Audio-Visual Deepfakes: The Risks and Preventative Measures for Personal Security and Information

Jo Nemanich

CONTENTS

***Abstract*—With the continuous improvement in deepfake media, audio-visual deepfakes pose a great risk to personal security and information. To gain a greater understanding of the potential risks for personal protection, this research first gained an understanding of deepfake creation and potential uses. Following this, cases of malicious deepfake use was explored, as well as legal implications. Measures such as the R.E.A.L. framework were found for personal protection. Searching through current and potential legal policies provided a range of protective measures and legal options for the average individual and potential victim. Findings of cases such as the Dr. Jordan Peterson case and college student Noelle Martin provided proof of potential devastating risks for victims of malicious deepfake media. This paper concludes with an emphasis on knowledge of risks and legal solutions, as well as the importance of ethical computing to assist in managing and preventing future victimization.**

I. INTRODUCTION

Audio-visual deepfakes are posing a threat to personal security and information. Preventative measures are important for the risks involved with deepfakes in media today. With the latest advances in artificial intelligence and machine learning, deepfake content is becoming progressively harder for human observers to detect. Throughout this survey, discussions of what an audio-visual deepfake is, how they are made, how they are used, any existing policies regarding deepfakes, personal protection strategies, and any further ethical issues that stem from audio-visual deepfakes will take place.

II. WHAT IS A DEEPFAKE?

What is a deepfake? "A deepfake is content, generated by an artificial intelligence, that is authentic in the eyes of a human being. The word deepfake is a combination of the words "deep learning" and "fake," and primarily relates to content generated by an artificial neural network, a branch of machine learning [20]." With the use of machine learning, we can create auditory and visual content that can be deemed "real" by the average person. The most common deepfakes seen are visual, but audio-visual deepfakes have become more common. This is something that has great potential for creative content but can also be used unethically to bypass security, threaten privacy, and provide false information.

"Deepfakes are primarily built using "auto encoder," a deep network architecture. Auto encoders are trained to recognize the main features of an input image to recreate it as their output subsequently [15]." Deepfakes utilize one encoder on two networks to compress over latent space to allow the ability to learn from an image and create another using a decoder, producing a deepfake (see Figure 1). The process is broken down into three simple steps:

- The extraction of the original picture
- Putting the original picture through deep learning algorithms to produce a copy of the original
- Placing the copied image is then rendered and put back into the original to produce a deepfake [15].

To extract the original picture from the frame, an encoder is used. "An encoder is responsible for extracting critical characteristics from the input image. The encoder compresses the original image from thousands of pixels to hundreds. These measurements are related to facial features such as movement

of eyes, head pose, skin tone, emotional expressions, etc [15]." Extracting these characteristics is critical for the next step of production. After the picture is extracted from the frame, it is used as an input on deep learning algorithms to produce the necessary copy.

The process of putting the original picture through deep learning algorithms utilizes latent space to produce a copy of the original. "Latent space represents unique facial features on which the image is trained. It is more focused on critical facial features. It excludes the noise/unimportant part of the image, indicating the picture as a compressed version which ultimately helps in memorizing the essential characteristics [15]." This process focuses on the critical features and individual characteristics in the image, while previously when extracting the image, the focus was on characteristics related to the elements that have body language that goes with these critical features and characteristics. After utilizing deep learning algorithms, the now copied image will be rendered and placed onto the copy to complete the deepfake.

To complete the deepfake, the copied image is placed back onto the original and rendered using a decoder. "A decoder decompresses the information in the latent space to reconstruct a look-alike of the original image. The comparison of input and output images provides the performance of the auto encoder. The more the similarity of input and output image, the more the encoder's performance [15]." With the now copied image from the decoder, the auto encoder communicates over a neural network to create the final image, producing the deepfake. "Neural networks are non-linear models for predicting or generating content based on an input. They are made up of layers of neurons, where each layer is connected sequentially via synapses. The synapses have associated weights that collectively define the concepts learned by the model [20]."

III. Types of Deepfakes

There are many types of deepfakes:

- Photo Deepfakes
- Auditory Deepfakes
- Video Deepfakes
- Audio-visual Deepfakes

Photo deepfakes can be used for face and body swapping. An example of a photo deepfake could be an app that alters your face to show what you would look like 60 years from now, or in a business sense, an app that lets you virtually try on clothes [18].

An auditory deepfake can be considered voice swapping or text-to-speech. An auditory deefake could be as simple as an audiobook narration, or using a deepfake of an individuals voice and turning it into text-to-speech, such as the Dr. Jordan Peterson case [14].

A video deepfake entails face-swapping, morphing, and body-puppetry. Face-swapping can be used in the movie industry to replace a body doubles face with the actors face [18]. Morphing is where two faces transition between eachother, such as in an app or a player putting their face onto their favorite video game character. Body-puppetry can be achieved through motion re-targeting to create a deepfake that transposes movement from the source video, such as in this video entitled "Everybody Dance Now" [4].

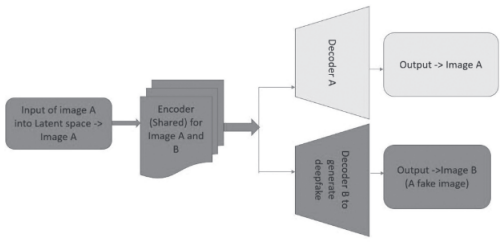

Fig. 1. In the process of creating deepfakes, communication is key over two autoencoders on a network. Shown in the figure above, is the relationship between the autoencoders needed to create a deepfake.

With audio-visual deepfakes, you can create a deepfake that mimics words and movements. An example of this, is a video created by Jordan Peele and Buzzfeed, mimicking President Obama [6]. With advancements deepfakes have made, deepfakes can be useful for content creation and business ventures, whether it's a virtual clothing app or creating different voices for an audiobook reader. With all of these advancements and room for positive opportunity, there is room for negative opportunity as well.

IV. Policies and Personal Protection Regarding Deepfakes

Currently there is a lack of laws and policies regarding criminalizing specifically the usage of deepfakes. "Virginia has passed a law criminalizing deepfakes used in revenge pornography, and Texas has criminalized deepfakes used to influence elections. Massachusetts and California considered but failed to pass bills aimed at countering deepfakes due to concerns about overregulation [21]." The problem currently with creating protective laws and policies is that it is hard to create a law that distinguishes malicious intent from creative parody. There is also concerns with legislating technology and political speech, as it is fraught with difficulty and civil-liberties concerns. While keeping the law in mind, two of the few ways the government can respond to deepfakes includes Technical solutions and Legal solutions. Following these potential responses to deepfakes, there are some prevention techniques that the average user can utilize to try and protect themselves from falling into the trap of misinforming deepfakes.

A. Technical Solutions

Regarding technical solutions, some argue that it is more efficient to utilize detection algorithms versus trying to use the law to regulate deepfakes. The problem with utilizing algorithms as a single solution, is that it will never completely solve the problem, rather manage it. "For example, detection software would have to keep pace with innovations in deepfake technology to retain efficacy. Moreover, if such technology existed and could be deployed through social media platforms, it would only reduce the systemic harms described

above, but by no means eliminate them [12]." The main issue with utilizing detection algorithms is that they will be stuck in a constant cycle with the deepfakes by constantly learning from each other. This is comaparable to CAPTCHA's and how bots are continually getting better at solving CAPTCHAs, forcing bot-detection systems to make the CAPTCHAs more difficult to solve, which the bots eventually learn to beat [5]. Even though technological solutions will not completely solve the issue, they can be used to mitigate the problem. By reducing the problem, the amount of low grade deepfakes can be reduced from media. Algorithms will never completely solve the problem of misinformation, but they can raise the cost and expertise required to spread convincing fake videos [24]. Efforts to mitigate deepfakes with technology has already been taken. The US Defense Advanced Research Projects Agency (DARPA)'s Media Forensics department awarded nonprofit research group SRI International three contracts to find ways to automatically detect digital video manipulations [5]. As efforts to use technology increase, issue with human cognitive bias holds the next barrier. "Detection software might not disabuse certain people's faith in deep fakes, especially those under the profound sway of cognitive bias [12]. Cognitive bias is "A systematic error in thinking that occurs when people are processing and interpreting information in the world around them and affects the decisions and judgments that they make [8]."

B. Legal Solutions

Legal solutions such as laws and policies have faced the issue of civil liberties and free speech. There are little laws currently passed regarding deepfakes directly, but there are current laws to utilize in our legal system today to assist victims of malicious deepfakes. Two ways the law can be used to combat deepfakes are outright banning and civil liability.

"No current criminal law or civil liability regime bans the creation or distribution of deep fakes. A threshold question is whether such a law would be appealing and, if so, constitutionally permissible [12]." As seen above, few laws have been passed regarding deepfakes directly, such as influencing elections and for usage in revenge pornography. Another issue is that not all deepfakes or types of media manipulations are inherently bad, or may not even be used for malicious intent. What if there was a law that required proof of a deep-fake creator's intent of serious harm or malicious intent to assist in reducing concerns about chilling public discourse? Even with a proposal like the one stated, concerns over speech still remain. "The American free speech tradition warns against government having the power to pick winners and losers in the realm of ideas because it will "tend to act on behalf of the ideological powers that be [12]." Attempting to fight the constitutional right of free speech will continually hold a barrier in the legal implications of malicious deepfakes. For example, "in the landmark 1964 decision New York Times v. Sullivan, the Supreme Court held that false speech enjoys constitutional protection insofar as its prohibition would chill truthful speech [12]. And in 2012, "in United States v. Alvarez, the Court went even further. In the plurality and concurring opinions, the Court concluded that "falsity alone" does not remove expression from First Amendment protection [12]."

	Examples	Advantages	Major Concerns	Unintended Consequences	Legal Responses
Deep Fake Pornography (e.g., revenge porn)	One's face transferred onto porn actor's naked body	Could mean opportunities to create more videos, if created with consent	Invasion into autonomy and sexual privacy; humiliation and abuse	Humiliation; exploitation; physical, mental or financial abuse of individuals or corporations	*Public law* (criminal law, administrative action) *Private law* (torts)
Political Campaigns	Speeches of politicians, news reports, information about socially significant events	Could promote freedom of speech	Damage to reputation, distortion of democratic discourse, hostile governments, impact on election results	Eroding of trust in institutions; deepening social divisions and polarisation; damage to national security and international relations	*Public law* (constitutional law, administrative law, criminal law) *Private law* (defamation, libel, slander, torts; copyright law)
Reduction of Transaction Costs	Translating video records into multiple languages	Facilitation of social interactions, creation of new business models	Ownership of IPRs to the content; privacy	Emergence of new data silos	*Private law:* contract and tort law
Creative and Original Deep Fakes	Nicolas Cage scenes, parody memes	Promotion of creativity and science, free speech	Ownership of IPRs, privacy	Bullying among children	*Private law* (fair use and copyright law, contract law, tort law) *Public law:* constitutional law

Fig. 2. This figure provides potential examples of deepfakes used for malicious intent and possible legal solutions. [19]

Civil liability is a legal obligation that requires a party to pay for damages or to follow other court enforcements in a lawsuit [1]. Problems that arise with civil liability are having enough metadata to track who the creator is, if the creator is located outside of the U.S. legal system, and the lack of victims wanting to spend the funds necessary in a legal suit. One way a victim can attempt to use civil liability to their advantage is by attempting to sue the creator of the deepfake. Within the spectrum of civil liability, victims can use laws that already exist to their advantage. As seen in Figure 2, there is a number of different legal responses with laws that already exist for victims of deepfake content (see Figure 2). Victims can sue for copyright, defamation, false light, and emotional distress [16]. Potentially a victim can sue for copyright of their own image only if they took the photos themselves [17]. Using civil liability is the most effective course of action for the victims, but does not prevent malicious deepfakes from appearing. It is a response to a deepfake versus a preventative measure.

C. Prevention Techniques (R.E.A.L.)

One issue found with deepfakes is the potential to easily spread misinformation. A way to combat misinformation as an individual is utilizing prevention techniques such as the R.E.A.L. proposal and knowing key features to look for to identify deepfakes with your own eyes.

As proposed in [18], a framework called R.E.A.L. was presented for managing deepfake risks and to assist in giving the everyday user techniques to combat deepfakes:

1) Record original content to assure deniability
2) Expose deepfakes early
3) Advocate for legal protection
4) Leverage trust (see Figure 3).

Step 1 of the REAL framework: For recording original content to ensure deniability, individuals will have to create evidence to support themselves. This will be to contrast malicious deepfakes, which often falsely portray someone saying or doing something. Providing this data is referred

to as an alibi service or a life log [13]. This will involve technology that can track and log a person's life in terms of location, communications, and activities [18]. The problem seen with this is a potential negative impact on privacy. From a technology perspective; mobile, wearable, and smart devices readily available can make collecting such data possible to some extent [18]. This data could be potentially stored and used to identify dark deepfakes.

Step 2 of the REAL framework: Exposing deepfakes early not only references step one of REAL by the personal responsibility of preparing for malicious content, but also the technology regarding deepfakes. "Thus, just as we adopt and develop the technological innovations that gave us deepfakes, there are technological innovations being developed to detect and classify them. These include using AI techniques to identify resolution inconsistencies; the scaling, rotation, and splicing of content that is often central to the creation of a deepfake; and the eye-blinking patterns of the human images [18]." Technology detecting deepfakes can be a vicious cycle, as stated above, but utilizing the technology we have is essential to the REAL framework outline. The international professional services firm KPMG advised that "establishing a governance framework that embraces disruptive technologies and encourages innovation while ensuring risks are identified and managed is essential to an organization's ability to survive and thrive in a digital world [9]."

Step 3 of the REAL framework: Advocating for legal protection is essential to step three of the REAL framework. "Victims should have legal recourse in instances of defamation, malice, breach of privacy, or emotional distress caused by deepfakes, as well as in cases of copyright infringement, impersonation, and fraud involving deepfakes [18]." As discussed earlier in this paper, civil liability covers legal instances like these. It is important to know the basic outline of what these legal instances entail and your options as a potential victim (see Figure 2).

Step 4 of the REAL framework: Leveraging Trust involves a give and take relationship. "When brands that are built on strong ethics are portrayed in an unfavorable light in deepfakes, the hope is that stakeholders will not simply believe their eyes and ears but be more critical and think for themselves [18]." Leveraging trust can be best seen when brands work towards delivering what they promise and making sure they are promoting and protecting customer relationships. "Strong brands will be better positioned to weather deepfake assaults as their stakeholders will want defend the brand [18]." This also involves promoting ethical computing, as not only a way to deter malicious deepfakes, but to promote trust in technology and creators.

V. Deepfake Cases

Though deepfakes have the potential to produce new content in a fresh and fun way, the potential security implications grow a stronger concern (see Figure 4). Deep learning techniques are improving every day, which also is improving the quality of deepfakes. Technology, especially video chat has become a social norm over the past few years due to the recent pandemic,

Fig. 3. This figure provides the outline of the REAL framework [18].

this grows a concern for the usage of audio-visual deepfakes. This can also increase an issue in the political world as well, where a video made of a politician saying or doing something can be career ending or produce faulty information to cause strife between parties. Three notable case types of malicious deepfakes are as follows:

- Puppeteering
- Revenge Porn
- Transaction Scams

A. Puppeteering

For example, a website was created to mimic a Dr. Jordan Peterson. The website claimed itself to be a neural network and not the real Dr. Peterson. The site told the user to type some text into a box, that would be fed into a neural network trained on hours of Peterson's actual voice and generated into audio that sounded a lot like the real thing [14]. This became a huge problem as videos surfaced of Dr. Peterson repeating vulgar phrases and much more. This shows that even as a smaller public figure, you are at risk for a larger scheme such as this where your image and words can be stolen to create a deepfake.

B. Revenge Porn

Another notable case of a malicious deepfake is a video of actress Gal Gadot having sex with her stepbrother on the internet. The video is a face-swapped Gal Gadot to look like she's performing in an existing incest-themed porn video [3]. The most notable aspect of this is that "deepfakes use open-source machine learning tools like TensorFlow, which Google makes freely available to researchers, graduate students, and anyone with an interest in machine learning [3]." This shows that access to tools to make a deepfake such as this is relatively accessible to anyone. Having a wide range of accessibility provides means to individuals looking at creating revenge porn with a malicious deepfake. Tools such as the Adobe tool which can make people say anything and the Face2Face algorithm that can swap a recorded video with real-time face tracking are available to anyone [3]. There are many cases of celebrity deepfakes in the media, but there also is cases of revenge porn for the average person as well. "Noelle Martin was an 18-year-old law student when, late one night, she did a reverse Google image search out of curiosity, uploading a

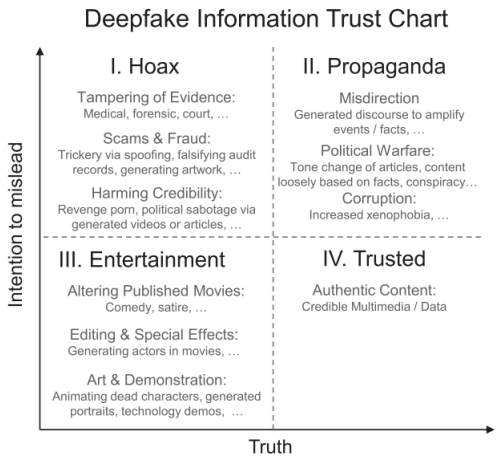

Fig. 4. This chart describes four categories of deepfake information types. It describes the relationship of information, truth and trust.

photo of herself to see where else it was on the internet. Instead of finding friends' social media pages, she found hundreds of explicit images of her face photo-shopped onto the bodies of porn actresses engaged in sexual acts [22]." This further shows that anyone is at risk of being a revenge porn victim. In another instance, in 2019 an anonymous programmer created a new app called DeepNude that used AI to create nonconsensual porn. If you fed it a picture of a clothed woman, it removed her clothes so that she appeared naked. DeepNude was shortly removed a few months later due to ethical backlash [23].

C. Transaction Scams

There was another instance where "criminals scammed a British energy company for $243,000 by spoofing a high-level executive's voice with AI and calling to demand payment [21]." This is not only a threat to major companies, but simply to an individual picking up the phone to a scammer call. These are known as transaction scams, where scam creators target individuals convince them through a deepfake to make certain payments [15]. These are just a few examples of the risks to personal privacy, security, and personal information. As deepfakes get stronger, so do threats such as these become a serious reality for the average person.

VI. Ethical Computing

A. Ethical issues

With deepfakes having the potential for a large amount of malicious content, ethics comes into question. Though it may seem like a great business venture for a company such as audible to utilize a deep auditory fake, is it ethical to replace the person who relies on that job as a reader with a machine? Deepfakes are only going to continue to improve as they use deep learning algorithms. Will we continue to see deepfakes used in a non-malicious way for a business just to replace a working individual? Though the deepfake is being used for growing the business, taking the job from a person could be considered a question of ethics. Or the ethics behind copying another person's likeness, such as a celebrity and using them within a seemly harmless body swapping app. For example, a video face-swapping Jim Carrey and Alison Brie created using DeepFaceLab was made and put onto youtube [7]. Looking at this initially, it is a seeminly harmless video, but is it a victimless crime? The celebrities in the video did not consent to their portrayal in the deepfake and potentially may object to the portrayal strongly. "The same technology that made the Carrey/Brie face-swap entertaining, for instance, was used time and again to transplant the face of Scarlett Johansson and many of her famous contemporaries onto the bodies of actors in adult videos [18]." The same video made as a form of entertainment, also unfortunately contributed to revenge porn. Deepfakes are only going to continue to learn and be used in media, where anyone can be a target.

B. Importance of Ethical Computing

What is the significance of ethical computing in regards to personal protective measures from malicious deepfake content? The most important note is, promoting ethical computing is a protective measure. First we must ask, are deepfakes an ethical tool? "The term 'greyfakes' has been used to pinpoint the blurred line between the positive and negative impacts of deepfake technologies [11]." Ultimately, you cannot completely remove deepfake content due to the fact that there is positive entertainment and content of value that has been created using this technology. Ethical concerns arise as deepfake media is extremely present and continuing to grow and become more available to the average individual. Ethical Computing is key to creating protective measures such as REAL and for finding and creating policies to help victims. Ways to promote ethical computing that work line with the REAL framework as a personal protective measure are as follows:

- Immediately deterring the creation of socially harmful deepfakes
- Making sure that lawmakers and regulators are knowledgeable about the technical details and implications of deepfake technology
- The availability of accurate resources to deal with the harmful implications of deepfake technologies (i.e. anti-misinformation and deepfake detection tools)
- Economically encouraging anti-deepfake measures that target the harmful aspects of deepfakes, as well as legally deterring those harmful aspects at the same time [11]

VII. Future Trends

The future of deepfake media resides in the current risks being faced and the potential improvements of deepfake content with improvements in artificial intelligence. Increasing the knowledge to the average media user becomes evermore important as tools to create deepfakes continue to become more available.

A. Growing Availability of Deepfake media

Research by DeepTrace suggests, "Publication of more experimental work and extension to new applications is indicative of these ideas potentially being transferred into reusable

code and more reliable and efficient tools that can be used by nonexperts." Deep Trace also noted that deepfake creation communities are growing. Github, 4chan, 8chan, and other forum-based websites all share open-source deepfake code [2]. As creation communities such as these are growing, that future availability to the average user grows rapidly. "The commodification of deepfake creation tools on these platforms will likely lead to the technology perpetuating harmful and malicious use cases, like cyber-bullying or political propaganda [2]."

B. Importance of Knowledge

With the growing availability of deepfake technology, it becomes increasingly important to provide knowledge to regular media users about deepfake media. As stated in the technical analysis portion of this paper, knowledge is power and safety in regards to fighting malicious deepfakes. Iproov conducted a global study in 2019 and again in 2022 regarding public deepfake media knowledge and compared the results. As seen in Figure 5, The first question asked was "What is a Deepfake?":

- Globally, 71% of respondents say that they do not know what a deepfake is. This results in under a third of global consumers claiming they are aware of deepfake media.
- Mexico and the UK are most familiar with deepfakes: 40% of Mexican respondents and 32% of UK respondents say they know what a deepfake is.
- Spain and Germany feel the least educated about deepfakes: 75% of respondents in both Spain and Germany answered "No". [10]

These results are significant as deepfakes have significant potential for misuse. When media users simply are not aware of what they are, they are less likely to be prepared to identify when they are encountering malicious content. The percentage of people who know what a deepfake is has more than doubled since Iproov's last survey – in 2019, only 13% said they knew what a deepfake was, compared with 29% in 2022 [10]. There is a positive show in awareness as deepfake threats continue to grow, but it is concerning that only 29% of people are aware of deepfakes in 2022.

VIII. Conclusion

Audio-visual deepfakes are becoming a stronger tool and threat every day. There is a number of different types of deepfakes with different implied risks. As there are many benefits in the world of business ventures and content creation, the risk audio-visual deepfakes poses on privacy and security is a harsh reality. Not only is there a risk with deepfake technology, but a large ethical discussion as well. Through policy awareness and personal protection, the potential for security and privacy risks can potentially be mitigated. It is imperative to stress the importance of ethical computing to

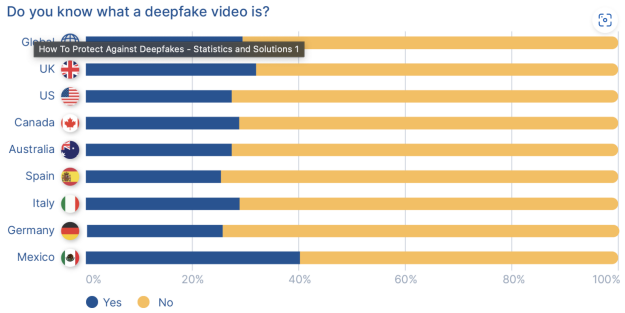

Fig. 5. This graph shows the results of Iproov's 3 year global study of public deepfake knowledge. This chart specifically shows the percent of average media users who are aware of what a deepfake is.

assist in creating a media space that is safe, knowledgeable, and promotes activism against malicious media. Deepfakes and the risks they bring will not go away, but by utilizing protective frameworks such as REAL and being educated on legal solutions with an emphasis on ethical computing, future victimization can be managed and prevented.

IX. Previous coursework CSCI reflection

Reflecting on my past 4 years at CSBSJU, a few courses come to mind for my performance in CSCI 373. I believe it is important to mention the initial computer science course CSCI 150 as it was the first foundational class taken within this major and I am now completing the final step with this capstone course. It is important to note that most past CSCI classes have played a role in my development in the major, specifically for this class and my research I believe that CSCI 332 Machine Learning and CSCI 338 Algorithms and Concurrency were the most helpful in my research process about deepfakes. I also would like to give Dr. Heather Amthauer, who taught the above courses, a special thanks for assisting me in finding a direction for my research. I believe this goes to show the strength of the computer science department at CSBSJU, as all the instructors are willing to help build strong researchers. This research project deepened my knowledge in computer science immensely. The amount of academic media searching I did to find good research was something I have never had to do in any previous course. I also made sure to attempt to make small advances on my research and writing throughout the semester, versus letting my procrastination tendencies take over. I gained an understanding of not only researching skills, but basic Latex skills, technical writing skills, and staying up to date on current computer science news and media. I was able to integrate previous course knowledge and work with the instructor of that course to assist in my research process.

References

[1] Civil liability.
[2] how deepfakes evolved so rapidly in just a few years, url=https://www.fastcompany.com/90414479/how-deepfakes-evolved-so-rapidly-in-just-a-few-years.
[3] Ai-assisted fake porn is here and we're all fucked, Dec 2017.
[4] *Everybody Dance Now*. YouTube, Aug 2018.
[5] There is no tech solution to deepfakes, Aug 2018.

[6] *You Won't Believe What Obama Says in This Video*. YouTube, Apr 2018.
[7] YouTube, Aug 2019.
[8] Evaluating fake news misinformation, Oct 2020.
[9] Four steps to emerging technology governance, Mar 2021.
[10] Deepfake statistics amp; solutions: Protect against deepfakes, Sep 2022.
[11] Arnold. Are deepfakes ethical in a world of media manipulation?, Apr 2020.
[12] Robert Chesney and Danielle Keats Citron. Deep fakes: A looming challenge for privacy, democracy, and national security, Jul 2018.
[13] Danielle Citron and Robert Chesney. Deepfakes and the new disinformation war, Sep 2022.
[14] Samantha Cole. A site faking jordan peterson's voice shuts down after peterson decries deepfakes. vice, 2019.
[15] Loveleen Gaur. *Deepfakes creation, detection, and impact*. CRC Press, 2023.
[16] David Greene. We don't need new laws for faked videos, we already have them, Feb 2018.
[17] Esq. Jeffrey Yano. Can you legally swap someone's face into porn without consent?, Mar 2019.
[18] Jan Kietzmann, Linda W. Lee, Ian P. McCarthy, and Tim C. Kietzmann. Deepfakes: Trick or treat? *Business Horizons*, 63(2):135–146, 2020. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING.
[19] Edvinas Meskys, Julija Kalpokiene, Paulius Jurcys, and Aidas Liaudanskas. Regulating deep fakes: Legal and ethical considerations, Dec 2019.
[20] Yisroel Mirsky and Wenke Lee. The creation and detection of deepfakes: A survey. *ACM Comput. Surv.*, 54(1), jan 2021.
[21] Arthur Nelson and James A. Lewis. Trust your eyes?: Deepfakes policy brief. Technical report, Center for Strategic and International Studies (CSIS), 2019.
[22] ABC News. 'humiliated, frightened and paranoid': The insidious rise of deepfake porn, Aug 2019.
[23] Sigal Samuel. A guy made a deepfake app to turn photos of women into nudes. it didn't go well., Jun 2019.
[24] Conrad Stosz. Policy options for fighting deepfakes, Jul 2019.

APPENDIX

List of figures

Below is my statement on how I have addressed all writing rules listed on page 25:

Rule 1: Assume your reader is intelligent but ignorant.

-My paper has an introduction included and is easily accessible to non-experts.

-I think my introduction could use some work

Rule 2: Tell them what you will say, say it, and tell them what you said, and more. Use the conclusion to make your final clear points, synthesizing content.

-I included in my introduction what I planned to say, throughout the paper I used those points as sections, withing the sections I "told them what I said, and more", and I used the conclusion to make my final clear points.

- I believe my conclusion could use work

Rule 3: Define all terms and acronyms.

-Any unfamiliar terms or acronyms were given the proper definition and description

Rule 4: When possible, use plain language and avoid jargon.

-Attempted to use enough words, not more. Attempted to avoid informal language

Rule 5: Make consistent use of terms and notation.

-I have read through my paper and made sure terms were being defined.

Rule 6: Search the literature and cite other works.

-I have 20 sources in my paper currently, at least 10 are high-quality

Rule 7: Use pictures, charts and graphs, but keep in mind rule 4.

-I have four figures included in my paper. I provided a descriptive caption for each and used them accordingly throughout the paper.

-I could improve my captions

Rule 8: Use examples to explain complex ideas.

-I attempted to use examples that are easy to understand to assist in describing complex topics

Rule 9:

-Headings (sections) and bulleted lists were included in the paper. The paper has a structure to it

Rule 10:

-I have provided navigational guidance such as a abstract, table of contents, and appendix.