Sri Lanka Institute of Information Technology

B.Sc. (Hons) Information Technology-

Cyber security

Y2 S1

Introduction to Cyber Security – IE 2022

Deepfakes behind Deception

M. A. AMANTHA

IT 23 1843 12

Contents

Abstraction

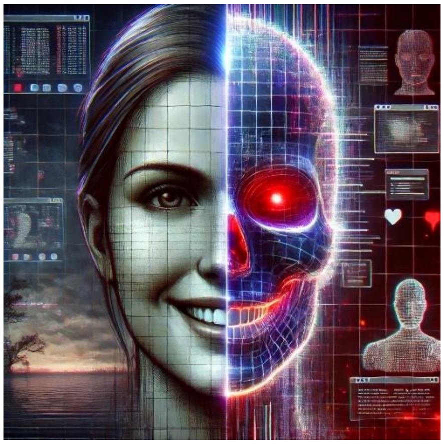


Figure 1 Deep fakes behind Deception

This report investigates the recent development in deepfake technology and its utilization in social engineering attacks. Deepfake threats have become as a severe problem within the area of cyber security Since their appearance in 2017, deepfakes have deeply attracted widespread media and popular attention because of their potential to tamper with digital media, deceive audiences, and break confidence in any information. Deepfakes utilize artificial intelligence to build up very realistic but actually fabricated content, including video, audio clips, and other forms of material which convincingly impersonate real individuals. It does so by focusing on how deepfakes have been weaponized in social, political, and financial contexts-from creating a fake narrative in political campaigns to defrauding through impersonation based on synthesized personalities. It is intended to explore the underlying technology, analyze examples of deepfakes used for deception in the real world, and discuss the ethical, legal, and security challenges one has to face with this innovation. In the beginning of this report, I decided to describe from the history, architecture up to the process of creating a deepfake and about social engineering, how this technology have affected to social engineering. The report finally underlines the need to develop mechanisms for detection and regulatory measures against misuse of deepfakes in present-day digital life and real-world examples for deepfakes used for social engineering.

Introduction

The arrival of deepfake technology marked a critical point in the digital era and came with serious implications concerning cybersecurity.[8] A technology that started as an experimental use of AI and ML grew into a powerful tool able to generate hyper-realistic, though totally fabricated, audio, video, and images. Deepfakes, a portmanteau of the "deep learning" techniques used to generate them, have evolved into becoming mostly indistinguishable from real media, exponents in the threat landscape against persons, enterprises, and governments, while this technology is increasingly used by cybercriminals for social engineering attacks.

Deepfakes are specifically dangerous in the context of social engineering. By generating convincingly real footage of people trusted by targeted individuals, cybercriminals can create fake personas imitating executives, political leaders, or personal acquaintances.

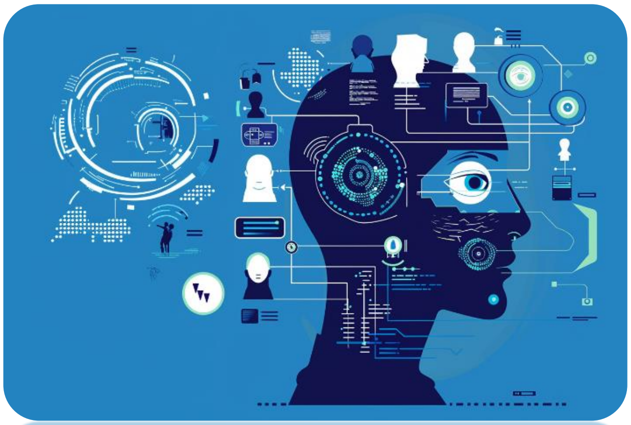


Figure 2 Introduction to Deepfake

The possibilities of deception are huge, ranging from corporate fraud and financial scams to manipulation on political levels and personal defamation. Among such popular cases, one happened in **2020** when a deepfake video of **Former US President Barack Obama** which deliver a speech where he says outrageous and inappropriate things was created by filmmaker Jordan Peele to raise awareness about the dangers of this technology. This report tends to look critically at the convoluted ways in which deepfakes have been weaponized for socially engineering attacks, examines real-world cases, analyzes their implications, and presents actionable countermeasures that could be taken to mitigate these emerging threats. As we explore these issues, it would appear rather evident that while deepfakes do have certain legal and practical applications in areas such as entertainment and customer service, the malicious use of the technology presents one of the most serious cybersecurity challenges of late.

What is Deepfake technology?

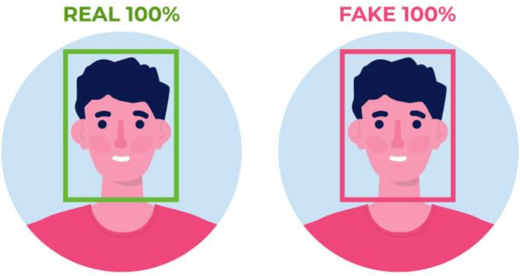


Figure 3 Real or Fake

Deepfake technology relies on the usage of AI, especially deep learning algorithms, in order to create digital content including very realistic videos, images, and audio that is completely fabricated. These may also involve media of people convincingly doing or saying things they never actually did, thereby making the deepfakes nearly indistinguishable from real footage. [8]

The word "**deepfake**" is a mix of "**deep** learning" and "**fake**," and it refers to applying deep learning methods-the subset of artificial intelligence-to make fake digital content, for example, a video or an image, look realistic.

Deepfake technology can be used to do things like make realistic movies of people doing or saying things. Analysis allows one to obtain more of what they never actually did or said through emulating the gestures. Capturing the lip, speech, and facial expressions of the individual in the original video and modifying the film to Create a new synthetic version of this that seems real.

People have been playing with ways of editing video and audio for years. Applications such as photo editing software have seen wide usage in creating memes or perfecting the images in the movie industry. Deepfake technology takes this manipulation to a new level; it uses AI-powered tools that create synthetic media convincingly impersonating real people. With advanced techniques such as autoencoders and Generative Adversarial Networks, it can be done in high levels of realism to replicate one's facial features, expressions, or movements of a person. Thus, it opened new doors to cybercriminals by letting them do highly realistic impersonations for deception.

Evolution of the Topic

The History of Deepfake

Deepfake technology originates in the rather long history of manipulation with media. Since the 19th century, techniques to edit images and videos were used to enhance or distort visual content in movies and photography. With the introduction of digital video to the world in the late 20th century, these techniques grew in sophistication and eventually gave birth to what we currently known as deepfakes. [1]

Early Development and Face-Swapping (1990s-2010s)

However, development in deepfake technology began in the 1990s when at-institution academic researchers started experimenting with neural networks and machine learning techniques to manipulate images and videos. That changed in the early 2010s when the rise of Generative Adversarial Networks let looser and more pioneering face-swapping applications. This is attributed to the fact that GANs operating on face-swapping allow a person to superimpose one video over another, which has raised substantially the popularity of this technology.

By 2017, deepfake technology went mainstream when open-source tools were developed that made the process simpler and accessible to non-experts.

Expanding to the voice and full-body manipulation

As deepfakes further evolved, the technology wasn't limited to face-swapping but also involved voice synthesis and even the manipulation of the full body. This introduction of voice deepfakes allowed attackers to impersonate the vocal patterns of targeted individuals through the generation of convincing fake audio. Full-body manipulation is another important development in this area, which has enabled the change of the whole human movements-thus adding another layer of realism to deepfake videos.

Accessibility and Open-source Tools

One of the important milestones in deepfakes development was when open-source tools and large datasets became available. These let users manipulate video content with ease, devoid of the need for in-depth technical knowledge. Apps like of **FakeApp** and **DeepFaceLab** let amateur users experiment with deepfake creation, accelerating the spread of technology.

The Rise of Deepfake Threats (2017-present)

With the advancement of technology, its misuses also grew. Starting from 2017, deepfakes prominently came into use for non-consensual explicit content, where faces of celebrities were mapped onto adult videos. As the quality of deepfakes continued improving, the technology soon came into use both for political disinformation and cybercrime. In 2020, a deepfake of **Gabonese President Ali Bongo** raised concerns about political stability, while cybercriminals began to use deepfake audio to impersonate chief executives and defraud companies. Current Status and Social Concerns Nowadays, deepfake technology has grown to the extent that it is able to convincingly impersonate public figures, celebrities, and even ordinary people. The most hazardous usages are in disinformation campaigns, financial fraud, and breaches of privacy. Deepfakes can seamlessly insert fake voices and full-body movements into some sort of performance; thus, this type of content is getting closer to real situations that are indistinguishable by detection systems.

Figure 4 Evolution of Deepfake Technology

What is GAN?

Generative Adversarial Networks, or GANs for short, are a class of advanced deep learning models that consist of two neural networks in competition with each other: a **generator** and a **discriminator**. [1] While the former generates synthetic data, the other evaluates either the credibility of that data or decides whether the input is real or fake. This adversarial relation, therefore, optimizes each of the networks in a fashion commonly called the **minimax game**, whereby the generator strives to produce data that is increasingly realistic to deceive the discriminator, and vice versa. Over time, these dynamics will train the network to generate high-quality synthetic outputs that can be images or audio; often these are well-performing and near, or even indistinguishable from, real data. Since the original invention by **Ian Goodfellow** in **2014**, GANs' have taken off as an extremely active area of research and applications across many domains such as computer vision, natural language processing, and audio synthesis.

Within **computer vision,** GANs' have had some successes in synthesizing new human faces, a challenging task. [2]Deep Convolutional GANs make use of CNNs in order to generate realistic images from random noise, while the discriminator evaluates the generated image quality against real ones. Other examples of enhancements include Enhanced Super-Resolution GANs, which are approaches where GAN architectures have been used for enhancing low-resolution images and increasing their quality by such a factor that they can be useful in many other applications, ranging from machine learning model training to generating realistic avatars for video games and virtual reality. The structural similarity coupled with content loss is considered in the perceptual loss function used by the ESRGANs, which helps retain the fidelity and aesthetic appeal in the images generated.

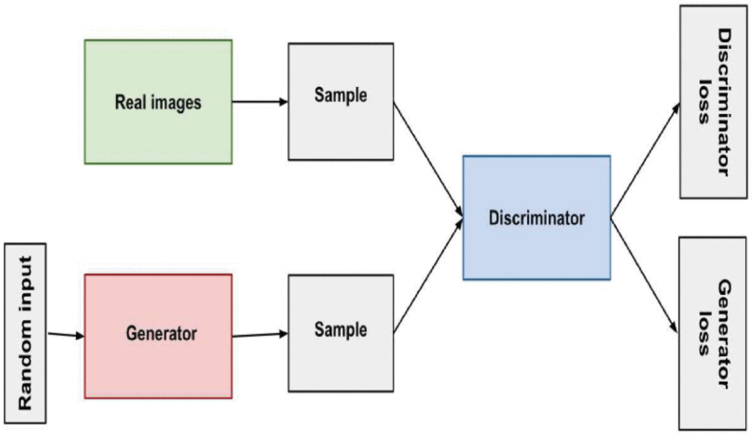


Figure 5 Model summary for the generator G and Discriminator D used in FCC-GAN

Going a step further from image generation, GANs find application in **text-to-image synthesis**, **image-to-image translation**, and even in generating synthetic audio. Considering that their capabilities included creating realistic content, several ethical issues arose with discussions around possible misuse in making deepfakes for malicious applications, ranging from misinformation to identity theft. Notwithstanding the challenges, their innovative nature combined with an ability to create synthetic data makes them game-changers in many industries and therefore a technology of critical interest in the evolution of artificial intelligence and machine learning. Continuous development and adaptation of GANs indicate a promising future by opening new ways of creation and innovation but also call for active vigilance in considering ethical consequences and societal impacts.

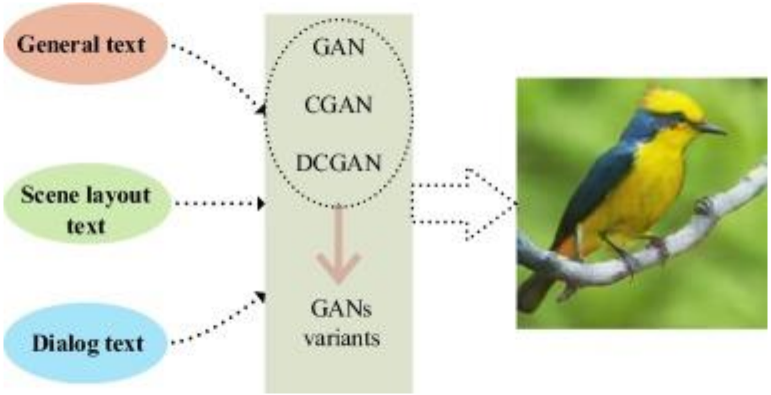


Figure 7 text-to-image synthesis

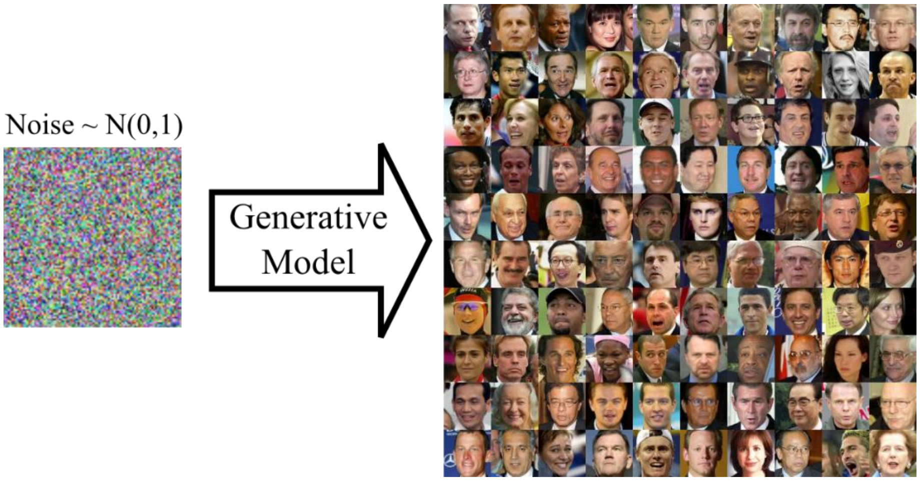


Figure 6 image-to-image translation

The Process of creating a Deepfake

Normally, creating a deepfake involves a number of important steps, tending to make extensive use of advanced techniques in artificial intelligence, especially Generative Adversarial Networks. The following represents a simplified overview of how this is typically done:

1. Data Collection
2. Preprocessing
3. Model Training
4. Face swapping
5. Post processing

Let’s discuss the above one by one.

1. Data Collection

Data collection is the most critical step in creating deepfakes. This will include a diverse, varied set of images or videos of the target individual to be used for training the model. The quality and diversity of the dataset will determine how realistic the final deepfake might look. High-resolution images, taken from different angles in all types of conditions, are very necessary for the model to learn and hence effectively mimic the same facial expressions. The preprocessing would involve the alignment of the face to make the process consistent through and through in the dataset so that it yields good results for training.

This provides a foundation for the deepfakes with the use of artificial intelligence.

2. Preprocessing

Preprocessing is an essential step in which the data collected is cleaned, consistent, and well-prepared for AI models while training in the creation of deepfakes. Preprocessing covers the face detection and alignment, cropping of images focusing on facial regions, resizing all images, normalizing lighting and color consistency, and frame extraction from a video dataset. Augmentation techniques increase diversity within the dataset to generalize better.

Preprocessing lays a good foundation in ensuring data quality for the creation of credible and realistic deepfakes.

3. Model Training

Model training in deepfakes essentially involves the use of artificial intelligence, especially Generative Adversarial Networks. This working out involves two key components: a generator that creates fake images or videos and a discriminator then detects them. They work together in a competitive setup, refining their accuracy. These models are trained using big datasets and optimized with loss functions that minimize generation and detection errors. This involves a very computation-intensive process, as it usually requires GPUs and a high number of training epochs for realistic results. Efficiency and accuracy are further enhanced with the use of more advanced techniques, including transfer learning and data augmentation.

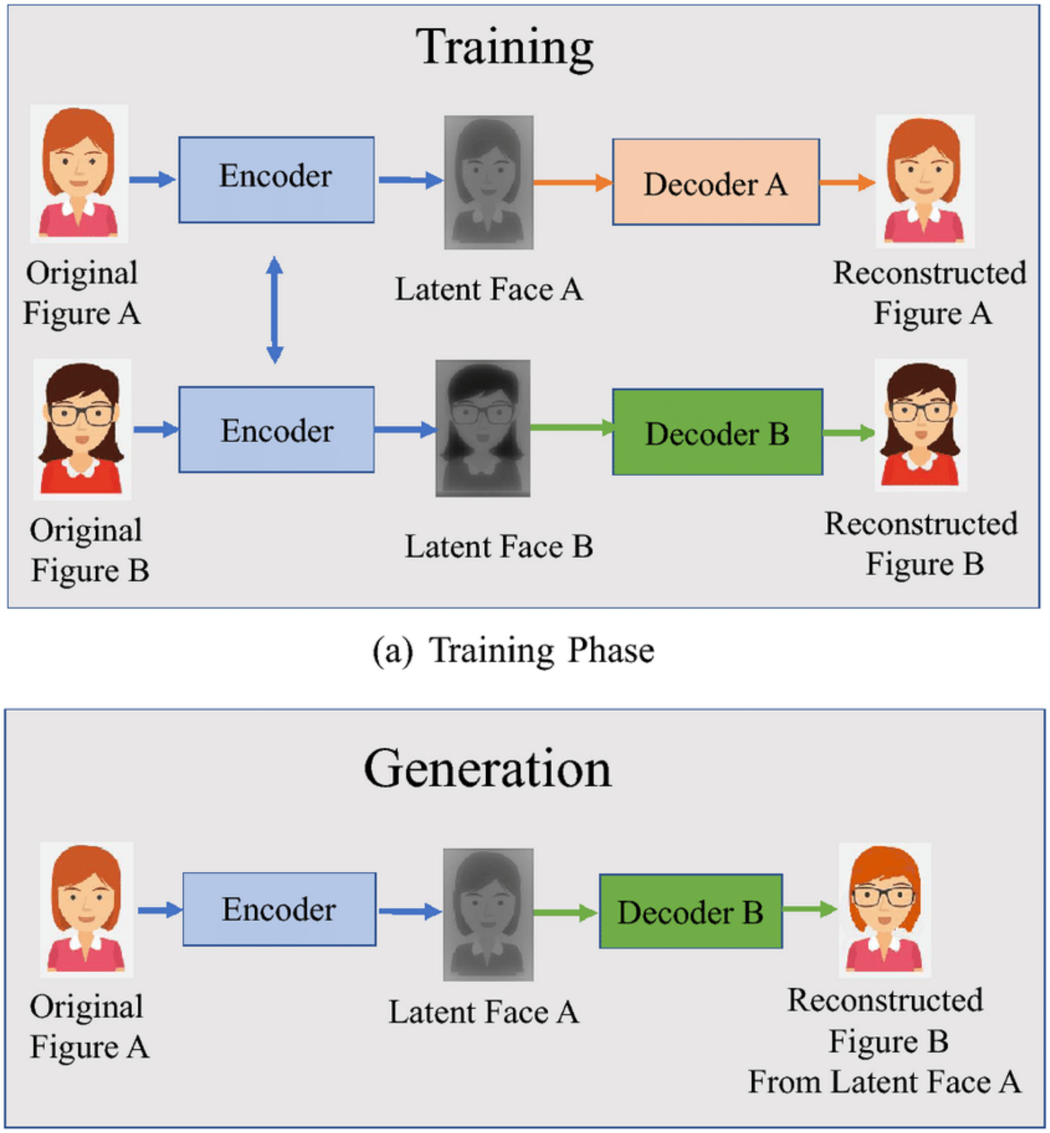
Deepfake models can iteratively build results in a series of trainings that can be extremely convincing at very high computational costs and careful tuning.

4. Face swapping

Face swapping is an application that allows for the perfect superimposition of a person's face onto another's body, enabled through AI technologies such as GANs' and autoencoders. Further, data collection regarding source and target faces is done, followed by the alignment of the facial landmarks detected, training the model to generate a source face to fit features and movements of the target face, and refinements. A new face is blended and rendered onto the target's body, usually with some post-processing in order to make the picture look more realistic. This technique has found very broad application in entertainment; however, it faces serious ethical concerns because of its misuse in deepfakes.

5. Post processing

This is a very important step in deepfake creation, and it is mainly used for enhancing the realism of the generated media. It includes the actual blending of the swapped face with the target body in order to eliminate seams, color and lighting adjustment for natural integrations, and synchronizing facial movements with the target's actions. The process further involves noise and artifact reduction, resolution enhancement for detail, and rendering the final output in a compatible format. In general, post-processing ensures deepfakes are indistinguishable from real media and thereby greatly increases the potential for their abuse.

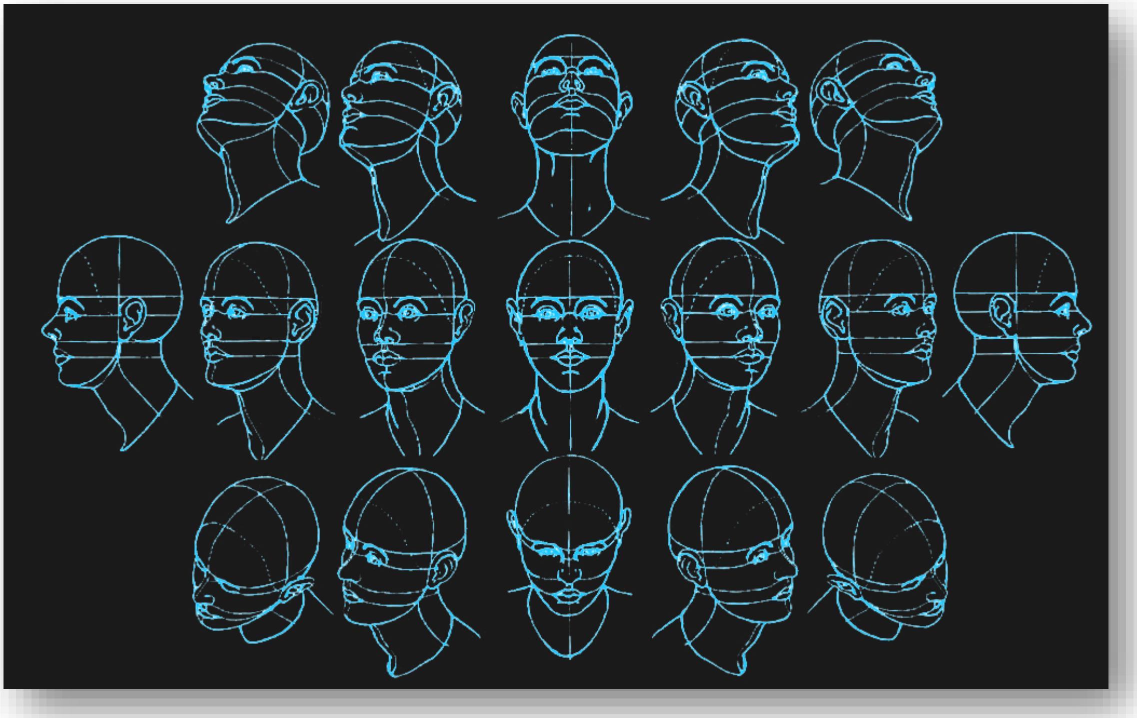


(a) Training Phase

(b) Generation Phase

Figure 8 Creation of deepfakes

Deepfake Apps and Websites



Following are some popular deepfake apps and websites allowing users to make or tamper with videos and images using deepfake technology.

Reface: This is a mobile platform application that helps users change their faces with famous personalities in video clips, even in GIFs. The app holds the most advanced face-swapping technology for realistic results; hence, it is one of the most in-demand applications for fun and creative content.

DeepFaceLab: This is a rather technical tool and also one of the popular free software options used to create deepfake videos. It boasts an array of capabilities that would satisfy even the most inquisitive tinkerers who want to work with deepfakes, and creators use this application for bigger projects.

Zao: This Chinese application went viral for its ability to let users swap faces with those of actors in popular movie scenes. Users simply upload a photo, and within minutes, Zao produces a video of themselves with the swapped face.

FaceSwap: This is open-source deepfake software-a community-based approach to face-swapping technology. Users can download it and experiment with different datasets and models to create their deepfakes.

Synthesis AI: A synthetic media platform that allows users to produce realistic videos with virtual characters. It would mostly be used for business, such as creating digital spokespersons or virtual influencers.

MyHeritage Deep Nostalgia: Animates the faces within still images in order to show them breathing, moving, and smiling. It is meant to allow genealogists to have an animated glimpse of what their ancestors might be like.

Synthesia is a video generation platform that creates professional-looking videos by using AI avatars. It's widely used in training, marketing, and communications for enterprises wanting to make videos without cameras or crews.

D-ID: This service deals in "live portrait" technology, meaning it animates portraits by letting them talk and move. It normally finds application in creating engaging content for marketing and entertainment.

These range from simple, fun applications for casual users to high-end professional software for proficient professionals. Entertainment, marketing, and communication are among those industries whose applications of deepfakes will grow really fast with the advancement of deepfake technology.

What is Social Engineering?

Social engineering means the methods used by hackers to make people believe in them and finally disclose sensitive information, give access to secure systems, or execute certain actions capable of compromising an organization's security. Except for purely technical attacks against the software or hardware vulnerabilities, social engineering attacks exploit the psychological aspects of human behavior, including building trusting relationships, satisfying curiosity, instigating fear, or creating urgency.[10]

Common tactics used in Social Engineering

- **Phishing:** Such emails appear to originate from a trusted authority and attempt to make the victim reveal personal information.
- **Pretexting**: Here, the hacker will only create a scenario through which people will believe in him so that he may be able to get sensitive information.
- **Baiting**: This will attract the user with a nice offer in which one puts his or her security at risk without knowing.
- **Tailgating**: In this, an attacker would tailgate a legitimate user physically into a restricted area so as to gain unauthorized access.

These techniques have proven to be very effective since they bypass all traditional security measures, pointing out how vulnerable human behavior is in the cyber world. In mitigating risks of social engineering, comprehensive training and awareness programs should be inculcated to build a culture of security vigilance amongst employees within an organization.[11]

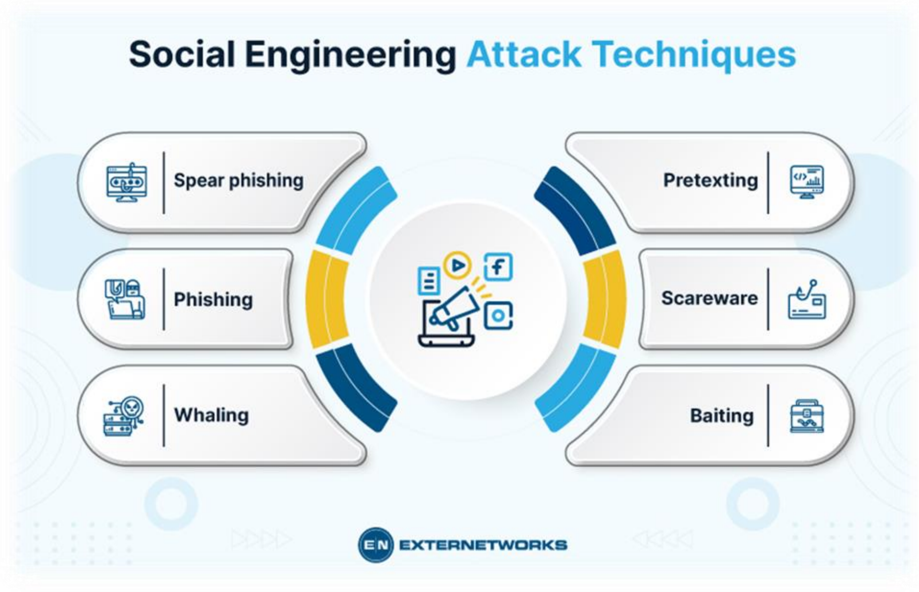


Figure 9 Social Engineering Tactics

Deepfakes in Social Engineering

Traditional social engineering has used devious emails or messages to trick targets into their traps.[4] Deepfake technologies are taking such attacks to a completely new dimension by making them visual and auditory in nature-a trait most of the attacks lack, and therefore much more convincing. Imagine receiving a video call from your supervisor asking you to share restricted information or to conduct a financial transaction. But how would you know for sure it was a scam, if the call sounded legitimate and the voice sounded just like your real boss?

This then raises the ante, in combination with sophisticated audio-visual manipulation, in relation to the danger of becoming its victim. Deepfake technology enables extremely plausible scenarios of how an attack can skip the usual skepticism that exists when receiving pure text-based phishing. As deepfake technology continues to improve, it becomes more and more of a concern for individuals and businesses alike, further demanding increased awareness and strong verification practices.

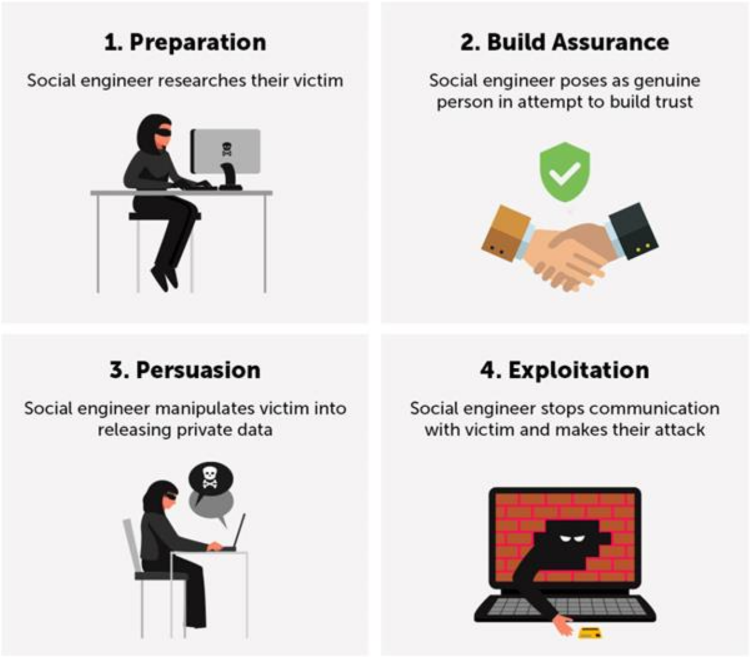

1. Preparation
Social engineer researches their victim
2. Build Assurance
Social engineer poses as genuine person in attempt to build trust
3. Persuasion
Social engineer manipulates victim into releasing private data
4. Exploitation
Social engineer stops communication with victim and makes their attack

Figure 10Deepfakes in Social engineering

Why Deepfakes are effective in Social Engineering

Deepfakes have grown to become a serious asset for cybercriminals,[5] who leverage them to manipulate human psychology based on strong confidence in what is seen and heard. Deepfakes differ from phishing emails or voice phishing calls-the old-school ways of social engineering that generally leave behind telltale signs in the form of misspelled words or awkward tones:

Why Deepfakes Excel in Deception:

- **Authentic Visual and Auditory Cues** - Deepfakes are created to impersonate facial expression, eye movements, and speech that come across as very realistic. Once employees receive video calls that display familiar faces-senior executives or colleagues-they are very likely to respond to a request without suspicion.
- **Real-Time Manipulation** - Advanced deepfake technology allows attackers to create manipulations in real time during live video interactions, making the process of detection quite hard. For instance, a financial specialist may receive an urgent video call from the person who looks and sounds like the chief executive officer, urgently requesting a funds transfer. This deepfake has the capability of responding dynamically to inquiries in a manner no traditional emails or prerecorded messages could.

Figure 11 Deepfakes in Social Engineering ii)

Real World Incidents

I. CEO Voice Sam (2019)

A high-profile incident involved a UK-based energy firm that was tricked into transferring $243,000 to a fraudulent account due to a **deepfake voice attack**. The criminals used AI-generated audio to replicate the **CEO’s German accent** and speech patterns, instructing a company executive over the phone to make an “urgent” payment to a Hungarian supplier.

II. Political Deepfakes: Misinformation and Public Manipulation

Deepfake video of Ukrainian President Volodymyr Zelenskyy pleading with his forces to surrender was published. Concerns were also raised about the possibility of election meddling and political misinformation.

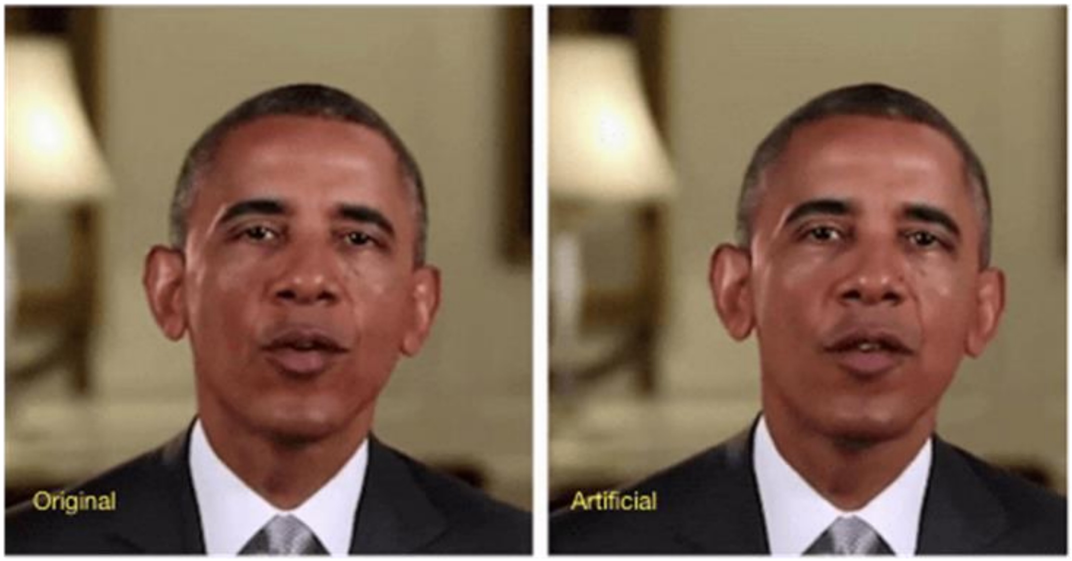


Figure 12 Real World Incidents

Identifying Deepfakes

Deepfakes are realistic, hence, their detection may be difficult, but a few notable signs and some specialized detection tools make that possible. [3]

How to Spot a Deepfake: Key Indicators of Deepfake Manipulation [6]

Inconsistent eye movements - Human eyes blink and move. Deepfakes sometimes stare with fixed gazes or slow blinks, resulting from algorithmic limitations.

Inconsistencies in Shading and Lighting - Observe the inconsistencies of shading and lighting on the face. It would be indicative of manipulation if mismatched light sources or uneven shades characterize how light interacts with the subject's face.

Lip-Sync Issues - One of the Achilles' heels of deepfakes is poorly synchronized lip movements. For instance, some scenarios may include lips not matching complex words or phrases; such can raise suspicion of manipulation.

Face-Background Blending - Observe unnatural blending around the edges of the face, especially the jaw and hairlines. A blurred or serrated edge may be indicative of poor integration with the background.[9]

Deepfake Detection Tools

Deepware Scanner - This tool scans video content for synthetic changes and offers a confidence score by which one could judge how deep faked the content is likely to be.

Sensity AI - Using machine learning, Sensity AI can detect differences in facial expressions and movement; the software produces detailed analysis reports with hotspots of visuals for further review.

Microsoft Video Authenticator -This detects a video frame against pixel-level anomalies, returning a probability score that should then indicate if a video is fake or not.

Knowing these signs and tools can further enhance one's deepfake detection skills and minimize one's chances of becoming a target of fraudulent media.

Future Developments

Anticipated Developments and Issues

Deepfakes in social engineering development are going to be very developed, while a number of trends are most likely to be noticed over the next years. [12]

Greater Realism and Accessibility - As deepfake technology advances, the tools for making realistic deepfakes would surface within a large group of people. That essentially means democratization of deepfake creation, which could lead to increased social engineering attacks since even unsavvy users could make convincing impersonations. [13]

Integration of AI and Machine Learning - Future deepfake systems will most likely integrate advanced AI and machine learning algorithms that could provide very realistic simulations of human behavior, including speech patterns and emotional displays. This allows social engineering tactics to be successful and much more undetectable by the individual from a delineated reality.

The capability for real-time manipulation - Real-time deepfake technologies will, in fact, be able to produce convincing fakes even during live interactions, such as in the course of a video call. Immediacy complicates detection efforts and increases the risk of financial fraud or data breaches.

Targeted attacks - Future deepfakes are very likely to be even more personalized, actually, in which the attacker will engineer contents that would directly attack the use of social media or public personas by specific individuals. This means cybercriminals can analyze data available online in order to compose tailored messages that might take undue advantage of confidence and familiarity for better success.

Legal and Ethical Concerns - The legal frameworks and ethical considerations concerning the application of deepfakes in social engineering may become much more debated with this sudden rise in usage. Specific regulations may be set up in order to reduce deepfake risks and strengthen cybersecurity measures on account of these.

Future-Ready Defense Strategies

While deepfake technology is continuously improving, the elaboration of future-compatible protection approaches will be crucial in mitigating its risks regarding social engineering and other malicious uses.[7] Here are some ways organizations can patch defenses against deepfake threats:

Employee Training and Awareness - Training programs should be in place on a periodic basis, increasing employees' awareness of deepfakes and social engineering methodologies. This ability to identify the risks associated with deepfakes and actually recognize a deepfake allows employees to more appropriately question suspicious communications and prevents them from falling victim to an attack. Regular drills and simulations will help reinforce the lessons learned.

Multi-factor authentication - MFA increases the level of security in which case, even when attackers use deepfake for impersonation of trusted individuals, it would not be that easy to gain unauthorized access. It helps in ensuring that sensitive information is not shared solely based upon visual or auditory cues.

Adopt advanced detection tools - it is expected that organizations will invest in dedicated tools designed for the detection of deepfakes and any other manipulated media. [3]These can analyze video and audio for signs of manipulation-inconsistent facial movements, discrepancies in lighting, speech that sounds unnatural, amongst others. Examples of advanced detection, such as Sensity AI and Microsoft Video Authenticator, are solutions to be incorporated into security protocols.

Verification Culture - A verification culture within the organization will be helpful in motivating employees towards verification of any request of sensitive information or financial transaction through an alternative communication channel, like a call, instead of just relying on visual or auditory confirmation. This practice will assist the organizations in avoiding successful deepfake attacks.

Engaging in Collective Defense - The benefiting can be done by organizations informing each other about the threats and best practices for mitigation. It can also involve collaboration among industry peers, cybersecurity forums, and government agencies to develop better collective defense mechanisms against deepfakes and social engineering.

Legal and Policy Frameworks - The advocacy of more stringent regulations and legal frameworks that address the malpractices of deepfake technology will also somewhat deter malicious actors from the intent. Organizations should also establish internal policies that outline proper use of AI technologies and establish clear consequences for violations.

Regular Security Audits and Assessments - Regular audits of security protocols and systems would contribute to the identification of vulnerabilities that could be attributed to deepfakes. This proactive nature of an organization, in relation to emerging threats, gets to adapt and update its defenses accordingly.

By implementing these strategies, organizations can prepare themselves better for the evolving deepfake technology landscape and the potential implications related to social engineering and cybersecurity.

Conclusion

In this report, I wanted to discuss such a multidimensional topic as deepfakes and their growing importance for cybersecurity in general and social engineering in particular. The investigation started with acquiring a profound understanding of deepfake technology, which demonstrated how the development from basic video and audio editing via sophisticated AI-driven systems powered by GANs happens. It ranged from the whole process of deepfake creation, starting with data collection to preprocessing, model training, and face swapping, including post-processing, with a focus on how technological advances have made deepfakes more accessible and realistic.

Another critical area was deepfakes in social engineering. I analyzed how cybercriminals exploit deepfake technology to make scams more convincing and much more effective. Deepfakes tap into human psychology and the latent confidence we build in relation to the contextual clues provided via visual and auditory hints, something quite impossible to replicate with regular phishing. In this report, synthetic media was considered particularly dangerous, as it could deceive individuals and organizations into taking some kind of action that would have disastrous financial consequences and loss of their reputation.

It also talked about spotting deepfakes by describing some key signs to look out for and what special tools could be useful in that respect. I have further underlined that proactive defense strategies are of essence, like training programs for employees, regular security audits, and the creation of technological solutions that can help fight against the abuse of deepfakes.

The conclusions from this study emphasize the need for heightened awareness and increased vigilance in respect of the threats originating from deepfake technology in social engineering attacks. As the technology continues to evolve, so too must our strategies and approaches to cybersecurity-to make sure that individuals and organizations can recognize such sophisticated threats and counter them. Ultimately, this will help in nurturing a security awareness culture and introducing advanced detection tools that could reduce the risks of deepfakes in the digital space.

References

- [1] Zian Shi, Junyi Teng, Shihao Zheng1, Kaifeng Guo1 “Exploring the Effects of Various Generative Adversarial Networks Techniques on Image Generation” in 2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)
https://vpn.sliit.lk/proxy/60163a0f/https/ieeexplore.ieee.org/document/10409102

- [2] Marjana Tahmid, Md. Samiul Alam , Mohammad Kalim Akram ,“Comparative Analysis of Generative Adversarial Networks and their Variants” in 2020 23rd International Conference on Computer and Information Technology (ICCIT), 19-21 December, 2020.

  https://vpn.sliit.lk/proxy/60163a0f/https/ieeexplore.ieee.org/document/9392660

- [3] JunShuai Zheng [a], XiYuan Hu [b], Chen Chen [c], YiChao Zhou “A new deepfake detection model for responding to perception attacks in embodied artificial intelligence” Available online 19 September 2024, Version of Record 28 September 2024.

  https://vpn.sliit.lk/proxy/60163a0f/https/www.sciencedirect.com/science/article/pii/S0262885624003846

- [4] John Farly , “Deepfake technology: The frightening evolution of social engineering”
[Accessed: Oct. 13, 2024]
https://www.ajg.com/us/news-and-insights/2023/jun/deep-fake-technology-the-frightening-evolution-of-social-engineering/

- [5] Legionoffensivesec, “Deepfakes the New Face of Social Engineering”
[Accessed: Oct. 13, 2024]
https://medium.com/@legionoffensivesec/deep-fakes-the-new-face-of-social-engineering-be67f9431588

- [6] Ian Sample “What are the deepfakes and how we can spot them”
[Accessed: Oct. 13, 2024]
https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

- [7] David Balaban “The Battle Against Fake News Enters The Age Of Deepfakes”
[Accessed: Oct. 13, 2024]
https://www.forbes.com/sites/davidbalaban/2023/05/18/the-battle-against-fake-news-enters-the-age-of-deepfakes/?sh=2fbeb09e67ca

- [8] Meradith Somers, “Deep fakes explained” July 20,2020
  [Accessed: Oct. 13, 2024]

  https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

- [9] Tripwire Integrity management “Deepfakes what are they and how to spot them”
  Posted on February 28, 2023
  [Accessed: Oct. 13, 2024]
  https://www.tripwire.com/state-of-security/deepfakes-what-they-are-and-tips-spot-them

- [10] Kaspersky Lab “What is Social Engineering”
  [Accessed: Oct. 13, 2024]
  https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

- [11] Cisco academy “What is Social Engineering in cyber security”
  [Accessed: Oct. 13, 2024]
  https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html

- [12] The Guardian “The future of undetectable Deepfakes”
  [Accessed: Oct. 13, 2024]
  https://www.theguardian.com/technology/2024/apr/08/time-is-running-out-can-a-future-of-undetectable-deepfakes-be-avoided

- [13] PhD. V.S. Subramanian “The future of Deep fakes”
  [Accessed: Oct. 13, 2024]
  https://buffett.northwestern.edu/news/breaking-boundaries-podcast/future-of-deepfakes-with-vs-subrahmanian.html