Deepfakes in Cyber Warfare: Threats, Detection, Techniques and Countermeasures

Abstract:

Technology known as deepfake (DT) has reached an entirely new level of complexity. Cybercriminals now have the ability to modify sounds, images, and videos in order to mislead individuals and businesses and spread false information. This constitutes a rising threat to international organizations as well as individuals, and it is imperative that something be done about it. This article presents an overview of deepfakes, discussing their usefulness to society as well as the operation of DT. This article focuses on the dangers that can be posed by deep fakes to the economic, political, and legal institutions of countries all over the world. In addition to this, the study will investigate various solutions to the problem of deepfakes, and it will finish by discussing potential directions for further research.

Key words: Deepfake, cyber warfare, threats, Cyber criminals, danger.

1. INTRODUCTION:

Deepfake technologies (DT) have come into existence as a direct result of developments in artificial intelligence (AI) [1, 2]. These technologies present a huge risk to institutions all over the world. Deepfake is a term that refers to a technology that is built on AI that has the ability to change images, audio, and video content in order to represent an event that did not actually take place. For example, it is becoming increasingly usual for the faces of politicians to be edited onto the bodies of other people, who then appear to say things that the politicians have never actually said. This expanding phenomenon has been used in political contexts to misinform the public on a variety of subjects, and it is only going to continue to do so. Take, for example, the use of a deepfake video by a satirical television show in Italy directed against Matteo Renzi, the current

Prime Minister of Italy. In the footage that was circulated on social media, he could be seen belittling other lawmakers. As the video became viral online, an increasing number of people started to assume it was real, which resulted in fury among the general population [3, 4]. “Deepfakes have also been used by cybercriminals to impersonate Chief Executive Officers (CEOs) at firms in order to trick staff, typically those working in finance departments, into transferring money to bank accounts controlled by the scammers” [5, 6]. The vast majority of deepfake alterations are created for use in entertainment mediums such as films, videogames, and instructional videos [7, 8]. Cybercriminals, on the other hand, have found ways to exploit the technology in order to mislead organizations and individuals and commit fraud. In addition, the production of such deep fakes demands knowledge in addition to specialized computer software and technology [9, 10]. However, the existence of freely available software like "FaceSwap" and "Reface" has made it possible for unskilled individuals to participate in media manipulation for the sake of either enjoyment or harmful intent [10-12].

Deepfake technology can be used to create synthetic media that is so convincing that people cannot tell the difference between it and the real thing. It is a relatively new field of research, and academics from both academia and industry have contributed deepfake databases, as well as synthesis and detection algorithms, all of which have contributed to the rise in popularity of deep fakes [13, 14]. “Deepfakes are the outcome of artificial intelligence (AI) applications that merge, combine, replace, and superimpose photos and video clips to generate fake videos that look to be legitimate” [15]. Deepfakes take advantage of current developments in deep neural networks to produce artificial media that is extremely lifelike [16]. When deepfake technology is applied to movies or still photos, it is possible to replace the face of a person with that of another person while leaving very little evidence of manipulation [17]. According to Cho and Jeong [18], the development of deep learning has rendered previously established phony face detection systems susceptible.

“The availability of deepfake datasets, as well as synthesis and detection techniques, has made it possible for the community and even less experienced users to construct realistic deepfakes. This, in turn, has resulted in an enormous increase in the amount of popularity deepfake videos have in the wild” [19]. Deepfakes that are convincing can swiftly reach millions of people and

have a harmful impact on our society [20]. This is made possible by the reach and speed of social media.

The increase in the volume of scholarly material that is relevant to deepfakes research has also been a reflection of this expansion. In addition to the technological aspects associated with the production and detection of deep fakes, the ethical, social, and legal implications have also been meticulously explored. There have already been some reviews written in particular sectors, such as the creation and detection of deepfakes [21], law [22], forensics [23], and social impact [24], to name just a few of these areas. Nevertheless, none of them considers the entire breadth of research fields in deepfakes, which we believe might be highly valuable for academics who intend to work on this research issue [25]. Despite the fact that it is still relatively young, research into deepfakes is a rapidly expanding field of study. Within this field, the research topics and how they relate to one another are continuously shifting over time, and new tendencies are emerging [26]. Researchers working on deepfakes come from a wide range of diverse academic and professional backgrounds, judging by the numerous subfields of research that are being conducted. In addition to the present tendencies, it is interesting to investigate the financing opportunities, since this can assist focus the study effort [27, 28].

2. LITERATURE REVIEW

The technology that is deployed in the fight against deep fakes can be broken down into three distinct categories:

(1) The detection of the deep fake;

(2) The authentication of the published material; and

(3) The prevention of the distribution of content that may be exploited for the development of deep fakes.

“Despite the rapid expansion of technology for the detection and verification of deep fakery, which is gaining foothold quickly, the capacity to produce deep fakes is increasing far faster than the ability to detect them. This is despite the fact that the technology is gaining ground swiftly. Because the creation of Deepfakes can be done with malicious intent, the detection of these fakes

presents a potential threat to system security". [107] Bismi et al. describe "a variety of creation and detection approaches that are currently being researched in Deepfake". "These methods make use of a variety of techniques, including Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short Term Memory (LSTM), and a number of other similar methods. These strategies provide a backbone for the creation of a new scheme that would be both more compactable and precise in the identification of Deep fakes"[29, 30]. Zhiming and colleagues present "a method for detecting Deepfakes that is built on MesoNet and includes a preprocessing module. In this procedure, the low-frequency signals in the image are filtered out, but the high-frequency signals that exhibit apparent variations are kept". "This results in a greater contrast in texture between the genuine and Deepfake-generated versions of the image"[31, 32]. Hina et al. provide "a comprehensive description of the different techniques that may be applied to the detection of deep fakes, which assists in mitigating the detrimental consequences that are caused by deep fakes". "According to the findings of the study, machine learning and deep learning models such as CNN and its variations, SVM, LR, and RF and their variants are quite helpful in discriminating between real and fraudulent information that is presented in the form of photographs and videos"[33, 34]. Xiaojun Li and his colleagues have developed "a CNN-based model that is capable of effectively recognizing videos that are dishonest by taking into consideration three distinct categories of characteristics. These categories are content features, uploader features, and environment features". "The findings of the trials showed that each of the three categories of features makes a significant contribution to the process of identifying fraudulent video footage"[35, 36].

Ammar Elhassan et al. provide "a detailed method and software implementation for identifying falsified videos made with Deep Learning technology"[37]. "When it comes to the creation of fake videos, this method depends on the exploitation of teeth and mouth movement as differentiating qualities" [38]. "Both of these characteristics continue to be very difficult to perfect. Separating the user video into frames and then preprocessing these frames with InceptionResNetV2 and LSTM is the basis for the technique that Priti Yadav proposes for automatically detecting deep fake". [107] This technique can be found in her presentation. The video of the user was broken up into individual frames so that this method could be devised. This method analyzes every video by making use of a convolutional LSTM system. Additionally, it helps in distinguishing deepfake faces that have been manipulated, which prevents real persons

from being defamed[39]. Kai Hong and Xiaoyu Du correlate the deepfake artifacts with some common noises as a strong tool to comprehend the unseen artifacts by using the Deepfake Artifact Discrepancy Detector (DADD) approach[40]. This method allows the authors to understand objects that are not visible to the naked eye. Njood and Abdul build a model that is capable of classifying the content (photos) of Instagram in order to recognize any potential dangers and fabricated shots. In order to build the model, we made use of deep learning strategies, notably the Convolutional Neural Network (CNN), the Alexnet network, and transfer learning using Alexnet [41]. If the adversary has complete or even partial knowledge of the detector, it is easy for them to circumvent the currently utilized methods that are regarded as the state-of-the-art for Deepfake detection[42]. Recently, there has been a lot of interest shown in authenticating digital images, music, and videos. This is owing to the fact that this content is exchanged via insecure media such as the internet and various forms of computer networks. Authentication solutions for digital photographs, music, and movies have garnered a lot of attention recently. The study on authentication tactics can be divided into two categories: those that use digital signatures, and those that use digital watermarking [43]. Each of these can be further subdivided into subcategories. Sulong Ge and his colleagues have come up with a solution for an end-to-end document picture watermarking system that makes use of the deep neural network. To provide a bit more clarity, an encoder and a decoder are developed in order to allow for the embedding and extraction of the watermark. A noise layer has been incorporated into the program in order to simulate the myriad of dangers that a user might face in the outside world. Cropout, dropout, gaussian blur, gaussian noise, resize, and JPEG compression are some of the attacks that fall under this category [44, 45]. Hong-Jyh et al. have come up with the idea of a wavelet-based watermark casting method in addition to a blind watermark retrieval method. Both of these methods have been offered. An adaptive watermark casting method is developed in order to first locate significant wavelet subbands and then select a couple of significant wavelet coefficients included within these subbands in order to insert watermarks. This method aims to detect significant wavelet subbands as quickly and efficiently as possible. This procedure is carried out numerous times until substantial wavelet subbands are discovered [46, 47].

The findings of the studies show that the embedded watermark is resilient against a wide variety of attacks, including signal processing and compression [48]. Salam has suggested a unique new strategy for the process of video watermarking that is founded on SLT, CT, and DCT. When it

comes to the most significant feature of the recommended method, which is the linkage between security, robustness, and imperceptibility, this has been accomplished by integrating the properties of all of the many transformation techniques that have been employed. This was done in order to achieve the aforementioned goal. The proposed method has demonstrated that it is useful and suitable for use in applications that require copyright protection as well as content authentication [49]. Cascading two well-known transformations, the discrete wavelet transform and the singular value decomposition, allowed Ali to propose an undetectable and robust method for audio watermarking[50, 51]. This method was based on the cascading of the transforms. The purpose of this method was to make it possible to secure one's intellectual property rights when digital audio is sent. Seyed and his colleagues have come up with a unique new approach for encrypting photos that is founded on the SHA-512 hashing algorithm [52, 53]. The core idea that lies at the heart of the method is to encrypt one half of the picture with the data from the other half of the image, while employing the other half of the image as the key. The algorithm is distinguished by its high level of security [54], which is also one of its distinctive qualities. Li Weng and his colleagues have developed a method for hashing films, which they have proposed. With this method, a hash value of 180 bits can be generated for movies of any running time. It may be deduced from the fact that the hash value is unaffected by common signal processing and suffers only very slight geometric distortion that the method is working effectively [55]. Applications that involve broadcast monitoring and database search could benefit from the utilization of a robust video hash function, as suggested by Baris et al. Within the context of this method, the 3D-DCT transform of video sequences is partitioned into low-frequency components. The work in question lends both uniqueness and tenacity to the video in question [56]. Despite this, these strategies are not the only ones that may be employed to fight the issue of deep fakes; there are many others. Therefore, it is extremely necessary to take part in awareness exercises and training in order to protect oneself from the early signs of a deepfake attack. As a consequence of this, the research presented here offers a number of potential solutions to the problem of deepfake [57]. In addition, we go over the processes involved in both the production of deep fakes and the identification of them.

3. How AI Deepfake Technology Works

Deepfakes are created by employing various methods of deep learning, such as generative adversarial networks, in order to digitally change and replicate a real person. Some examples of malicious behavior include imitating a manager's orders to staff, fabricating a message to a family that was in need of assistance, and spreading bogus embarrassing images of persons [58, 59].

Figure 1 : Worldwide Fraud Identification report

There have been an increasing number of incidents like this one as deep fakes get increasingly convincing and difficult to spot. In addition to this, it is now much simpler to produce them as a result of developments made to tools that were first developed for lawful objectives [60, 61]. One company, Microsoft, for instance, has recently introduced a new language translation service that can simulate the voice of a human speaking another language. However, the fact that these tools also make it simpler for malicious actors to interfere with corporate operations is a major cause for concern. Thankfully, the technologies that can detect deep fakes are also getting better. Deepfake detectors are able to search a video for telltale biometric indications, such as a

person's heartbeat or a voice made by human vocal organs as opposed to a synthesizer. Ironically, the same technologies that are being used to train and improve these detectors right now could one day be used to train the next generation of deepfakes as well [62, 63].

In the meanwhile, organizations can take a number of actions to prepare for the growing frequency and sophistication of deepfake attacks. These steps range from simple training of personnel to recognize symptoms of these attacks to the implementation of more advanced authentication and security tools and procedures [64, 65].

Deepfake attacks can be separated into four general categories, according to Robert Scalise, global managing partner of risk and cyber strategy at Tata Consultancy Services (TCS):

- Misinformation, disinformation and malinformation.
- Intellectual property infringement.
- Defamation.
- Pornography.
- Deepfake attack examples

According to Oded Vanunu, head of products vulnerability research at IT security vendor Check Point Software Technologies, the first significant deepfake attack occurred in 2019 [66]. This information comes from Vanunu[67]. Hackers successfully impersonated a phone request from a CEO, which led to a bank transfer of 243,000 dollars. Because of that event, financial institutions were required to be more watchful and to take additional safeguards, while cybercriminals continued to increase their level of sophistication [68].

In the year 2021, dishonest individuals successfully conned a bank manager into moving a staggering $35 million to a bogus bank account. "The criminals knew that the company was about to make an acquisition and would need to initiate a wire transfer to purchase the other company," said Gregory Hatcher, founder of the cybersecurity consultancy White Knight Labs. "The criminals knew that the company was about to make an acquisition and would need to initiate a wire transfer." The crooks carried out their plan with pinpoint accuracy, and the bank manager was able to transfer the monies [69].

Sam Crowther, founder and CEO of bot prevention and mitigation software vendor Kasada, stated that the most recent generation of bots are utilizing deepfake technology in order to avoid being discovered. "Deepfakes, when combined with bots, are becoming an increasingly dangerous threat to our social, business, and political systems," he explained. "Bots help spread fake news." Deep fakes are becoming increasingly convincing and accessible as a result of recent developments in artificial intelligence (AI) and malevolent automation, and they are disseminating misinformation on a scale that was previously unfathomable. For example, the pro-China propaganda operation known as Spamouflage makes use of bots to generate phony accounts, share deep bogus movies, and disseminate false material throughout many social media sites [70-72].

4. Deep Fake Detection

Deep fake detection is an area of research that is just entering its formative stages as 2018's first few months' progress. There are two distinct classifications of approaches to take [73, 74]. Biological signals: Several researches have explored abnormal movements in deep fake videos, such as a lack of blinking, facial deformities, and erratic movement. Among these anomalous actions is a lack of facial expression. These methods might be improved by making a few straightforward adjustments to the procedures involved in the production of the video, such as adding blinking [75, 76].

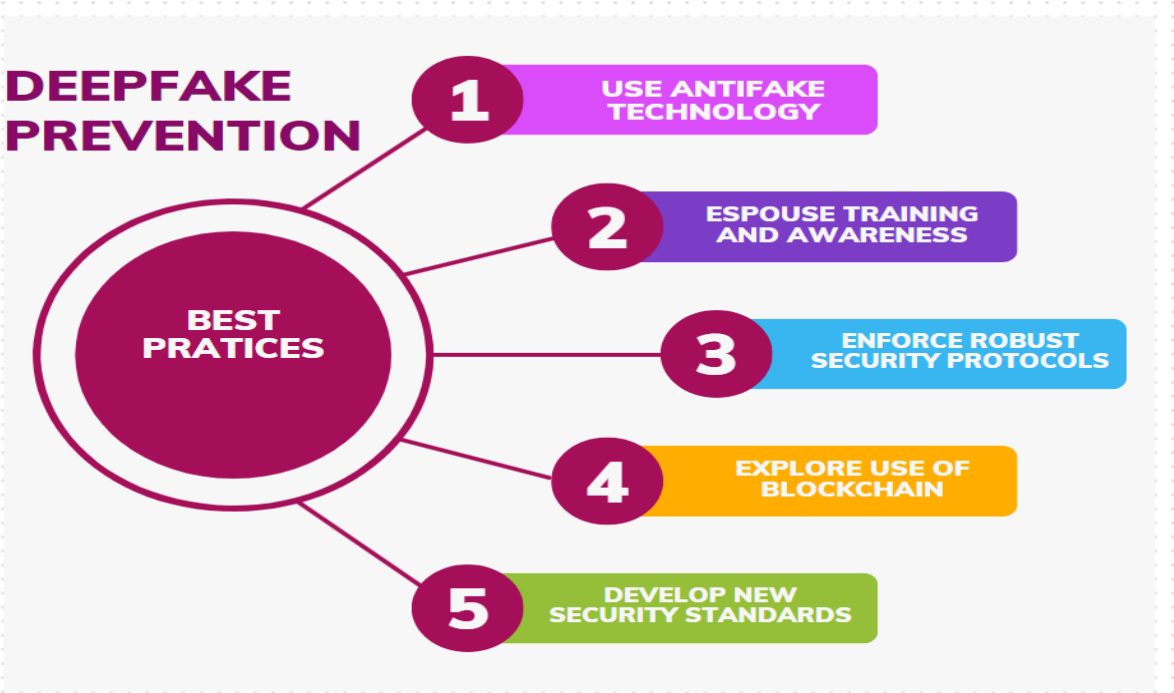

Figure 2 Deepfake prevention

Pixel Level Irregularities: There is a broader spectrum of research that extracts faces and uses various types of deep learning to target intra-frame or inter-frame inconsistencies. This research aims to address pixel level irregularities [77]. These researches are published in a number of scholarly journals, which can be accessed online [78-81]. Although many of these algorithms perform brilliantly on certain kinds of manipulations, they are unable to generalize to many and unknown forms of deep fakes, which is a quality that is needed for open-world detection and is missing from many of these techniques. None of the strategies that have been suggested for identifying deep fakes have yet been developed into an actual instrument that can be deployed for detection purposes in the real world. To the best of our knowledge, there has also been no research carried out on the topic of how to successfully develop such a tool for use by journalists [82].

5. Analyzing The Technology

There have already been a great number of deep fakes that have been successful. Despite this, there are very few, if any at all, specific variables that can be used to describe what constitutes a

good deep fake. The testing environment that we have constructed is meant to provide lucid details on the current state of deepfake technology as well as the picture material requirements for producing convincing fakes. Research projects are currently being carried out with the goal of determining the limits of the technology that is already available [83-85]. The findings of this research are determined by a wide range of criteria. The following criteria have been devised in order to evaluate whether or not these prerequisites have been satisfied:

- The total number of images in the collection
- The overall illumination conditions that are present
- The quantity and quality of the material that was used as a source
- The direction in which the source material was oriented;
- Differences in the characteristics of the face;
- Things that run into each other and overlap

5.1. The Possible Threats of Deep fakes

Deep fakes provide a huge threat to our society, political system, and the corporate sector for a variety of reasons, some of which are listed below: They impede citizen trust toward information provided by authorities; they threaten national security by spreading propaganda and interfering in elections; they put pressure on journalists who are already struggling to differentiate between real and fake news; and they raise cybersecurity issues for individuals and organizations [86, 87].

1) They impede citizen trust toward information provided by authorities.

2) They threaten national security by spreading propaganda and interfering in elections.

3) They put pressure on journalists who are already struggling to differentiate between real and fake news.

6. The Benefits of Deep fake Technology

The film industry, the educational media and digital communications industry, the gaming and entertainment industry, the healthcare and social media industries, the material science industry, and a variety of business fields such as the fashion and eCommerce industries all stand to benefit from the implementation of deepfake technology. The motion picture industry stands to gain in a

variety of different ways from the implementation of deepfake technology. For instance, it can be beneficial in the process of producing digital voices for actors who have lost their own due to sickness, or it can be helpful in the process of updating film footage rather than reshooting it. Both of these processes are examples of when this technology can be used. When it comes to post-production, filmmakers will have the ability to make use of advanced face editing software in addition to special effects software. Additionally, the quality of amateur videos will be able to be improved to a level that is comparable to that of videos created by professionals. In addition to this, they will be able to produce new movies that star actors who have already passed away. In addition, the Deepfake technology makes it possible to create automatic and convincing voice dubbing for films in any language. This opens the door for a far larger range of individuals to find enjoyment in watching films and other types of instructional media. An educational campaign that featured David Beckham in 2019 and was targeted at increasing awareness about malaria was able to break over language barriers by using visual and voice-altering technologies to make him appear to speak various languages. The overall goal of the advertising was to raise awareness about malaria [88-91].

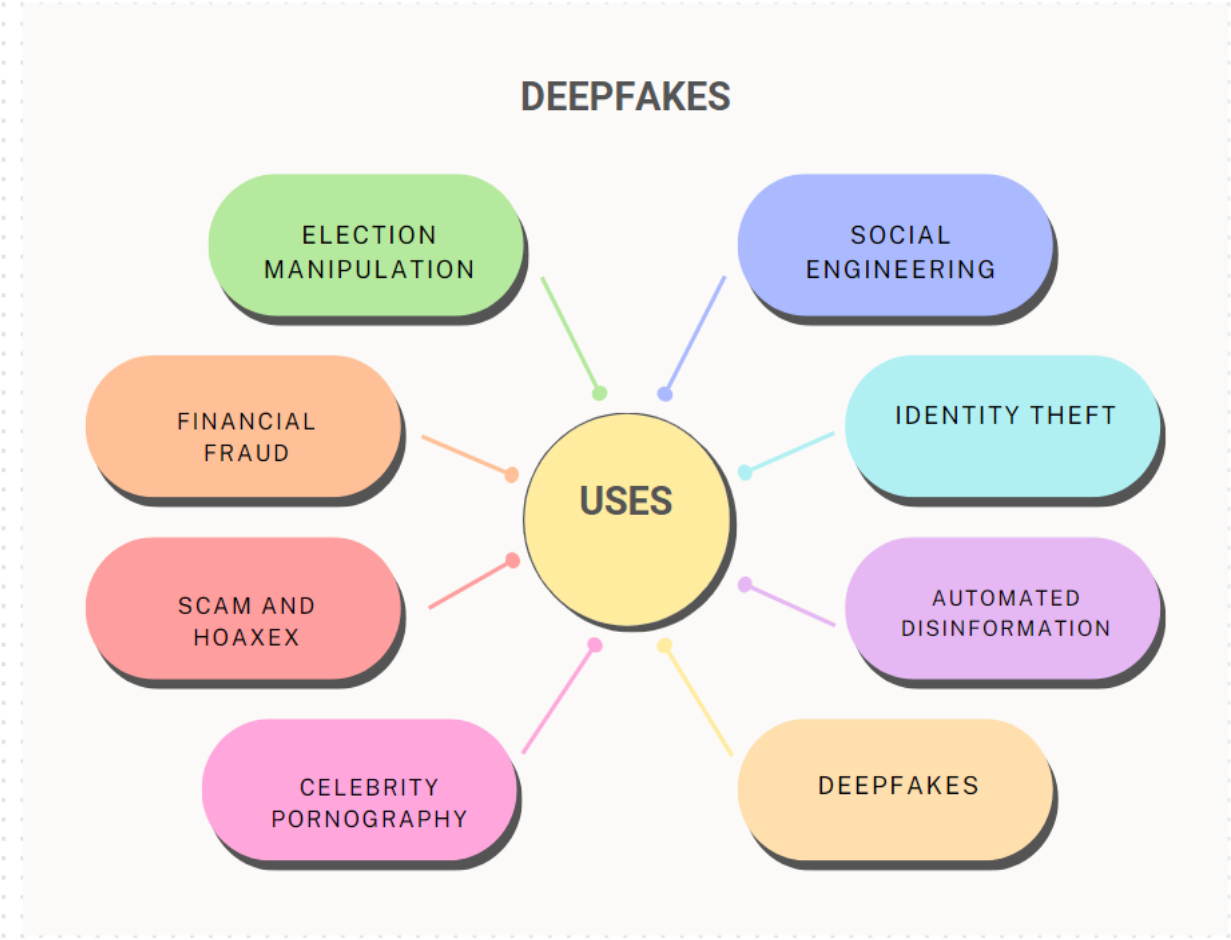

Figure 3 Deepfake uses

Similarly, the deepfake technology may translate speech while concurrently modifying face and lip motions during video conference calls. This can increase eye contact and provide the impression that everyone is speaking the same language. This has the potential to eliminate any linguistic obstacles that may arise during these calls. The underlying technology that enables deep fakes makes it possible for online games and virtual chat worlds to have better telepresence, natural-sounding and –looking smart assistants, and digital doubles of actual people. This helps to foster the growth of human connections and interactions that are more positive and constructive within the digital world. Along these same lines, it's possible that advances in technology could have positive implications in the fields of social work and medicine. Deep fakes can help people cope with the sadness that comes with the loss of a loved one by digitally "reviving" a deceased friend or loved one. This can be a comforting experience for those who have suffered such a loss. This may make it possible for someone who is grieving to finally say

goodbye to their loved one who has passed away. In addition to this, it may be able to digitally replace a lost limb on an amputee or enable transgender people to view themselves more properly in the gender identity that corresponds to their desired gender [92-95].

Patients diagnosed with Alzheimer's disease could potentially benefit from the use of deep fake technology, which would enable them to interact with a younger version of themselves that they may remember. Researchers are also investigating GANs for their potential to be employed in the synthesis of virtual chemical compounds, which would speed up the process of scientific and medical discovery. This would be beneficial for a number of reasons. GANs are being used to search for and find X-ray aberrations. Because of the significant ways in which it has the potential to change eCommerce and advertising, businesses are captivated by the idea of brand-applicable deep fake technology. For instance, fashion companies may use "supermodels" who are not genuinely supermodels in order to display their wares on models with a variety of skin tones, heights, and weights. This is done in order to appeal to a wider audience. The technology enables virtual fitting so that customers can see how an outfit will look on them before making a purchase, and it can generate targeted advertisements for fashion that change depending on the time of day, the weather, and the person viewing them (FRB02; FRB07). Additionally, deep fakes make it possible to create highly personalized content that transforms customers into models. The technology enables users to not only make digital clones of themselves and have these personal avatars travel with them across stores, but it also enables users to try on a bridal gown or suit in digital form and then virtually experience a wedding venue. In addition, the technology enables users to build digital clones of themselves and have these personal avatars travel with them across stores. People are able to make digital clones of themselves and have these personal avatars travel with them across stores thanks to a new technology that allows consumers to try on items online. This technology also enables people to create digital clones of themselves and have these personal avatars travel with them across stores. In addition to this, AI is able to provide a variety of artificial voices that can be utilized to differentiate between companies and their products, which simplifies the process of branding [96, 97].

6. Preventing Deepfake Attacks

Phishing attacks can easily be launched against users, and it will be significantly more difficult to detect deepfake phishing attempts. Training in cybersecurity awareness is one of the most fundamental aspects of any security program, and those that don't contain it are deficient. Be sure to include information on how to identify a fake when writing your article [98-100].

This is a lot less complicated than you could possibly think it is. The technology that makes these assaults possible is efficient, but it is not infallible by any means. During the course of a webinar, Raymond Lee, who is the Chief Executive Officer of FakeNet.AI, and Etay Maor, who is the Senior Director of Security Strategy at Cato Networks, highlighted how tough it is to improve facial characteristics. In particular, they concentrated on how difficult it is to produce an exact duplicate of an individual's eyes. If the eyes look funny or the movement of the facial features looks off, there is a good chance that the image has been edited in some way [101].

The highest possible standards, along with an utter lack of faith in anyone else. Verify all that you think you see. Verify the message's origins using a minimum of two different methods. Conduct a search for images and make an effort to locate the original if at all possible. In spite of the significance of technology safeguards, there are also alternative methods available for protecting against Deepfake videos. Surprisingly effective against Deepfake are even the most fundamental security techniques [102, 103]. For instance, the incorporation of automated checks into any process involving the distribution of funds would have significantly lowered the risk of falling victim to frauds like Deepfake and others like it. In addition to that:

- It is important that you let your friends and family know about the hazards of deepfake as well as how it works. Gain the ability to spot a Deepfake and instruct others on how to do the same. Make it a priority to stay informed on the latest news and consult sources of information that you can trust [104].
- "Trust, but verify" is an essential core practice that should be put into place. It is hard to guarantee that you will not be tricked, but you can prevent many potential problems by approaching voicemails and videos with a fair amount of suspicion. Keep in mind that if hackers start using Deepfake to get into household and corporate networks, the most important thing you can do to defend yourself is to follow fundamental cyber-security best practices. This is the most critical thing you can do to protect yourself in the event that this happens. If you use strong,

unique passwords for each account, you can assure that even if one network or service is compromised, it won't automatically affect the others. Additionally, doing regular backups protects your data from ransomware and enables you to recover data that has been deleted. Nobody wants Facebook hackers to be able to access their other online profiles and do anything they want with them. Utilize a dependable security suite such as Kaspersky Total Security to shield your personal computer, wireless network at home, and mobile device from threats that can be found online. With the Virtual Private Network (VPN) that is included in this package, you will be able to protect your computer and camera from malicious software and hackers. Because the use of deep fakes as an attack vector has just recently begun, cybersecurity teams still have time to create countermeasures before the methods that can be used to counter them grow more complex. As a direct consequence of this, you should now have one fewer thing to stress about [105, 106].

Conclusions:

The advancement of computer vision and deep learning technologies has resulted in the introduction of rapidly developing methods that enable anyone to generate films and photographs that are both fake and extremely lifelike. These methods have been made possible as a result of the rapid expansion of these technologies. These types of technologies are typically referred to collectively as deepfake methodologies. Using the deepfake breakthrough, it is now possible to do face alteration in both videos and still images with a high level of realism. There has been a significant increase in the circulation of deepfake recordings across the internet, the vast majority of which target politicians or celebrity individuals. On the other hand, the research has shown a number of potential solutions that can be utilized to address the problems that are caused by deepfake. In this piece, we carry out a review by examining and comparing two different types of deepfake tools and models: (1) the significant academic contributions in the field of deepfake models, and (2) the commonly used deepfake tools. In addition to that, we have developed two distinct taxonomies for the deepfake models and tools. These models and tools are also compared with one another based on the algorithms that lie beneath them, the datasets that they

have used, and their levels of accuracy. In addition to that, a number of obstacles and unresolved problems have been found.

COMPETING INTERESTS:

Authors have declared that they have no known competing financial interests OR non-financial interests OR personal relationships that could have appeared to influence the work reported in this paper.

References

1. *Agarwal S, Farid H (2021) Detecting deep-fake videos from aural and oral dynamics. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 981–989, https://doi.org/10.1109/CVPRW53098.2021.00109.*
2. *Agarwal S, Farid H, El-Gaaly T, et al. (2020a) Detecting deep-fake videos from appearance and behavior. In: 2020 IEEE International Workshop on Information Forensics and Security, WIFS 2020, https://doi.org/10.1109/WIFS49906.2020.9360904.*
3. *Agarwal S, Farid H, Fried O, et al. (2020b) Detecting deep-fake videos from phoneme-viseme mismatches. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 2814–2822, https://doi.org/10.1109/CVPRW50498.2020.00338.*
4. *Agarwal S, Farid H, Gu Y, et al. (2019a) Protecting world leaders against deep fakes. pp 38–45, conference of 32nd IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, CVPRW 2019 ; Conference Date: 16 June 2019 Through 20 June 2019; Conference Code:159074.*
5. *Agarwal S, Farid H, Gu Y, et al. (2019b) Protecting world leaders against deep fakes. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 38–45.*
6. *Agarwal H, Singh A, Rajeswari D (2021) Deepfake detection using svm. In: Proceedings of the 2nd International Conference on Electronics and Sustainable Communication Systems, ICESC 2021, pp 1245–1249, https://doi.org/10.1109/ICESC51422.2021.9532627.*
7. *Agrawal R, Sharma D (2021) A survey on video-based fake news detection techniques. In: Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021, pp 663–669, https://doi.org/10.1109/INDIACom51348.2021.00117.*
8. *Ahmed M, Miah M, Bhowmik A, et al. (2021) Awareness to deepfake: A resistance mechanism to deepfake. In: 2021 International Congress of Advanced Technology and Engineering, ICOTEN 2021, https://doi.org/10.1109/ICOTEN52080.2021.9493549.*

9. *Ajoy A, Mahindrakar C, Gowrish D, et al. (2021) Deepfake detection using a frame based approach involving cnn. In: Proceedings of the 3rd International Conference on Inventive Research in Computing Applications, ICIRCA 2021, pp 1329–1333, https://doi.org/10.1109/ICIRCA51532.2021.9544734.*
10. *Alattar A, Sharma R, Scriven J (2020) A system for mitigating the problem of deepfake news videos using watermarking. In: Adnan M. A.M. GGNasir D. N.D. (ed) IS and T International Symposium on Electronic Imaging Science and Technology, https://doi.org/10.2352/ISSN.2470-1173.2020.4.MWSF-117.*
11. *Aliman NM, Kester L (2020) Malicious design in aivr, falsehood and cybersecurity-oriented immersive defenses. In: Proceedings - 2020 IEEE International Conference on Artificial Intelligence and Virtual Reality, AIVR 2020, pp 130–137, https://doi.org/10.1109/AIVR50618.2020.00031.*
12. *Amerini I, Caldelli R (2020) Exploiting prediction error inconsistencies through lstm-based classifiers to detect deepfake videos. In: IH and MMSec 2020 - Proceedings of the 2020 ACM Workshop on Information Hiding and Multimedia Security, pp 97–102, https://doi.org/10.1145/3369412.3395070.*
13. *Amerini I, Galteri L, Caldelli R, et al. (2019a) Deepfake video detection through optical flow based cnn. In: 2019 IEEE/CVF International Conference on Computer Vision Workshop (ICCVW). IEEE Computer Society, Los Alamitos, CA, USA, pp 1205–1207, https://doi.org/10.1109/ICCVW.2019.00152, https://doi.ieeecomputersociety.org/10.1109/ICCVW.2019.00152.*
14. *Amerini I, Galteri L, Caldelli R, et al. (2019b) Deepfake video detection through optical flow based cnn. In: Proceedings - 2019 International Conference on Computer Vision Workshop, ICCVW 2019, pp 1205–1207, https://doi.org/10.1109/ICCVW.2019.00152.*
15. *Bailer W, Thallinger G, Backfried G, et al. (2021) Challenges for automatic detection of fake news related to migration : Invited paper. In: Proceedings - 2021 IEEE International Conference on Cognitive and Computational Aspects of Situation Management, CogSIMA 2021, pp 133–138, https://doi.org/10.1109/CogSIMA51574.2021.9475929.*
16. *Bondi L, Daniele Cannas E, Bestagini P, et al. (2020) Training strategies and data augmentations in cnn-based deepfake video detection. In: 2020 IEEE International Workshop on Information Forensics and Security, WIFS 2020, https://doi.org/10.1109/WIFS49906.2020.9360901.*
17. *Bonettini N, Bondi L, Cannas E, et al. (2020) Video face manipulation detection through ensemble of cnns. In: Proceedings - International Conference on Pattern Recognition, pp 5012–5019, https://doi.org/10.1109/ICPR48806.2021.9412711.*
18. *Bose A, Aarabi P (2019) Virtual fakes: Deepfakes for virtual reality. In: IEEE 21st International Workshop on Multimedia Signal Processing, MMSP 2019, https://doi.org/10.1109/MMSP.2019.8901744.*
19. *Burroughs S, Gokaraju B, Roy K, et al. (2020) Deepfakes detection in videos using feature engineering techniques in deep learning convolution neural network frameworks. In: Proceedings - Applied Imagery Pattern Recognition Workshop, https://doi.org/10.1109/AIPR50011.2020.9425347.*
20. *Carlini N, Farid H (2020) Evading deepfake-image detectors with white-and black-box attacks. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 2804–2813, https://doi.org/10.1109/CVPRW50498.2020.00337.*
21. *Chang X, Wu J, Yang T, et al. (2020) Deepfake face image detection based on improved vgg convolutional neural network. In: Fu J. SJ (eds). Chinese Control Conference, CCC, pp 7252–7256, https://doi.org/10.23919/CCC50068.2020.9189596.*

22. *Chen P, Liu J, Liang T, et al. (2020) Fsspotter: Spotting face-swapped video by spatial and temporal clues. In: Proceedings - IEEE International Conference on Multimedia and Expo, https://doi.org/10.1109/ICME46284.2020.9102914.*
23. *Chintha A, Rao A, Sohrawardi S, et al. (2020a) Leveraging edges and optical flow on faces for deepfake detection. In: IJCB 2020 - IEEE/IAPR International Joint Conference on Biometrics, https://doi.org/10.1109/IJCB48548.2020.9304936.*
24. *Chowdhury S, Lubna J (2020) Review on deep fake: A looming technological threat. In: 2020 11th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2020, https://doi.org/10.1109/ICCCNT49239.2020.9225630.*
25. *Chugh K, Gupta P, Dhall A, et al. (2020) Not made for each other- audio-visual dissonance-based deepfake detection and localization. In: MM 2020 - Proceedings of the 28th ACM International Conference on Multimedia, pp 439–447, https://doi.org/10.1145/3394171.3413700.*
26. *Ciftci U, Demir I, Yin L (2020) How do the hearts of deep fakes beat? deep fake source detection via interpreting residuals with biological signals. In: IJCB 2020 - IEEE/IAPR International Joint Conference on Biometrics, https://doi.org/10.1109/IJCB48548.2020.9304909.*
27. *Cozzolino D, Poggi G, Verdoliva L (2019) Extracting camera-based fingerprints for video forensics. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 130–137.*
28. *Dang H, Liu F, Stehouwer J, et al. (2020) On the detection of digital face manipulation. In: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp 5780–5789, https://doi.org/10.1109/CVPR42600.2020.00582.*
29. *Gu Y, Zhao X, Gong C, et al. (2021) Deepfake video detection using audio-visual consistency. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12617 LNCS:168–180. https://doi.org/10.1007/978-3-030-69449-4_13.*
30. *Han J, Gevers T (2021) Mmd based discriminative learning for face forgery detection. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12626 LNCS:121–136. https://doi.org/10.1007/978-3-030-69541-5_8.*
31. *Hänska M (2021). Communication against domination: Ideas of justice from the printing press to algorithmic media. https://doi.org/10.4324/9780429280795.*
32. *Hartmann K, Giles K (2020) The next generation of cyber-enabled information warfare. In: International Conference on Cyber Conflict, CYCON, pp 233–250, https://doi.org/10.23919/CyCon49761.2020.9131716.*
33. *Hazan S (2020) Deep fake and cultural truth - custodians of cultural heritage in the age of a digital reproduction. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12215 LNCS:65–80. https://doi.org/10.1007/978-3-030-50267-6_6.*
34. *Hernandez-Ortega J, Tolosana R, Fierrez J, et al. (2021) Deepfakeson-phys: Deepfakes detection based on heart rate estimation. In: CEUR Workshop Proceedings.*
35. *Hongmeng Z, Zhiqiang Z, Lei S, et al. (2020) A detection method for deepfake hard compressed videos based on super-resolution reconstruction using cnn. In: ACM International Conference Proceeding Series, pp 98–103, https://doi.org/10.1145/3409501.3409542.*
36. *Hosier B, Stamm M (2020) Detecting video speed manipulation. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 2860–2869, https://doi.org/10.1109/CVPRW50498.2020.00343.*
37. *Hosler B, Salvi D, Murray A, et al. (2021) Do deepfakes feel emotions? a semantic approach to detecting deepfakes via emotional inconsistencies. In: IEEE Computer Society Conference on*

Computer Vision and Pattern Recognition Workshops, pp 1013–1022, https://doi.org/10.1109/CVPRW53098.2021.00112.

38. *Houde S, Liao V, Martino J, et al. (2020) Business (mis)use cases of generative ai. In: Geyer W. SSMKhazaeni Y. (ed) CEUR Workshop Proceedings.*
39. *Huang R, Fang F, Nguyen H, et al. (2020a) Security of facial forensics models against adversarial attacks. In: Proceedings - International Conference on Image Processing, ICIP, pp 2236–2240, https://doi.org/10.1109/ICIP40778.2020.9190678.*
40. *Huang Y, Juefei-Xu F, Wang R, et al. (2020b) Fakepolisher: Making deepfakes more detection-evasive by shallow reconstruction. In: MM 2020 - Proceedings of the 28th ACM International Conference on Multimedia, pp 1217–1226, https://doi.org/10.1145/3394171.3413732.*
41. *Huber E, Pospisil B, Haidegger W (2021) Modus operandi in fake news : Invited paper. In: Proceedings - 2021 IEEE International Conference on Cognitive and Computational Aspects of Situation Management, CogSIMA 2021, pp 127–132, https://doi.org/10.1109/CogSIMA51574.2021.9475926.*
42. *Hu S, Li Y, Lyu S (2021) Exposing gan-generated faces using inconsistent corneal specular highlights. In: ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, pp 2500–2504, https://doi.org/10.1109/ICASSP39728.2021.9414582.*
43. *Hussain S, Neekhara P, Jere M, et al. (2021) Adversarial deepfakes: Evaluating vulnerability of deepfake detectors to adversarial examples. In: Proceedings - 2021 IEEE Winter Conference on Applications of Computer Vision, WACV 2021, pp 3347–3356, https://doi.org/10.1109/WACV48630.2021.00339.*
44. *Ivanov N, Arzhskov A, Ivanenko V (2020) Combining deep learning and super-resolution algorithms for deep fake detection. In: S. S (ed) Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020, pp 326–328, https://doi.org/10.1109/EIConRus49466.2020.9039498.*
45. *Jafar M, Ababneh M, Al-Zoube M, et al. (2020) Digital forensics and analysis of deepfake videos. In: 2020 11th International Conference on Information and Communication Systems, ICICS 2020, pp 53–58, https://doi.org/10.1109/ICICS49469.2020.239493.*
46. *Jeong Y, Choi J, Kim D, et al. (2021) Dofnet: Depth of field difference learning for detecting image forgery. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12627 LNCS:83–100. https://doi.org/10.1007/978-3-030-69544-6_6.*
47. *Jiang L, Li R, Wu W, et al. (2020) Deeperforensics-1.0: A large-scale dataset for real-world face forgery detection. In: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp 2886–2895, https://doi.org/10.1109/CVPR42600.2020.00296.*
48. *Jiang J, Wang B, Li B, et al. (2021) Practical face swapping detection based on identity spatial constraints. In: 2021 IEEE International Joint Conference on Biometrics, IJCB 2021, https://doi.org/10.1109/IJCB52358.2021.9484396.*
49. *Kang M, Park J (2020) Contragan: Contrastive learning for conditional image generation. In: Advances in Neural Information Processing Systems.*
50. *Katarya R, Lal A (2020) A study on combating emerging threat of deepfake weaponization. In: Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020, pp 485–490, https://doi.org/10.1109/I-SMAC49090.2020.9243588.*
51. *Kawa P, Syga P (2021) Verify it yourself: A note on activation functions' influence on fast deepfake detection. In: di Vimercati S.De.C. SP (ed) Proceedings of the 18th International Conference on Security and Cryptography, SECRYPT 2021, pp 779–784, https://doi.org/10.5220/0010581707790784.*

52. *Khalid H, Woo S (2020) Oc-fakedect: Classifying deepfakes using one-class variational autoencoder. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 2794–2803, https://doi.org/10.1109/CVPRW50498.2020.00336.*
53. *Khalil H, Maged S (2021) Deepfakes creation and detection using deep learning. In: 2021 International Mobile, Intelligent, and Ubiquitous Computing Conference, MIUCC 2021, pp 24–27, https://doi.org/10.1109/MIUCC52538.2021.9447642.*
54. *Kharbat F, Elamsy T, Mahmoud A, et al. (2019) Image feature detectors for deepfake video detection. In: Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA, https://doi.org/10.1109/AICCSA47632.2019.9035360.*
55. *Khodabakhsh A, Loiselle H (2020) Action-independent generalized behavioral identity descriptors for look-alike recognition in videos. In: BIOSIG 2020 - Proceedings of the 19th International Conference of the Biometrics Special Interest Group.*
56. *Ki Chan C, Kumar V, Delaney S, et al. (2020) Combating deepfakes: Multi-lstm and blockchain as proof of authenticity for digital media. In: 2020 IEEE / ITU International Conference on Artificial Intelligence for Good, AI4G 2020, pp 55–62, https://doi.org/10.1109/AI4G50087.2020.9311067.*
57. *Kim M, Tariq S, Woo S (2021b) Fretal: Generalizing deepfake detection using knowledge distillation and representation learning. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 1001–1012, https://doi.org/10.1109/CVPRW53098.2021.00111.*
58. *Demir I, Ciftci U (2021) Where do deep fakes look? synthetic face detection via gaze tracking. In: S.N. S (eds) Eye Tracking Research and Applications Symposium (ETRA), https://doi.org/10.1145/3448017.3457387.*
59. *Du C, Duong L, Trung H, et al. (2020a) Efficient-frequency: A hybrid visual forensic framework for facial forgery detection. In: 2020 IEEE Symposium Series on Computational Intelligence, SSCI 2020, pp 707–712, https://doi.org/10.1109/SSCI47803.2020.9308305.*
60. *Du M, Pentyala S, Li Y, et al. (2020b) Towards generalizable deepfake detection with locality-aware autoencoder. In: International Conference on Information and Knowledge Management, Proceedings, pp 325–334, https://doi.org/10.1145/3340531.3411892.*
61. *El Rai M, Al Ahmad H, Gouda O, et al. (2020) Fighting deepfake by residual noise using convolutional neural networks. In: 2020 3rd International Conference on Signal Processing and Information Security, ICSPIS 2020, https://doi.org/10.1109/ICSPIS51252.2020.9340138.*
62. *England P, Malvar H, Horvitz E, et al. (2021) Amp: Authentication of media via provenance. In: MMSys 2021 - Proceedings of the 2021 Multimedia Systems Conference, pp 109–121, https://doi.org/10.1145/3458305.3459599.*
63. *Fazheng W, Yanwei Y, Shuiyuan D, et al. (2021) Research on location of chinese handwritten signature based on efficientdet. In: 2021 IEEE 4th International Conference on Big Data and Artificial Intelligence, BDAI 2021, pp 192–198, https://doi.org/10.1109/BDAI52447.2021.9515222.*
64. *Fernandes S, Jha S (2020) Adversarial attack on deepfake detection using rl based texture patches. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12535 LNCS:220–235. https://doi.org/10.1007/978-3-030-66415-2_14.*
65. *Fernandes S, Raj S, Ewetz R, et al. (2020) Detecting deepfake videos using attribution-based confidence metric. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 1250–1259, https://doi.org/10.1109/CVPRW50498.2020.00162.*
66. *Frank J, Eisenhofer T, Schönherr L, et al. (2020) Leveraging frequency analysis for deep fake image recognition. In: Daume H. SA (eds) 37th International Conference on Machine Learning, ICML 2020, pp 3205–3216.*

67. *Frick R, Zmudzinski S, Steinebach M (2021) Detecting deepfakes with haralick's texture properties. In: Adnan M. A.M. GGNasir D. N.D. (eds) IS and T International Symposium on Electronic Imaging Science and Technology, https://doi.org/10.2352/ISSN.2470-1173.2021.4.MWSF-271.*
68. *Fung S, Lu X, Zhang C, et al. (2021) Deepfakeucl: Deepfake detection via unsupervised contrastive learning. In: Proceedings of the International Joint Conference on Neural Networks, https://doi.org/10.1109/IJCNN52387.2021.9534089.*
69. *Gandhi A, Jain S (2020) Adversarial perturbations fool deepfake detectors. In: Proceedings of the International Joint Conference on Neural Networks, https://doi.org/10.1109/IJCNN48605.2020.9207034.*
70. *Goebel M, Nataraj L, Nanjundaswamy T, et al. (2021) Detection, attribution and localization of gan generated images. In: Adnan M. A.M. GGNasir D. N.D. (eds) IS and T International Symposium on Electronic Imaging Science and Technology, https://doi.org/10.2352/ISSN.2470-1173.2021.4.MWSF-276.*
71. *Guan H, Kozak M, Robertson E, et al. (2019) Mfc datasets: Large-scale benchmark datasets for media forensic challenge evaluation. In: Proceedings - 2019 IEEE Winter Conference on Applications of Computer Vision Workshops, WACVW 2019, pp 63–72, https://doi.org/10.1109/WACVW.2019.00018.*
72. *Gupta P, Chugh K, Dhall A, et al. (2020) The eyes know it: Fakeet- an eye-tracking database to understand deepfake perception. In: ICMI 2020 - Proceedings of the 2020 International Conference on Multimodal Interaction, pp 519–527, https://doi.org/10.1145/3382507.3418857.*
73. *Korshunov P, Marcel S (2019) Vulnerability assessment and detection of deepfake videos. In: 2019 International Conference on Biometrics, ICB 2019, https://doi.org/10.1109/ICB45273.2019.8987375.*
74. *Korshunov P, Marcel S (2021) Subjective and objective evaluation of deepfake videos. In: ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, pp 2510–2514, https://doi.org/10.1109/ICASSP39728.2021.9414258.*
75. *Kubanek M, Bartłomiejczyk K, Bobulski J (2021) Detection of artificial images and changes in real images using convolutional neural networks. Advances in Intelligent Systems and Computing 1267 AISC:197–207. https://doi.org/10.1007/978-3-030-57805-3_19.*
76. *Kukanov I, Karttunen J, Sillanpaa H, et al. (2020) Cost sensitive optimization of deepfake detector. In: 2020 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference, APSIPA ASC 2020 - Proceedings, pp 1300–1303.*
77. *Lewis J, Toubal I, Chen H, et al. (2020) Deepfake video detection based on spatial, spectral, and temporal inconsistencies using multimodal deep learning. In: Proceedings - Applied Imagery Pattern Recognition Workshop, https://doi.org/10.1109/AIPR50011.2020.9425167.*
78. *Liang T, Chen P, Zhou G, et al. (2020) Sdhf: Spotting deepfakes with hierarchical features. In: Alamaniotis M. PS (ed) Proceedings - International Conference on Tools with Artificial Intelligence, ICTAI, pp 675–680, https://doi.org/10.1109/ICTAI50040.2020.00108.*
79. *Liang J, Deng W (2021) Identifying rhythmic patterns for face forgery detection and categorization. In: 2021 IEEE International Joint Conference on Biometrics, IJCB 2021, https://doi.org/10.1109/IJCB52358.2021.9484400.*
80. *Li L, Bao J, Zhang T, et al. (2020b) Face x-ray for more general face forgery detection. In: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp 5000–5009, https://doi.org/10.1109/CVPR42600.2020.00505.*
81. *Li M, Liu B, Hu Y, et al. (2020c) Exposing deepfake videos by tracking eye movements. In: Proceedings - International Conference on Pattern Recognition, pp 5184–5189, https://doi.org/10.1109/ICPR48806.2021.9413139.*

82. *Li M, Liu B, Hu Y, et al. (2021a) Deepfake detection using robust spatial and temporal features from facial landmarks. In: Proceedings - 9th International Workshop on Biometrics and Forensics, IWBF 2021, https://doi.org/10.1109/IWBF50991.2021.9465076.*
83. *Li Y, Lyu S (2021) Obstructing deepfakes by disrupting face detection and facial landmarks extraction. Advances in Computer Vision and Pattern Recognition pp 247–267. https://doi.org/10.1007/978-3-030-74697-1_12.*
84. *Ling H, Huang J, Zhao C, et al. (2021) Learning diverse local patterns for deepfake detection with image-level supervision. In: Proceedings of the International Joint Conference on Neural Networks, https://doi.org/10.1109/IJCNN52387.2021.9533912.*
85. *Li W, Wang Q, Wang R, et al. (2021b) Exposing deepfakes via localizing the manipulated artifacts. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12919 LNCS:3–20. https://doi.org/10.1007/978-3-030-88052-1_1.*
86. *Li Y, Yang X, Sun P, et al. (2020d) Celeb-df: A large-scale challenging dataset for deepfake forensics. pp 3204–3213, https://doi.org/10.1109/CVPR42600.2020.00327, conference of 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR 2020 ; Conference Date: 14 June 2020 Through 19 June 2020; Conference Code:162261.*
87. *Li Y, Yang X, Sun P, et al. (2020e) Celeb-df: A large-scale challenging dataset for deepfake forensics. In: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, pp 3204–3213, https://doi.org/10.1109/CVPR42600.2020.00327.*
88. *Lomnitz M, Hampel-Arias Z, Sandesara V, et al. (2020) Multimodal approach for deepfake detection. In: Proceedings - Applied Imagery Pattern Recognition Workshop, https://doi.org/10.1109/AIPR50011.2020.9425192.*
89. *Lv L (2021) Smart watermark to defend against deepfake image manipulation. In: 2021 IEEE 6th International Conference on Computer and Communication Systems, ICCCS 2021, pp 380–384, https://doi.org/10.1109/ICCCS52626.2021.9449287.*
90. *Lyu S (2020) Deepfake detection: Current challenges and next steps. In: 2020 IEEE International Conference on Multimedia and Expo Workshops, ICMEW 2020, https://doi.org/10.1109/ICMEW46912.2020.9105991.*
91. *Maksutov A, Morozov V, Lavrenov A, et al. (2020) Methods of deepfake detection based on machine learning. In: S. S (ed) Proceedings of the 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, EIConRus 2020, pp 408–411, https://doi.org/10.1109/EIConRus49466.2020.9039057.*
92. *Malolan B, Parekh A, Kazi F (2020) Explainable deep-fake detection using visual interpretability methods. In: Proceedings - 3rd International Conference on Information and Computer Technologies, ICICT 2020, pp 289–293, https://doi.org/10.1109/ICICT50521.2020.00051.*
93. *Masi I, Killekar A, Mascarenhas R, et al. (2020) Two-branch recurrent network for isolating deepfakes in videos. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 12352 LNCS:667–684. https://doi.org/10.1007/978-3-030-58571-6_39.*
94. *Masood M, Nawaz M, Javed A, et al. (2021) Classification of deepfake videos using pre-trained convolutional neural networks. In: 2021 International Conference on Digital Futures and Transformative Technologies, ICoDT2 2021, https://doi.org/10.1109/ICoDT252288.2021.9441519.*
95. *Matern F, Riess C, Stamminger M (2019a) Exploiting visual artifacts to expose deepfakes and face manipulations. pp 83–92, https://doi.org/10.1109/WACVW.2019.00020, conference of 19th IEEE Winter Conference on Applications of Computer Vision Workshops, WACVW 2019 ; Conference Date: 7 January 2019 Through 11 January 2019; Conference Code:145024.*

96. *Matern F, Riess C, Stamminger M (2019b) Exploiting visual artifacts to expose deepfakes and face manipulations. In: Proceedings - 2019 IEEE Winter Conference on Applications of Computer Vision Workshops, WACVW 2019, pp 83–92, https://doi.org/10.1109/WACVW.2019.00020.*
97. *Mcglynn C, Johnson K (2021) Cyberflashing: Recognising Harms, Reforming Laws.*
98. *Medoff N, B.K. K (2021) Interconnected by the internet. https://doi.org/10.4324/9781003020721-5.*
99. *Megahed A, Han Q (2020) Face2face manipulation detection based on histogram of oriented gradients. In: Proceedings - 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2020, pp 1260–1267, https://doi.org/10.1109/TrustCom50675.2020.00169.*
100. *Megías D, Kuribayashi M, Rosales A, et al. (2021) Dissimilar: Towards fake news detection using information hiding, signal processing and machine learning. In: ACM International Conference Proceeding Series, https://doi.org/10.1145/3465481.3470088.*
101. *Mitra A, Mohanty S, Corcoran P, et al. (2020) A novel machine learning based method for deepfake video detection in social media. In: Proceedings - 2020 6th IEEE International Symposium on Smart Electronic Systems, iSES 2020, pp 91–96, https://doi.org/10.1109/iSES50453.2020.00031.*
102. *Mittal T, Bhattacharya U, Chandra R, et al. (2020b) Emotions don't lie: An audio-visual deepfake detection method using affective cues. In: MM 2020 - Proceedings of the 28th ACM International Conference on Multimedia, pp 2823–2832, https://doi.org/10.1145/3394171.3413570.*
103. *Mittal H, Saraswat M, Bansal J, et al. (2020a) Fake-face image classification using improved quantum-inspired evolutionary-based feature selection method. In: 2020 IEEE Symposium Series on Computational Intelligence, SSCI 2020, pp 989–995, https://doi.org/10.1109/SSCI47803.2020.9308337.*
104. *Montserrat D, Hao H, Yarlagadda S, et al. (2020) Deepfakes detection with automatic face weighting. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops, pp 2851–2859, https://doi.org/10.1109/CVPRW50498.2020.00342.*
105. *Nasar B, Sajini T, Lason E (2020) Deepfake detection in media files - audios, images and videos. In: 2020 IEEE Recent Advances in Intelligent Computational Systems, RAICS 2020, pp 74–79, https://doi.org/10.1109/RAICS51191.2020.9332516.*
106. *Nguyen H, Derakhshani R (2020) Eyebrow recognition for identifying deepfake videos. In: BIOSIG 2020 - Proceedings of the 19th International Conference of the Biometrics Special Interest Group.*

107. Taha MA, Khudhair WM, Khudhur AM, Mahmood OA, Hammadi YI, Al-husseinawi RS, Aziz A. EMERGING THREAT OF DEEP FAKE: HOW TO IDENTIFY AND PREVENT IT. InProceedings of the 6th International Conference on Future Networks & Distributed Systems 2022 Dec 15 (pp. 645-651).