous innovation, given their rapid evolution, necessitating ongoing research and adaptation of tools, especially within the realm of machine learning. In this ongoing battle, a multifaceted approach and sustained research efforts are vital to effectively combat the escalating threat posed by deepfakes.

Neethirajan Suresh in [4] (2021) Summarizing the impact of deepfake technology reveals both positive and negative aspects. While potential benefits in biomedical, behavioral, and agricultural fields are emerging, these areas are in early stages and require further development before widespread use. Standards, security measures, and comprehensive implementation are crucial to prevent manipulation. Pilot studies are needed to understand deepfake technology's broader scientific implications beyond human applications. Ultimately, deepfakes hold promise for positive contributions but require careful exploration to maximize benefits and minimize risks.

IV. PROPOSED METHODOLOGY AND DISCUSSION

Deepfake Creation Techniques

Deepfakes leverage deep learning techniques due to their ability to handle complex data. Early deepfakes utilized autoencoders, a type of deep neural network, to extract and reconstruct latent features of face images. The encoder-decoder architecture is a common framework for deepfake creation. During the training phase, a dual encoder-decoder setup is used where both networks share a common encoder but possess distinct decoders. For generating a deepfake, an image of face A is encoded using the shared encoder and then decoded using decoder B, blending features from both input images. This setup is used in applications like DeepFaceLab, DFaker, and DeepFake tf.

Advanced deepfake models like faceswap-GAN incorporate adversarial and perceptual losses, such as VGGFace, to enhance realism and consistency in facial features, resulting in higher-quality output videos. Moreover, different neural network architectures are utilized to improve the quality of deepfakes. Techniques such as FaceNet’s multi-task CNN are employed for stable face detection and alignment, and CycleGAN is used for generative network implementation.

Generative Adversarial Networks (GANs) play a significant role in deepfake creation. GANs consist of a generator and a discriminator engaged in a minimax game, where the generator aims to produce realistic images while the discriminator aims to distinguish real from fake images. StyleGAN, a variant of GAN, is designed specifically for realistic face image generation. It introduces a mapping network and a synthesis network, allowing for style control during image synthesis via adaptive instance normalization (AdaIN) operations. StyleGAN's generator architecture can separate and control high-level attributes in image synthesis, enabling intuitive manipulation of specific attributes like pose and identity in faces.

Deepfake Detection

Deep learning has made significant strides in effectively detecting deepfakes. Neural network-based methods analyze statistical features of images to enhance the detection of fake face images created by humans. For instance, deep convolutional neural networks (CNNs) are specifically designed for detecting fake images generated by GANs by extracting and fine-tuning face features for real/fake image detection. Forensics CNNs employ image preprocessing steps like Gaussian Blur and Gaussian Noise to detect fake human images by neglecting low-level high-frequency clues artifacts in GAN images. Hybrid approaches use a combination of techniques to improve detection accuracy. For example, a two-stream network for detecting face tampering uses a face classification stream for training on tampered and authentic images and a patch triplet stream to analyze features using steganalysis feature extractors, capturing low-level camera characteristics and local noise residuals.

For video detection, analyzing physiological signals such as eye movement and blinking can help identify fake face videos. Heartbeat analysis models detect deepfakes by analyzing biological signals like photoplethysmogram (PPG) cells. Audio-visual modality interaction frameworks use Siamese network-based architecture to extract speech and face modalities simultaneously to discriminate between real and fake videos. Temporal sequence analysis and combining spatial and temporal constraints further enhance video detection models. Models like Recycle-GAN and recurrent convolutional networks leverage spatial and temporal data using conditional generative adversarial networks to achieve effective results.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

Data Collection Process

In the field of deepfake detection, several public datasets have emerged as crucial resources for researchers and developers. These datasets serve as vital benchmarks for training and evaluating algorithms designed to identify manipulated or synthetic content in media. Key datasets include FFHQ (Flickr-Faces-HQ), 100K-Faces, DFFD (Diverse Fake Face Dataset), CASIA-WebFace, VGGFace2, The Eye-Blinking Dataset, and DeepfakeTIMIT. These datasets provide diverse and extensive data for analysis, training, and assessment of detection algorithms, encompassing a wide range of facial attributes, gender and age representations, and manipulated video content.

Challenges in Deepfake Detection

Several challenges arise in deepfake detection. Real-time detection demands significant computational resources and balancing detection accuracy while minimizing processing time. Achieving high accuracy without raising false positives and ensuring effectiveness across various media types, such as images, videos, and audio, is challenging. Detection models must adapt to recognize deepfakes despite alterations like compression, noise, resolution changes, and transformations. Developing models that generalize well across diverse datasets and variations in deepfake creation methods is another significant challenge. Understanding the decision-making process of deep learning models is crucial for accountability and trust, particularly in forensic applications, yet the black-box nature of these models limits interpretability. Ethical concerns arise in accessing private or sensitive data for training detection models, necessitating privacy-preserving methods. Ensuring datasets used for training detection models are sufficiently diverse and free from biases, as well as addressing the scarcity of high-quality annotations, impacts the quality of training data. Adversarial perturbations can exploit weaknesses in detection algorithms, making robustness a significant challenge.

Strategies to Enhance Deepfake Detection

To enhance deepfake detection, advanced learning techniques such as meta-learning and metric learning can improve model adaptability across diverse deepfake variations. Implementing efficient architectures like Transformers can enhance detection accuracy and efficiency. Feature restoration and attention mechanisms can restore altered features and focus on crucial details for better detection. Integrating adversarial training and data augmentation techniques can improve model robustness against alterations. Exploring privacy-preserving methods allows model training on decentralized data without compromising individual privacy. Developing countermeasures to identify and counter adversarial attacks hinders the creation of deceptive deepfakes. Utilizing digital watermarking techniques and blockchain can embed and verify the authenticity of digital content, making tampering evident. Implementing programs to educate users on recognizing manipulation signs and verifying media authenticity reduces the impact of deepfakes. Establishing regulations to deter malicious use, define liabilities, and safeguard individuals' rights against the misuse of deepfake technology is essential.

Tools and Software for Creating Deepfakes

Several tools and software are commonly used to create deepfakes. These include Avatarify, Reface: Face Swap Video App, FaceApp, MorphMe, Deepfakes web β, DeepFaceLab, FaceSwap, Revive AI, Deepbrain AI, DeepAI, FacePlay – Face Swap Videos, Adobe's Project Morpheus, Deep Dream Generator, and Mimic – AI Photo Face Animator. Each tool caters to different user preferences, from those seeking entertainment and fun face-swapping to professionals interested in advanced deepfake creation or artistic image manipulation. Prices and features vary across these platforms, providing users with a wide range of choices based on their specific needs and skill levels.

Impact of Deepfakes on Society

Deepfakes significantly impact various aspects of society, leading to an erosion of trust and altering perceptions of reality. The pervasive nature of manipulated content causes widespread skepticism, undermining trust in media and institutions. Constant exposure to deepfakes creates a state of doubt, making it increasingly challenging to distinguish between authentic and fabricated information.

In the realm of public opinion and social harmony, deepfakes possess the potential to manipulate elections, incite social unrest, and propagate false narratives. This poses a substantial threat to democratic principles by amplifying discord

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

and division within society. Additionally, businesses face cybersecurity vulnerabilities and corporate risks, including reputational damage, financial manipulation, and identity fraud. The misuse of deepfakes for corporate sabotage or scams leads to severe threats to corporate stability and consumer trust.

Psychologically, prolonged exposure to manipulated content can lead to 'reality apathy,' where individuals habitually distrust all information, whether genuine or not. The constant dissemination of misinformation could fundamentally alter societal perceptions, resulting in a breakdown of shared understanding and discourse.

Efforts in Detecting and Mitigating the Harmful Effects of Deepfakes:

Efforts to detect and mitigate the harmful effects of deepfakes are extensive, involving technological advancements, policy initiatives, and educational campaigns. Technological advances include the development of AI-powered algorithms that scrutinize videos and images for inconsistencies, anomalies, or artifacts indicating manipulation. Biometric analysis utilizes subtle changes in facial blood flow, Photo Response Non-Uniformity (PRNU) patterns unique to camera sensors, and audio-based inconsistencies to authenticate content. Digital watermarking techniques embed unique signatures into content for verification, while blockchain technology enhances traceability and authenticity verification.

Policy initiatives involve adapting existing laws or introducing new ones to address deepfake-related offenses such as libel, defamation, and identity fraud. Balancing regulation of deepfake technology while upholding free speech and privacy rights remains a challenge. Social media platforms and tech companies are implementing policies to detect, flag, and remove deepfake content, collaborating to prevent the spread of manipulated content.

Educational campaigns focus on raising public awareness about the potential misuse of AI and deepfakes, emphasizing critical thinking and digital literacy. These programs teach individuals to identify fake news, understand evolving technology landscapes, and protect personal data.

V. IMPLEMENTATION DETAILS

Face Swap using Roop Library

This phase leverages the Roop library's tools to merge features from a target and facial image, generating deep fake images through detailed technical steps. The process harnesses Roop's image processing and deep learning capabilities.

Face Swap using First Order Model (Video)

In this phase, the first-order model is used to create a deepfake video. This involves downloading the necessary models and configuring the environment to perform the face swap. The procedure starts with identifying a source image and a target image. The process culminates in generating the output image , which is integrated into a video format, showcasing the seamless transition between the images.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

VI. RESULTS

Face Swap using Roop Library

Figure 1: Target (On Left) And Source Image (On Right)

Figure 2: Result Image.

The initial step involves selecting a target image. Following this, a face image is chosen, which will be merged with the target. The final step generates the output image, showcasing the deep fake result. This process is repeated with a second set of images, selecting another target image and a new face image, leading to the creation of another output image.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

Face Swap using First Order Model (Video)

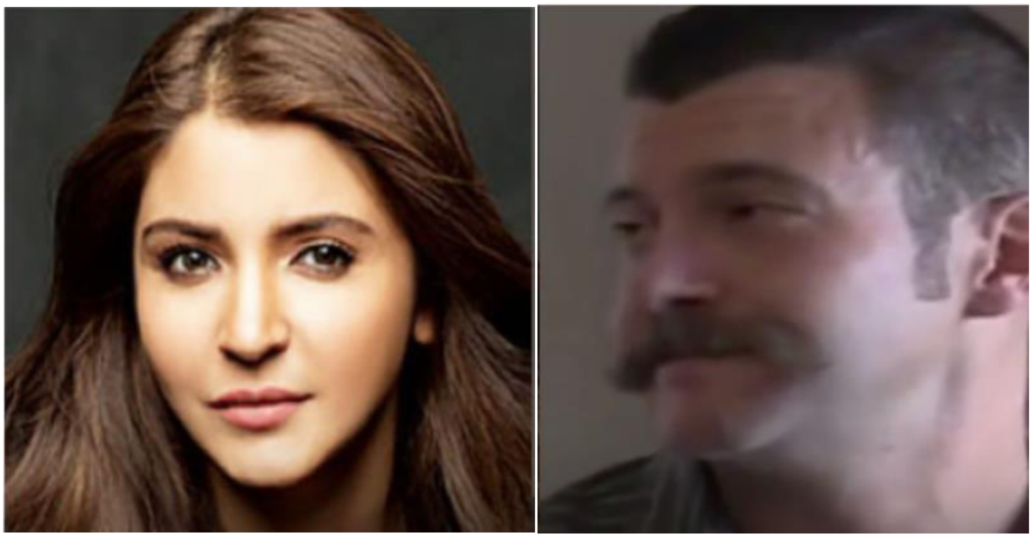


Figure 3: Target (On Left) And Source Image (On Right).

Figure 4: Result Image.

VII. CASE STUDY

The Viral Tom Cruise Deepfakes on TikTok

In recent years, deepfake technology has emerged as a significant advancement, allowing for the creation of remarkably realistic videos through machine learning techniques. One notable case involves the viral Tom Cruise deepfakes on TikTok, created by Chris Ume, a skilled VFX specialist, in collaboration with Tom Cruise impersonator Miles Fisher. This project aimed to showcase the capabilities of deepfake technology while entertaining audiences.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

The project began with Ume's fascination with Fisher's video depicting a fictitious presidential run by Tom Cruise, leading to their collaboration. They produced a series of "harmless" clips posted on the @deeptomcruise TikTok account, quickly gaining traction and amassing a large following. Ume highlighted the meticulous nature of the deepfake creation process, combining traditional CGI and VFX techniques with open-source DeepFaceLab algorithms and video editing tools. Each clip required weeks of work, emphasizing careful adjustments and attention to detail to ensure seamless appearances and eliminate glitches. Fisher's expertise in impersonating Tom Cruise's mannerisms significantly contributed to the success of the deepfakes.

The viral success of these deepfakes sparked discussions about the implications of deepfake technology. While Ume's project aimed at entertainment, it raised concerns about potential misuse, particularly in creating non-consensual or deceptive content. Ume also highlighted the positive potential of deepfakes, such as their use in film, TV, restoring old footage, and CGI character animation, emphasizing the need for human intervention to ensure believability and the technology's inevitability in the media landscape.

VIII. CONCLUSION

This exploration into deepfake technology has emphasized its practical implementation through the use of the Roop library in Google Colab, showcasing the ease and accessibility of executing face swapping. The technical demonstration highlighted the simplicity of creating such manipulations, underscoring the urgency of establishing robust measures to counter potential adverse societal impacts. However, this technical focus needs to be complemented by a deeper analysis of ethical considerations and broader societal implications.

The societal impact of deepfakes was extensively discussed, revealing significant concerns such as the erosion of trust, manipulation of public opinion, cybersecurity vulnerabilities, and the psychological impact of prolonged exposure to manipulated content. While commendable efforts have been made in detecting and mitigating deepfakes, further exploration into their societal and psychological effects is crucial. Strengthening the discourse on ethical considerations, societal implications, and potential misuse is necessary for a comprehensive understanding of deepfakes.

Future work should take a multifaceted approach, expanding technological advancements beyond detection to encompass a deeper understanding of the psychological, social, and ethical dimensions of deepfakes. Comprehensive frameworks addressing the ethical use of this technology are needed. Additionally, enhancing public awareness and digital literacy is vital to empower individuals to critically analyze and navigate the digital landscape. As the technology evolves, striking a balance between innovation and ethical considerations will be pivotal for the responsible integration of deepfake technology into various domains.

REFERENCES

[1] Korshunov, P., & Marcel, S. (2019). Vulnerability assessment and detection of Deepfake videos. DOI: 10.1109/ICB45273.2019.8987375

[2] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Journal Name, 9(11).

[3] Lal, A., Katarya, R. (2020). A Study on Combating Emerging Threat of Deepfake Weaponization. In Proceedings of the Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), DVD Part Number: CFP20OSV-DVD; ISBN: 978-1-7281-5463-3. DOI: 10.1109/I-SMAC49090.2020.9243588.

[4] Neethirajan, S. (2021). Is Seeing Still Believing? Leveraging Deepfake Technology for Livestock Farming. Frontiers in Veterinary Science, 8:740253.

[5] Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., Nguyen, T. T., Pham, Q.-V., & Nguyen, C. M. (Year). Deep Learning for Deepfakes Creation and Detection: A Survey (Version 5). Computer Vision and Image Understanding, 223, 103525.

[6] Almars, A. M. (2021). Deepfakes Detection Techniques Using Deep Learning: A Survey. Journal of Computer and Communications, 9(5), Article 95003.

[7] Tariq, S., Lee, S., Kim, H., Shin, Y. and Woo, S.S. (2018) Detecting Both Machine and Human Created Fake Face Images in the Wild. Proceedings of the 2nd International Workshop on Multimedia Privacy and Security, Toronto, 15 October 2018, 81-87.

[8] Li, H., Li, B., Tan, S. and Huang, J. (2018) Detection of Deep Network Generated Images Using Disparities in Color Components.

[9] Do, N.-T., Na, I.-S. and Kim, S.-H. (2018) Forensics Face Detection from GANS Using Convolutional Neural Network. ISITC.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 6, June 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1206094 |

[10] Xuan, X., Peng, B., Wang, W. and Dong, J. (2019) On the Generalization of GAN Image Forensics. In: Chinese Conference on Biometric Recognition, Springer, Berlin, 134-141.

[11] Liu, F., Jiao, L. and Tang, X. (2019) Task-Oriented GAN for PolSAR Image Classification and Clustering. IEEE Transactions on Neural Networks and Learning Systems, 30, 2707-2719.

[12] Zhou, P., Han, X., Morariu, V.I. and Davis, L.S. (2017) Two-Stream Neural Networks for Tampered Face Detection. 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Honolulu, 21-26 July 2017, 1831-1839.

[13] Hsu, C.-C., Zhuang, Y.-X. and Lee, C.-Y. (2020) Deep Fake Image Detection Based on Pairwise Learning. Applied Sciences, 10, 370.

[14] Li, Y., Chang, M.-C. and Lyu, S. (2018) In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking. 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, 11-13 December 2018, 1-7.

[15] Ciftci, U.A., Demir, I. and Yin, L. (2020) How Do the Hearts of Deep Fakes Beat? Deep Fake Source Detection via Interpreting Residuals with Biological Signals. 2020 IEEE International Joint Conference on Biometrics (IJCB), Houston, 28 September-1 October 2020, 1-10.

[16] Mittal, T., Bhattacharya, U., Chandra, R., Bera, A. and Manocha, D. (2020) Emotions Don't Lie: An Audio-Visual Deepfake Detection Method Using Affective Cues. Proceedings of the 28th ACM International Conference on Multimedia, Seattle, 12-16 October 2020, 2823-2832.

[17] Korshunov, P. and Marcel, S. (2018) Deepfakes: A New Threat to Face Recognition? Assessment and Detection.

[18] Bansal, A., Ma, S., Ramanan, D. and Sheikh, Y. (2018) Recycle-GAN: Unsupervised Video Retargeting. Proceedings of the European Conference on Computer Vision (ECCV), Glasgow, 23-28 August 2018, 119-135.

[19] Sabir, E., Cheng, J., Jaiswal, A., AbdAlmageed, W., Masi, I. and Natarajan, P. (2019) Recurrent Convolutional Strategies for Face Manipulation Detection in Videos. CVPR Workshops.

[20] Karras, T., Laine, S. and Aila, T. (2019) A Style-Based Generator Architecture for Generative Adversarial Networks. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, 15-20 June 2019, 4401-4410.

[21] Dang, H., Liu, F., Stehouwer, J., Liu, X. and Jain, A.K. (2020) On the Detection of Digital Face Manipulation. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, 13-19 June 2020, 5781-5790.

[22] Yi, D., Lei, Z., Liao, S. and Li, S.Z. (2014) Learning Face Representation from Scratch.

[23] Cao, Q., Shen, L., Xie, W., Parkhi, O.M. and Zisserman, A. (2018) Vggface2: A Dataset for Recognising Faces across Pose and Age. 2018 13th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), Xi'an, 15-19 May 2018, 67-74.

[24] Güera, D. and Delp, E.J. (2018) Deepfake Video Detection Using Recurrent Neural Networks. 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, 27-30 November 2018, 1-6.

[25] Zhu, J.-Y., Park, T., Isola, P. and Efros, A.A. (2017) Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks. Proceedings of the IEEE International Conference on Computer Vision, Venice, 22-29 October 2017, 2223-2232.

[26] Naitali, A., Ridouani, M., Salahdine, F., & Kaabouch, N. (2023). Deepfake Attacks: Generation, Detection, Datasets, Challenges, and Research Directions. Computers, 12(10), 216.

[27] Siarohin, A., Lathuilière, S., Tulyakov, S., Ricci, E., & Sebe, N. (2019). First Order Motion Model for Image Animation. In Advances in Neural Information Processing Systems 32 (NeurIPS 2019).

.