EMERGING THREAT OF DEEP FAKE: HOW TO IDENTIFY AND PREVENT IT

Murooj Amer Taha
Bilad Alrafidain University College, Department of Computer Engineering Techniques, Diyala, Iraq
muroj@bauc14.edu.iq

Wijdan Mahood Khudhair
Bilad Alrafidain University College, Department of Computer Engineering Techniques, Diyala, Iraq
Wijdanm@bauc14.edu.iq

Ahmed Mahmood Khudhur
Bilad Alrafidain University College, Department of Computer Engineering Techniques, Diyala, Iraq
Dr.ahmedm@bauc14.edu.iq

Omar Abdulkareem Mahmood
Department of Communications Engineering, College of Engineering, University of Diyala, 32001, Iraq
omar_abdulkareem@uodiyala.edu.iq

Yousif I. Hammadi
Bilad Alrafidain University College, Department of Medical Instruments Engineering Techniques, Diyala, Iraq
yousif.ibrahim.hammadi@gmail.com

Riyam Shihab Ahmed Al-Husseinawi
Bilad Alrafidain University College, Department of Computer Engineering Techniques, Diyala, Iraq
reyam@bauc14.edu.iq

Ahmed Aziz
International Business Management Department, Tashkent State University of Economics, Tashkent, Uzbekistan
a.mohamed@tsue.uz

ABSTRACT

Although manipulations of visual and aural media have been around for as long as there have been media, the relatively recent introduction of deep fakes has marked a turning point in the creation of fake information. Deep fakes are automated methods that allow the creation of fake information that is becoming increasingly difficult for human observers to see. These procedures are made possible by the most recent technological advancements in artificial intelligence and deep learning. Deep Learning is a powerful method that is now being implemented in a variety of industries, including natural language processing, computer vision, image processing, and machine vision. Deep fakes are created by the use of deep learning algorithms in order to synthesize and modify photos, videos, or sounds of a person, to the point that human people are unable to discern the fake from the real one. In this article, we present a workable description of deep fakes as well as an outline of the technology that lies underneath them. In order to assist people in thinking about the future of deep fakes, we outline the benefits of the deepfake as well as the potential threats. This study presents a complete analysis of deep fake methods and discusses the most effective strategies for preventing counterfeiting.

ICFNDS '22, December 15, 2022, Tashkent, TAS, Uzbekistan

ACM ISBN 978-1-4503-9905-0/22/12…$15.00
https://doi.org/10.1145/3584202.3584300

ACM Reference Format:
Murooj Amer Taha, Wijdan Mahood Khudhair, Ahmed Mahmood Khudhur, Omar Abdulkareem Mahmood, Yousif I. Hammadi, Riyam Shihab Ahmed Al-Husseinawi, and Ahmed Aziz. 2022. EMERGING THREAT OF DEEP FAKE: HOW TO IDENTIFY AND PREVENT IT. In *The 6th International Conference on Future Networks & Distributed Systems (ICFNDS '22), December 15, 2022, Tashkent, TAS, Uzbekistan.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3584202.3584300

1 INTRODUCTION

In recent times, there has been a lot of focus placed on deep fake technology. Growing public anxiety can be attributed to the possibility that deep fake technology would produce offensive information and violate individuals' right to privacy. The fact that it is able to cast doubt on the veracity of what we see has a significant bearing on our everyday lives. However, technology may frequently be used for both bad and positive purposes, such as deep fakes[1]. Deep fakes, which get their name from the combination of the terms "deep learning" and "fake," are produced by methods that can superimpose face images of a target person onto a video of a source person to create a video of the target person doing or saying things the source person does. This is one definition of the term "deep fake." In the realm of deep fakes, this falls under the category known as face swap. Deep fakes are, in a more general sense, pieces of material that have been generated by artificial intelligence. This type of content may also be classified as either lip-sync or puppet-master, which are two additional distinct types of content. Deep fakes of lip sync are videos that have been altered such that the mouth movements are in time with the audio recording. Videos of a target person, known as a "puppet," who is animated to follow the facial expressions, eye and head movements of another person,

Figure 1: Example of a deep fake: the left-hand image is the original; on the right is the fake. Source: SRF

known as a "master," who is seated in front of a camera are examples of puppet-master deep fakes[1,2].

Simply said, deep fakes allow for the replacement of one person's face in a picture or video with that of another. Until recently, this kind of change needed expert-level knowledge of video editing software. Anyone with the right amount of drive, time, and processing power may now access the technology [3]. An anonymous Reddit user using the handle "deep fakes" (deep learning fakes) uploaded the first deep fakes, which involved inserting celebrities who were unaware of the situation into pornographic videos. By making available the code used to create the deep fakes, the interest in them quickly spread across the Reddit community, resulting in a flood of maliciously created material. Actors' (e.g., Emma Watson and Scarlett Johansson), musicians' (e.g., Katy Perry), and politicians' (e.g., Obama and Trump) likenesses were the first to be used in deep fakes without their knowledge or consent. In 2017, "Synthesizing Obama" became one of the first deep fakes to demonstrate the potential of AI and deep learning with its amazing use of lip-syncing technology based on existing audio material. The leader of one nation may now be delivering an address written by the leader of another[4]. The research is structured as follows: a description of the technology's inner workings; methods for detecting deep fakes; an examination of the technology's pros and cons; a discussion of the threats posed by deep fakes; and finally, a brief mention of some approaches for avoiding them.

2 LITERATURE REVIEW

The technology that is used to combat deep fakes can be broken down into three distinct categories: (1) the identification of the deep fake; (2) the authentication of the published material; and (3) the prevention of the distribution of content that may be utilized for the development of deep fakes. The capacity to manufacture deep fakes is progressing far faster than the ability to detect them, despite the rapid growth of technology for the detection and verification of deep fakery, which is gaining ground quickly. The development of Deepfakes can be done with nefarious intentions, making their identification a potential security risk. Bismi et al. present various creation and detection methods that are up now in research in Deepfake using various techniques such as Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Long Short Term Memory (LSTM), etc.... These techniques provide a backbone in the implementation of a new scheme that would be more compactable and accurate in the detection of Deep fakes[5]. Zhiming et al. propose a Deepfake detection method based on MesoNet with a preprocessing module. This method involves filtering low-frequency signals in the image; however, high-frequency signals with apparent differences are retained. This increases the texture difference between authentic and Deepfake-generated images [6]. Hina et al. offer a detailed summary of the many methods that may be used to identify deep fakes, which helps to reduce the negative effects of deep fakes. According to the findings of the analysis, machine learning and deep learning models such as CNN and its variations, SVM, LR, and RF and their variants are highly useful in distinguishing between authentic and fraudulent information in the form of pictures and videos[7]. Xiaojun Li and colleagues offer a CNN-based model that, by taking into account three kinds of characteristics, is able to efficiently recognize videos that are deceptive (i.e., content features, uploader features, and environment features). The results of the trials demonstrated that all three classes of characteristics contribute significantly to the process of identifying false video content[8].

Ammar Elhassan et al. present a comprehensive method and software implementation for identifying fabricated videos created with Deep Learning technology [9]. This method relies on the utilization of teeth and mouth movement as distinguishing features, both of which continue to be very difficult to perfect when it comes to creating phony videos. Priti Yadav offers a method that can automatically detect deep fake based on separating user video into frames, and then preprocessing these frames using InceptionResNetV2 and LSTM. This method was developed by dividing user video into frames. The approach examines every video by utilizing a convolutional LSTM system, and it also assists in recognizing deepfake faces that have been modified, which stops people from being defamed [10]. Kai Hong and Xiaoyu Du associate the deepfake artifacts with some common noises as a powerful tool to understand the unseen artifacts through the use of the Deepfake Artifact Discrepancy Detector (DADD) method [11]. Njood and Abdul construct a model that is capable of classifying the content (pictures) of Instagram in order to identify any potential risks and faked photographs. Deep learning techniques, specifically the Convolutional Neural Network (CNN), Alexnet network, and transfer learning with Alexnet were utilized in the construction of the model [12]. If the opponent has entire or even partial knowledge of the detector, it is simple for them to go around the existing approaches that are considered state-of-the-art for Deepfake detection [13]. Authentication methods for digital photographs, music, and videos have lately received a lot of interest due to the fact that this content is transferred across insecure mediums such as the internet and different forms of computer networks. The research on authentication strategies may be broken down into two categories: those that make use of digital signatures and those that employ digital watermarking [14]. An end-to-end document picture watermarking system that makes use of the deep neural network has been proposed by Sulong Ge and colleagues. To be more specific, an encoder and a decoder are created so that the watermark may be embedded and extracted. A noise layer is included in order to replicate the numerous assaults that a user could experience in the real world. These attacks include cropout, dropout, gaussian blur, gaussian noise, resize, and JPEG compression [15]. Both a wavelet-based watermark casting approach and a blind watermark retrieval technique have been proposed by Hong-Jyh et al. An adaptive watermark casting approach is created in order to first find significant wavelet subbands and then pick a couple of significant wavelet coefficients inside these subbands in order to incorporate watermarks. This process is repeated until significant wavelet subbands are identified.

The results of the experiments demonstrate that the embedded watermark can withstand many types of assaults including signal processing and compression[16]. A brand new method of video watermarking based on SLT, CT, and DCT has been proposed by Salam. When it comes to the most important aspect of the suggested method, the linkage between security, robustness, and imperceptibility, this has been accomplished by combining the properties of all of the different transformation techniques that have been applied. The suggested approach has proved that it is helpful and appropriate for applications involving copyright protection as well as content authentication [17]. Ali suggested an undetectable and robust audio watermarking technology that was based on cascading two well-known transforms: the discrete wavelet transform and the singular value decomposition [18]. This technique was intended to enable copyright protection of digital audio transmissions. A brand new method for the encryption of images, based on SHA-512, has been proposed by Seyed and colleagues. The fundamental concept behind the technique is to encrypt one half of the picture with the data from the second half of the image, using the first half of the image as a key. One of the algorithm's distinguishing features is its high level of security [19]. An technique for hashing videos has been proposed by Li Weng and colleagues. This approach generates a 180-bit hash value for films of any duration. The hash value is immune to typical signal processing and only very minimal geometric distortion, indicating that the algorithm is performing well [20]. A robust video hash function is something that Baris et al. suggest for use in broadcast monitoring and database search applications. The 3D-DCT transform of video sequences is binarized into low-frequency components for this approach. The work contributes originality and resiliency to the video [21]. Despite this, these techniques are not the only ones that may be used to combat the problem of deep fakes. Therefore, it is absolutely necessary to participate in awareness activities and training in order to avoid the early indications of deepfake assaults. As a result, we identify various strategies in this study that may be used to prevent deepfake. Additionally, we discuss the methods for creating deep fakes as well as detecting them

3 HOW DOES THE TECHNOLOGY ACTUALLY FUNCTION?

Different techniques exist for producing deep fakes, but they all use some form of artificial intelligence, or more precisely, the branch of machine learning known as deep learning. There are artificial neural networks involved here. The FakeApp graphical user interface employs an autoencoder, a neural network optimized for data compression and optimal picture replication [3]. Autoencoders are a type of deep network architecture that attempt to approximate the way in which a human observer interprets a human face (auto referring to the self). Autoencoders are taught to detect essential traits of a face based on a given, huge number of input photographs (e.g., all displaying Alison Brie) and to replicate input images as their output. Using an encoder, a latent space, and a decoder, the system is able to recognize a very limited set of facial traits in the input and then generate realistic-looking faces in the output (see Figure 2)

A compression procedure is carried out by the encoder in a manner that is analogous to that of an artist sketching a picture. It collects tens of thousands of pixels and compresses them down into an average of 300 metrics that relate to distinct face traits. They encode a variety of properties, such as whether the eyes are open or closed, the head attitude, the emotional expression, the eye expressions, the surrounding light, or the skin tone, all of which an artist may choose to pay attention to. The encoder makes it possible for information to flow from an input image that is exceedingly detailed into something that is referred to as a compressed information bottleneck. Consider the case of an encoder that condenses the data being entered into only two measures: the first of these measurements represents the horizontal angle of the head, and the second indicates whether a person is smiling or looking astonished. In response to the provision of an input picture, the encoder will provide two measurements that together encode the subject's emotional state and head orientation. These may be pictured as a point in a two-dimensional space, where the two measurements are represented by the place where the x-axis and the y-axis intersect. The term "latent space" refers to the space that contains all of the potential combinations of measurements of face traits. The extraordinary compression that may be obtained by encoding an input picture into the latent space If the latent space was made up of 300

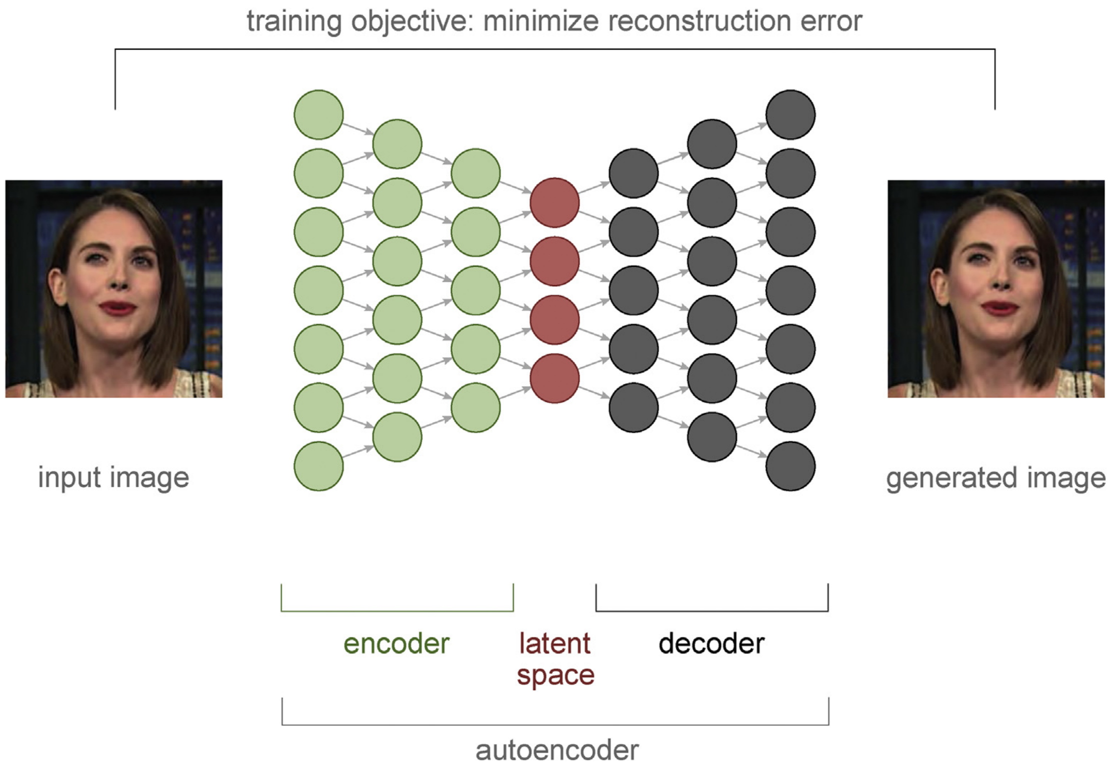

Figure 2: Autoencoder: A DNN architecture commonly used for generating deep fakes (Brie image)

measurements, then it would only take up 0.1% of the memory that is required to retain the initial input image. As was said before, the latent space is a representation of many facial characteristics of the individual on which it is trained. An autoencoder that has been trained on photographs of Alison Brie's face, for example, will learn to map a given input image of her into a latent space that precisely represents her. This may be done by training the autoencoder on images of Alison Brie's face.

From the input to the output, there must be a re-creation of the latent space's picture. The decoder is what you need. The decoder's job is to unpack all that data and use it to rebuild the image as faithfully as possible. The similarity between the input and produced (output) pictures is used as a metric of the autoencoder network's effectiveness. In conclusion, the autoencoder goes further than pre-existing picture data by learning a generative model of a human face. Every location in the latent space represents an image of a certain individual, as was previously explained. The decoder of a Brie-trained autoencoder can produce convincingly false pictures of Brie. One way to fool an autoencoder is to train two of them with the same encoder but different decoders for different people. This encoder will be trained to make advantage of generic characteristics present in both individuals' faces. This allows for two separate people's images to be placed in the same spot in the latent space.

The key to understanding how deep fakes are created is to look for similar measures that arise from photos of two different persons. They make it possible for us to alter a photograph depicting the face of one person so that it depicts the face of another one. The final product will be completely fictitious, but the created face will have the same facial expression, head posture, and other characteristics as those shown in the original image that was used as input. After that, the newly created image may be composited with the original photograph to produce a fictitious setting.[4]

4 DEEP FAKE DETECTION

Beginning in the early part of 2018, deep fake detection is a study field that is still in its infancy. There are two distinct categories of methods.

Biological signals: Several studies have investigated anomalous actions in deep fake films, including a lack of blinking, facial deformities, and erratic movement. These strategies might benefit from some easy tweaks to the video production processes, including the addition of blinking.

Pixel level irregularities: There is a broader range of research that extracts faces and employs various types of deep learning to target intra-frame or inter-frame discrepancies. These studies may be found in a variety of academic journals. Although many of these algorithms work admirably on certain kinds of manipulations, they are unable to generalize to many and unknown kinds of deep fakes, which is a capability that is essential for open-world detection. None of the methods that have been proposed for detecting deep fakes have yet been turned into an actual tool that can be utilized for detection in the real world. To our knowledge, there have also

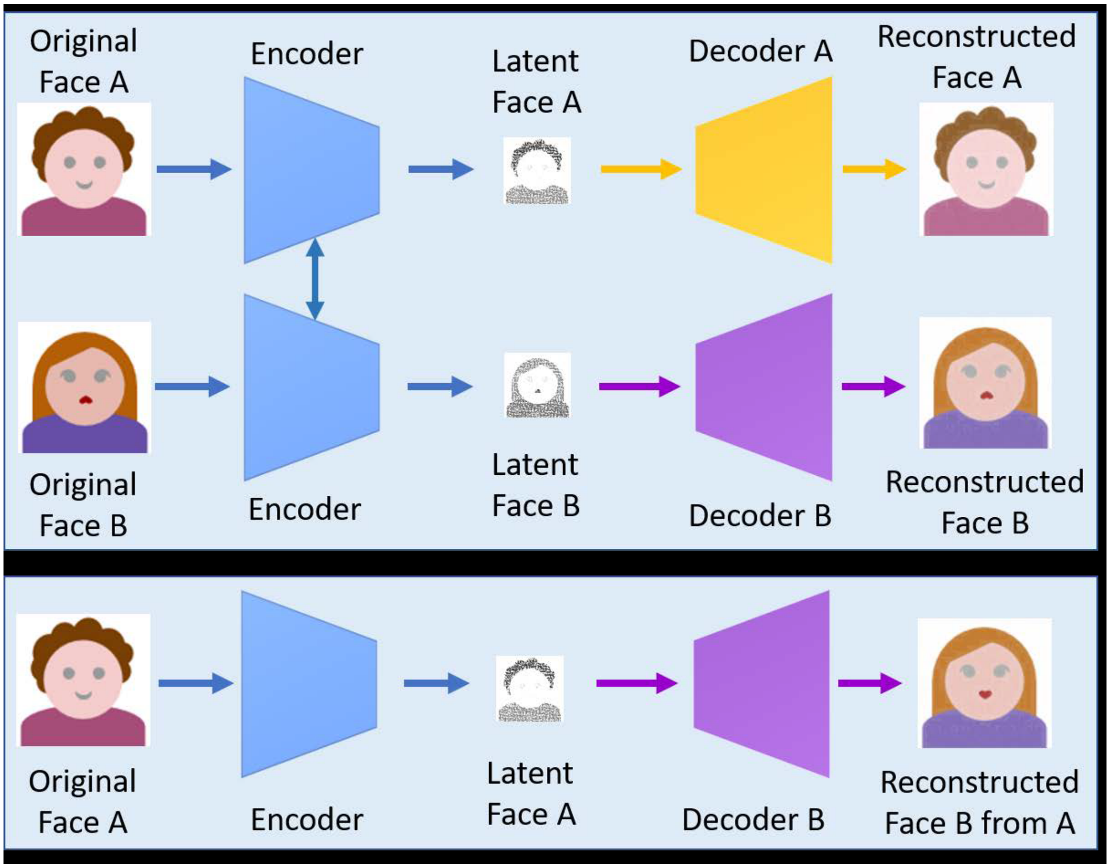

Figure 3: A deep fake creation model using two encoder-decoder pairs.

not been any research conducted on the topic of how to effectively create such a tool for use by journalists [22].

5 ANALYZING THE TECHNOLOGY

There are already a great number of effective instances of deep fakes; nevertheless, there are very few, if any at all, particular factors that can be used to define what defines a successful deep fake. The testing environment that we have built is intended to offer clear information on the present status of deepfake technology as well as the picture material needs for making effective fakes. Studies are currently being conducted to identify the boundaries of the technology that is now accessible. These studies are based on a variety of parameters. In order to assess compliance with these prerequisites, the following criteria have been established:

•The total number of photographs
•The prevailing lighting conditions
•The magnitude and quality of the source material;
•The orientation of the source material;
•Variations in face features;
•Objects that overlap one another [3]

5.1 The Possible Threats of Deep fakes

Deep fakes are a major threat to our society, political system, and business for the following reasons: 1) they put pressure on journalists who are already struggling to differentiate between real and fake news; 2) they threaten national security by spreading propaganda and interfering in elections; 3) they impede citizen trust toward information provided by authorities, and 4) they raise cybersecurity issues for individuals and organizations[23].

5.2 The Benefits of Deep fake Technology

Deepfake technology also has beneficial applications in a variety of other industries, such as 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. There are many different ways in which the film business might profit from deepfake technology. For instance, it can be helpful in the process of creating digital voices for performers who have lost their own due to illness, or in the process of updating film material rather than reshooting it. When it comes to post-production, filmmakers will be able to make use of special effects and advanced face editing software, as well as improve the quality of amateur videos so that they are on par with those produced by professionals. They will also be able to create new films that star actors who have passed away. Additionally, the Deepfake technology enables automated and lifelike voice dubbing for films of any language, making it possible for a wider variety of people to take pleasure in watching films and other forms of instructional media. An educational advertisement aimed at raising awareness about malaria that featured David Beckham in 2019 was able to break through language barriers with the use of visual and voice-altering technologies to make him appear to speak other languages.

Similarly, the deepfake technology can translate speech while simultaneously altering facial and mouth movements to improve eye contact and make it appear as though everyone is speaking the same language during video conference calls. This can break down the language barrier that can exist during these calls. The technology that underpins deep fakes makes it possible for multiplayer games and virtual chat worlds to have enhanced telepresence, natural-sounding and –looking smart assistants, and digital doubles of real people. This contributes to the development of healthier human connections and interactions inside the digital space. In a similar vein, technology may also have beneficial applications in the social and medical sectors. By digitally bringing a departed friend "back to life," deep fakes can assist individuals in dealing with the grief that comes with the loss of a loved one. This can enable a grieving loved one to finally say goodbye to the person who passed away. In addition, it may digitally replace a missing limb on an amputee or let transgender persons view themselves more accurately in their desired gender identity (USAT04).

Deep fake technology can potentially assist patients with Alzheimer's disease by allowing them to engage with a younger version of themselves that they may recall. GANs are also being investigated by researchers for their potential to be used in the creation of virtual chemical compounds, which would speed up the process of scientific and medical discovery. X-ray anomalies are being detected using GANs. Businesses are intrigued by the prospect of brand-applicable deep fake technology because of the important ways in which it has the potential to revolutionize eCommerce and advertising. For instance, fashion businesses may show off their wares on models with a range of skin tones, heights, and weights by using "supermodels" who are not actually supermodels. In addition, deep fakes make it possible to create highly personalized content that transforms customers into models; 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). The technology not only enables people to create digital clones of themselves and have these personal avatars travel with them across stores, but it also enables people to try on a bridal gown or suit in digital form and then virtually experience a wedding venue. One obvious potential use is the ability to quickly try on clothes online; the technology not only enables people to create digital clones of themselves and have these personal avatars travel with them across stores, but it also enables people to try on clothes online. Additionally, AI is able to offer various artificial voices that may be used to differentiate firms and products, which makes the process of branding easier [24, 25].

6 PREVENTING DEEPFAKE ATTACKS

Users are susceptible to phishing assaults, and deepfake phishing efforts will be much harder to spot. Security programs that don't include cybersecurity awareness training are lacking in their most basic component. Make sure that you give information on how to spot a phony.

This is far simpler than you could ever imagine. The technology that enables these assaults is effective, but it is not foolproof. Raymond Lee, CEO of FakeNet.AI, and Etay Maor, senior director of security strategy at Cato Networks, discussed the difficulty of perfecting facial characteristics during a webinar. In particular, they focused on how challenging it is to replicate an individual's eyes. If the eyes appear strange or the movement of the facial features looks odd, there is a significant likelihood that the image has been manipulated.

The highest standards and a complete lack of confidence in anybody. Make sure of whatever you see. Verify the message's origins via at least two means. If you can, try to discover the original by doing a search for images.

Although technological measures are important, there are other ways to safeguard against Deepfake films. Basic security practices are surprisingly effective against Deepfake. For instance, many Deepfake and related scams may have been prevented with the implementation of automated checks into any procedure for disbursing payments. You may also:

•Inform your friends and family about the dangers of Deepfaking and how it operates. Learn to recognize a Deepfake and teach others to do the same. Take care to be well-versed in the media and consult reputable outlets for your news.

•"Trust but verify" are important fundamental procedures to have in place. Not being duped is impossible to ensure, but you may avoid many pitfalls by approaching voicemails and videos with a healthy dose of skepticism. Keep in mind that if hackers start using Deepfake to get into residential and business networks, the most important thing you can do to protect yourself is to follow fundamental cyber-security best practices. Use unique, strong passwords for each account to ensure that if one network or service is breached, it won't automatically affect the others; regular backups safeguard your data from ransomware and allow you to retrieve lost data. No one wants Facebook hackers to have free reign over their other online profiles. Protect your home network, laptop, and smartphone from online dangers with a reliable security suite, such as Kaspersky Total Security. You can safeguard your computer and camera from viruses and hackers with the VPN included in this bundle. Since deep fakes have only begun to be used as an attack vector, cybersecurity teams have time to develop countermeasures before the methods to counter them become more sophisticated. As a result, you should have one less item to worry about [26, 27].

7 CONCLUSION

Trust in media has been weakened by the proliferation of deep fakes since mere exposure is no longer sufficient to instill belief. They may provoke political conflict, public outrage, bloodshed, or even war, and they may have devastating consequences for the people who are singled out. In this work, we thus give a comprehensive analysis of the technology, risks, advantages, and prevention of deepfake assaults, along with an exhaustive description of deepfake and its detection methodologies. To that end, our research will help the AI research community create efficient strategies for countering deep fakes.

REFERENCES

[1] Bingquan Zhu *et al.* 2020. " Deepfakes for Medical Video De-Identification: Privacy Protection and Diagnostic Information Preservation". In Proceedings of the 2020 AAAI/ACM Conference on AI, Ethics and Society (AIES '20), February 7–8, 2020, New York, NY, USA. ACM, New York, NY, USA, 7 pages.
[2] Thanh Thi Nguyena *et al.* (2022). " Deep Learning for Deepfakes Creation and Detection: A Survey". Computer Vision and Image Understanding. ELSEVIER.
[3] Andrea Hauser and Marc Ruef (Editor). 2018. " Deepfake - An Introduction". skip Labs.
[4] Samsung SDS *et al* . 2022. " FrePGAN: Robust Deepfake Detection Using Frequency-level Perturbations". Association for the Advancement of Artificial Intelligence (www.aaai.org).
[5] Bismi Fathima Nasar *et al.* 2020. " A Survey on Deepfake Detection Techniques ". International Journal of Computer Engineering in Research Trends.
[6] Zhiming Xia *et al* . 2022. " Deepfake Video Detection Based on MesoNet with Preprocessing Module". MDPI.
[7] Hina Fatima Shahzad. 2022. "A Review of Image Processing Techniques for Deepfakes". MDPI. '
[8] Xiaojun Li *et al.*2022. "A CNN-based misleading video detection model ". Scientific Reports, nature portfolio.
[9] Ammar Elhassan *et al.* 2022. "DFT-MF: Enhanced deepfake detection using mouth movement and transfer learning ". SoftwareX, ELESEVIER.
[10] Priti Yadav. 2021. "DeepFake Detection using InceptionResNetV2 and LSTM ". International Conference on Emerging Technologies: AI, IoT, and CPS for Science Technology Applications, September 06–07, 2021, NITTTR Chandigarh, India.
[11] Kai Hong and Xiaoyu Du. 2021. "Self-Supervised Deepfake Detection by Discovering Artifact Discrepancies ". CEUR Workshop Proceedings.
[12] Njood Mohammed AlShariah and Abdul Khader Jilani Saudagar. 2019. "Detecting Fake Images on Social Media using Machine Learning". International Journal of Advanced Computer Science and Applications.
[13] Shehzeen Hussain *et al.* 2021. "Adversarial Deepfakes: Evaluating Vulnerability of Deepfake Detectors to Adversarial Examples ". IEEE.
[14] Basna Mohammed Salih Hasan etal. 2021. "Image Authentication Based on Watermarking Approach: Review". Asian Journal of Research in Computer Science.
[15] Sulong Ge *et al* .2020. "A Robust Document Image Watermarking Scheme using Deep Neural Network". JOURNAL OF LATEX CLASS FILES.
[16] Hongoung-Jyh Mike Wang *et al.* 1998. " Wavelet-based digital image watermarking". Optica publishing group.
[17] Salam Abdulnabi Thajeel. 2017. "Robust Video Watermarking of Hybrid Based Techniques". Iraqi Journal of Science.
[18] Ali Al-Haj. 2014. " An imperceptible and robust audio watermarking algorithm". Springer.
[19] Seyed Mohammad Seyedzade *et al* . 2010. "A Novel Image Encryption Algorithm Based on Hash Function". Research gate.
[20] Li Weng and Bart Preneel. 2015. " A Novel Video Hash Algorithm ". research gate.
[21] Baris Coskun, Bulent Sankur. 2014. " ROBUST VIDEO HASH EXTRACTION ". IEEE.
[22] Saniat Javid Sohrawardi *et al* . 2020 . " DeFaking Deepfakes: Understanding Journalists' Needs for Deepfake Detection". Conference: Computation+Journalism Conference 2020. At: Boston, MA Project: DeFake Project.
[23] Matthew Groh *et al* . 2021. " Deepfake detection by human crowds, machines, and machine-informed crowds". PNAS
[24] MikaWesterlund. 2019 " The Emergence of Deepfake Technology: A Review". Technology innovation management review.
[25] Hrisha Yagnik *et al.* 2020. " A Brief Study on Deepfakes". International Research Journal of Engineering and Technology(IRJET)
[26] Suganthi ST *et al.*2022. " Deep learning model for deep fake face recognition and detection". PeerJ Comput. Sci., DOI 10.7717/peerj-cs.881 3/20
[27] Shruti Agarwal and Hany Farid. 2019. " ProtectingWorld Leaders Against Deep Fakes". IEEE.