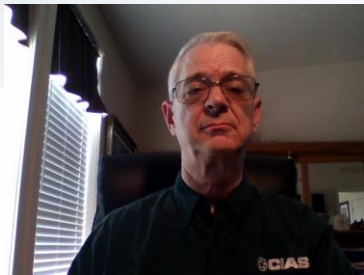
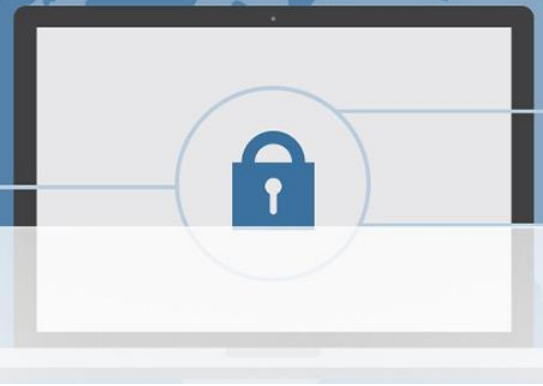
Deepfakes
Part 2. What is the Future?

WYOCAN
WYOMING CYBERSECURITY ACTION NETWORK

Gregory B. White, Ph.D.
Aug 2021



Brought to you by your local library and the Wyoming CAN Committee



WYOCAN
WYOMING CYBERSECURITY ACTION NETWORK

SPECIAL AGENT
DIVISION OF CRIMINAL INVESTIGATION

MANUFACTURING WORKS

Wyoming SBDC Network

Laramie WYOMING

Wyoming Rural Water

wyfi
Wyoming Financial Insurance, Inc.
Established 1990
Subsidiary of WSBCN

UWIT TRAINING

FIRST FEDERAL BANK & TRUST

Meridian Trust FEDERAL CREDIT UNION

Campbell County Health

CYBER WYOMING

CYBERWYOMING ALLIANCE
AWARENESS • EDUCATION • OUTREACH

Wyoming STATE LIBRARY

WYOMING HOMELAND SECURITY
Prevention
Protection
Mitigation
Response
Recovery

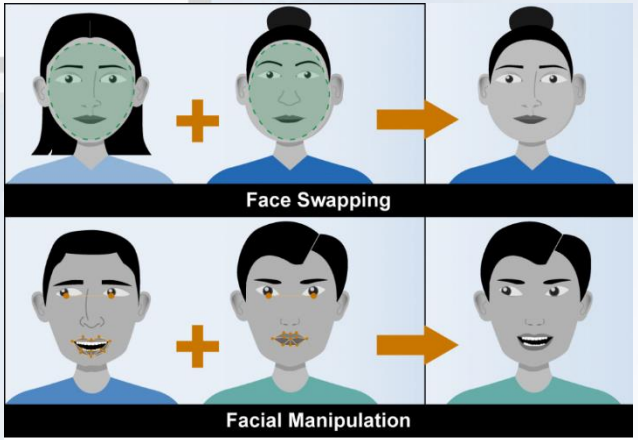
CSB CHEYENNE STATE BANK

JONAH BANK® OF WYOMING

Deepfakes

Review from part 1

- "The term *deepfake* is typically used to refer to a video that has been edited using an algorithm to replace the person in the original video with someone else (especially a public figure) in a way that makes the video look authentic."
    - From: https://www.merriam-webster.com/
    - Image from: **https://iwar.org.uk/2020/02/20/science-tech-spotlightdeepfakes/**



Source: GAO. | GAO-20-379SP

Review

- Pictures may not be worth a 1000 words anymore!

- Neither are videos.
- What might be the impact of a deepfake video on an election if introduced without time to determine if it was fake or not?
- As technology progresses, this may very well become a significant issue.

» **Image from: https://thegadgetflow.com/blog/what-are-deepfakes/**

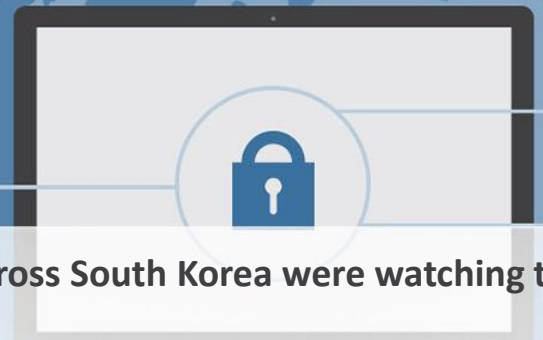
Future

- Deepfakes carry a negative connotation. Are there legitimate uses of the technology?

- Users of the technology in fields such as education, the news media, and entertainment have used different terms to describe the technology.
  - “AI-generated videos”, or “synthetic media”

Image from: https://www.weforum.org/agenda/2018/11/deep-fakes-may-destroy-democracy-can-they-be-stopped/

Legitimate Use

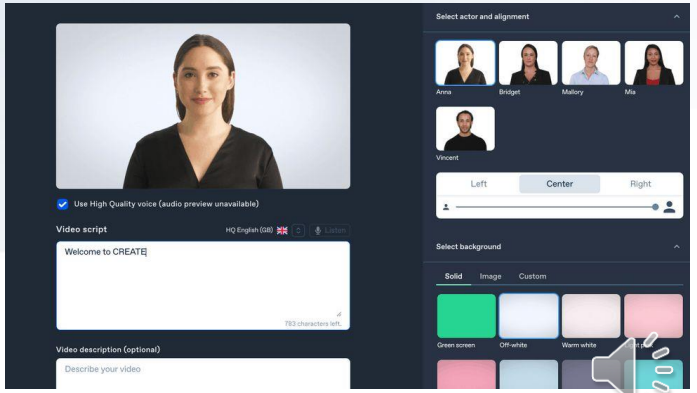


- **“A few months ago, millions of TV viewers across South Korea were watching the MBN channel to catch the latest news.**
- At the top of the hour, regular news anchor Kim Joo-Ha started to go through the day's headlines. It was a relatively normal list of stories for late 2020 - full of Covid-19 and pandemic response updates.
- Yet this particular bulletin was far from normal, as Kim Joo-Ha wasn't actually on the screen. Instead she had been replaced by a "deepfake" version of herself - a computer-generated copy that aims to perfectly reflect her voice, gestures and facial expressions.
- Viewers had been informed beforehand that this was going to happen, and **South Korean media reported a mixed response after people had seen it.** While some people were amazed at how realistic it was, others said they were worried that the real Kim Joo-Ha might lose her job.
- MBN said it would continue to use the deepfake for some breaking news reports, while the firm behind the artificial intelligence technology - South Korean company Moneybrain - said **it would now be looking for other media buyers in China and the US.**

https://www.bbc.com/news/business-56278411

Legitimate Use

- “…usage is growing rapidly in sectors including news, entertainment and education, with the technology becoming increasingly sophisticated.
- One of the early commercial adopters has been Synthesia, a London-based firm that creates AI-powered corporate training videos for the likes of global advertising firm WPP and business consultancy Accenture.
- "This is the future of content creation," says Synthesia chief executive and co-founder Victor Riparbelli.
- To make an AI-generated video using Synthesia's system you simply pick from a number of avatars, type in the word you wish for them to say, and that is pretty much it.

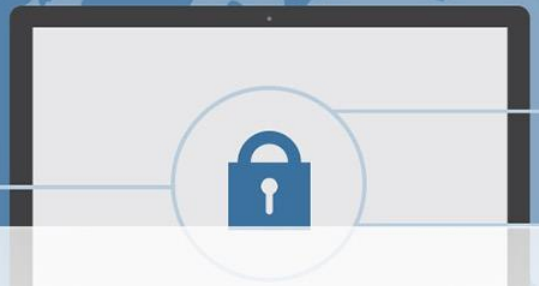


https://www.bbc.com/news/business-56278411

Legitimate Use

"This is why deepfakes are good The good side of deepfakes Deepfakes explained" https://www.youtube.com/watch?v=Nn99WfK9PIk&t=7s

How to Handle Them

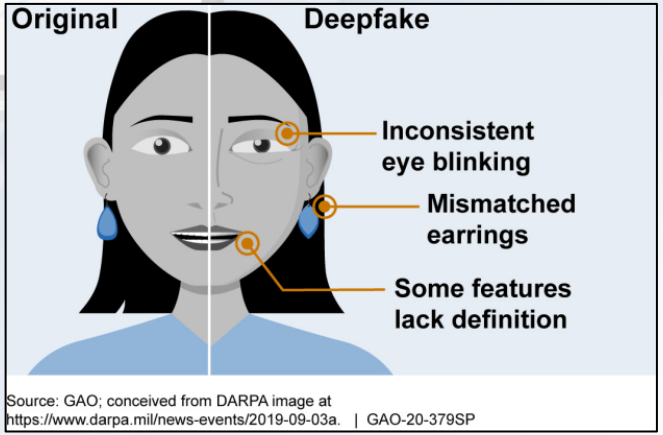


- “Deborah Johnson, professor of applied ethics, emeritus, at the University of Virginia, [stated] "Deepfakes are part of the larger problem of misinformation that undermines trust in institutions and in visual experience - we can no longer trust what we see and hear online.
- "Labelling is probably the simplest and most important counter to deepfakes - if viewers are aware that what they are viewing has been fabricated, they are less likely to be deceived.“”

https://www.bbc.com/news/business-56278411

Detection

- In order to not be deceived, researchers are exploring methods to detect deepfakes.



- "… current DeepFake algorithms can only generate images of limited resolutions, which are then needed to be further transformed to match the faces to be replaced in the source video. Such transforms leave certain distinctive artifacts in the resulting DeepFake Videos"
  - "Exposing DeepFake Videos By Detecting Face Warping Artifacts" , https://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Li_Exposing_DeepFake_Videos_By_Detecting_Face_Warping_Artifacts_CVPRW_2019_paper.pdf

Image from: https://iwar.org.uk/2020/02/20/science-tech-spotlightdeepfakes/

Thank you for attending the Cyber-in-a-Box Library Program

WYOCAN
WYOMING CYBERSECURITY ACTION NETWORK

Visit us at www.wyocan.org