Article Review #2 - Types of Image Content Related to Societal Norms

Collin Sloan

UIN - 01267943

CYSE 201S: Cyber Security and the Social Sciences

Diwakar Yalpi

April 6, 2025

Relation to Social Sciences

Deepfake technology is utilized in the process of taking an image or video and mapping a person's face then putting that face on the person in the image or video. This technology has evolved a great deal in the past few years. The onset of this type of technological advancement allows for members of society to create characters often fictionally that hold a true representation of a powerful message unique to them in some way. It is through these connections that powerful messages in private or professional realms can be shared amongst various societal groups. In essence the power of technology allows for the power of expression to be shown even more digitally with this concept utilization.

In some instances, it is difficult to decide whether or not something is a true photo or video of someone or it is a deepfake. Deepfakes could pose true danger in the field of social science and society as anyone could create these deepfake images or videos, with the technology becoming more widely available. People may create deep fake images in an innocent manner but the image could be hacked and utilized for malicious purposes. For example, a video could be made of a person giving their opinion on various topics that could be seen as controversial, then using this deepfake technology, the user could import anyone's face into the video to make it seem as if they are giving their own opinions. In conjunction with Artificial Intelligence (AI) voice generators, anyone could be at risk of having their image manipulated and tarnished with this technology. With how this technology is developing, it is becoming increasingly difficult for the general public to spot the difference between real image and video and deepfake ones.

Research Questions

Research questions that could address this new deepfake technology opportunity include "What are signs that an image or video is a deepfake?" or "How to check image data to determine if it was altered?". While deepfake technology is advancing, it is not a perfect piece of content. There are sometimes flaws in the finished product that could show whether or not this image or video has been altered. Another way to determine if an image was altered is to check the image data. Every electronic picture or video has information associated with it when you inspect it. These image data parameters such as device, location and date identify the photo or image representing the time uniqueness to the user. In essence, the validity of the content is verified in an original image or video. By inspecting an image with these parameters, it is possible to see if it was altered in any way from when it was originally taken. Members of society often worry that they may not be able to decipher between a real image and a deepfake altered image in their life experiences. Knowing what information to trust, is an important step to maintaining digital integrity within societal groups.

Research Methods

The data presented in this article was gathered via descriptive research as well as quantitative research. By definition, descriptive research is the process of making observations with great detail, which is done when looking at the results of the general public attempting to find the truth between reality and deepfakes. The descriptive research methods can be noted in the publication of Bray et al., 2023 that involved the concept of the following descriptive methodology information.

> Deepfake generation processes can be conceptually identical to processes that were previously possible, such as the seamless transplantation of one human face onto another within video footage. This example is achievable either through a manual or computational process that involves cutting and pasting, frame-by-frame, parts of existing footage onto the target footage.(para. 2)

Also, Quantitative research methods were utilized with interesting methodology. By definition, Quantitative research methods involve the process of analyzing statistical data which was done once the descriptive research yielded research structure. The quantitative research methods included "First, the authors of the study do not report standard errors or inferential statistics and so it is not possible to determine if accuracy varied in a reliable way across the three deepfake dataset conditions."(Bray et al., 2023) It is through these types of instances of statistical data research methodology that the power of unique personal content pieces or deepfake ones that cross references can be made by both Individuals and hackers alike.

Data Analysis

The data collected throughout this article was analyzed via statistical analysis. By looking at the statistics gathered with the two different research methods, conclusions were made based on the information. From the article, "Thus, although participant accuracy was 62% overall, this accuracy across images ranged quite evenly between 85 and 30%, with an accuracy of below 50% for one in every five images."(Bray et al., 2023) we are able to deduce that some images using deepfake are easier to spot than others. This data reference shows that in essence people are correct to question validity in images, videos or anything in a digital format to remain safe in

online environments within their own world structure. Pictures or videos should be reliable but sadly they are not always what they seem to be. Thus, the emerging digital environment our new world as a society represents. By the data provided, the accuracy number percentages are not showing a true confidence in the notability of detecting the original content from the deepfake content.

Powerpoint Information in Relation to the Article

The conceptual content is related to the allowance and notification of deepfake content detection in various facets. People are a vital piece of this research process. Research methods are used to match the research questions to the target group being studied. In an effort to gain the needed information, people were contacted.Surveys were conducted to describe the methods for noticing real content from deepfake content in image or video media.

The content references the study of psychology being the study of the mind. The mind is very powerful and connects content to reference points that can vary between Individuals. The perception ability of a person being able to spot an authentic piece of content over a deepfake one primarily depends on perception. The avenue of perception is related to the concepts that make up the psyche of the individual. One person can possibly spot one content piece over another only due to vantage point of reference all based on what is in their mind.

Relation to Marginalized Groups

The existence of unique content or deepfakes create a boundary for the safety of marginalized groups in society. The outlying groups represent unique subsets of Individuals that

can be tricked into believing deepfakes and acting accordingly. It is through the enhancement of comfort level strategies that differences can be noted. These differences can range from believing if the content is real or deepfake or whether to act on the underlying message from the content itself. It is through the creation of deepfake content that mixed messages can be misconstrued by groups in these outer ranges. Content such as these pieces is created so it has a negative connotation in the sense that it can be used to make someone look bad to others thus tarnishing their outward image. This concept is related to marginalized groups as it could be used to target different members of different marginalized groups in a negative way to make them look bad or complete acts they would not normally take part in themselves. For example, someone could make a deepfake of a person to try and extort them for money. The marginalized person in one of these outlying societal groups would not necessarily know whether or not to believe the realization of the content. It is extremely important to be able to tell the difference between the truth in original content and deepfakes as there could be true consequences to the people involved in the deepfaked image or video.

Overall Contributions to Society

The contributions to our society with respect to deepfake images is very powerful, especially with the increased usage of social media. These reels show multiple videos that send powerful messages to Individuals. The message provides the thought yet it is the decision of the person to understand what they are seeing to be deemed real and act accordingly. The concept of deepfake content creates a heightened multi-tiered level of unrest such as fear and concern among members of societal groups. The initial notification of an image being real or deepfake is concerning to societal members. Consequently, the next stage of the analysis of the content stems

from their own perception between right and wrong. The fact that they may not know how to differentiate between original and deepfake content all stems from aspects in their own unique skill set within their mind. Aspects of the contributions to society members from the power of the image itself. Deepfakes contribute a level of unease within societal members. With this technology, someone could make harmful fake videos or images to sully a person's name. This action could make people worry that they may be targeted in the future if they make a bad impression on someone. Technology has created a heightened level of fear when they do not know if they should believe the message that the content is sharing with them as true. It is especially powerful to see the data from the research methods with such a low confidence of differentiation for these original versus deepfake pieces of content as understood by our societal groups. It is through recognizing the differences and showcasing how that media pieces affect the group members.

Conclusion

The tests have been executed and the data has been collected so at this point conclusions can be drawn. These tests create both a test group and the testable group of people when both groups could have differing responses. Vantage points are often a large part of the decision making process. It is through these actual decisions that unique content can be compared to deepfake content pieces. Sadly, there is low confidence for the skill set of the notification of these two types of content pieces. People need to remain vigilant to themselves to think about all of the reasons why the content might be accurate and unique in nature.

Source

Sergi D Bray, Shane D Johnson, Bennett Kleinberg, Testing human ability to detect ‘deepfake’ images of human faces, Journal of Cybersecurity, Volume 9, Issue 1, 2023, tyad011, https://doi.org/10.1093/cybsec/tyad011

Link to Article -

https://academic.oup.com/cybersecurity/article/9/1/tyad011/7205694?searchresult=1

Title of Article - **Testing Human Ability to Detect ‘deepfake’ Images of Human Faces**