KSU Proceedings on Cybersecurity Education, Research and Practice

2022 KSU Conference on Cybersecurity Education, Research and Practice

Nov 14th, 9:05 AM - 9:30 AM

What You See Is Not What You Know: Deepfake Image Manipulation

Cathryn Allen
Kennesaw State University, cyalle7394@ung.edu

Bryson Payne
University of North Georgia, bryson.payne@ung.edu

Tamirat Abegaz
University of North Georgia, tamirat.abegaz@ung.edu

Chuck Robertson
University of North Georgia, Chuck.Robertson@ung.edu

Allen, Cathryn; Payne, Bryson; Abegaz, Tamirat; and Robertson, Chuck, "What You See Is Not What You Know: Deepfake Image Manipulation" (2022). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 2.
https://digitalcommons.kennesaw.edu/ccerp/2022/Research/2

Abstract

Research indicates that deceitful videos tend to spread rapidly online and influence people's opinions and ideas. Because of this, video misinformation via deepfake video manipulation poses a significant online threat. This study aims to discover what factors can influence viewers' capability of distinguishing deepfake videos from genuine video footage. This work focuses on exploring deepfake videos' potential use for deception and misinformation by exploring people's ability to determine whether videos are deepfakes in a survey consisting of deepfake videos and original unedited videos. The participants viewed a set of four videos and were asked to judge whether the videos shown were deepfakes or originals. The survey varied the familiarity that the viewers had with the subjects of the videos. Also, the number of videos shown at one time was manipulated. This survey showed that familiarity of subjects has a statistically significant impact on how well people can determine a deepfake. Notably, however, almost two thirds of study participants (102 out of 154, or 66.23%) were unable to correctly identify a sequence of just four videos as either genuine or deepfake. Overall, the study provides insights into possible methods for countering disinformation and deception resulting from the misuse of deepfakes.

Disciplines

Information Security | Management Information Systems | Technology and Innovation

What You See Is Not What You Know: Deepfake Image Manipulation

Cathryn Allen
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, GA, USA
cyalle7394@ung.edu
0000-0001-5552-968X

Bryson R. Payne
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, GA, USA
bryson.payne@ung.edu
0000-0003-4539-0308

Tamirat T. Abegaz
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, GA, USA
tamirat.abegaz@ung.edu
0000-0003-1263-8469

Chuck Robertson
Department of Psychological Science
University of North Georgia
Dahlonega, GA, USA
chuck.robertson@ung.edu
0000-0003-0476-9119

***Extended Abstract*—Research indicates that deceitful videos tend to spread rapidly online and influence people’s opinions and ideas. Because of this, video misinformation via deepfake video manipulation poses a significant online threat. This study aims to discover what factors can influence viewers’ capability of distinguishing deepfake videos from genuine video footage. This work focuses on exploring deepfake videos’ potential use for deception and misinformation by exploring people’s ability to determine whether videos are deepfakes in a survey consisting of deepfake videos and original unedited videos. The participants viewed a set of four videos and were asked to judge whether the videos shown were deepfakes or originals. The survey varied the familiarity that the viewers had with the subjects of the videos. Also, the number of videos shown at one time was manipulated. This survey showed that familiarity with the subject(s) depicted in a deepfake video has a statistically significant impact on how well people can determine it is a deepfake. Notably, however, almost two-thirds of study participants (102 out of 154, or 66.23%) were unable to correctly identify a sequence of just four videos as either genuine or deepfake. The potential for deepfakes to confuse or misinform a majority of the public via social media should not be underestimated.**

This study provides insights into possible methods for countering disinformation and deception resulting from the misuse of deepfakes. Familiarity with the target individual depicted in a deepfake video contributed to viewers’ accuracy in distinguishing a deepfake better than showing unaltered authentic source videos side-by-side with the deepfakes. Organizations, governments, and individuals seeking to contain or counter deepfake deception will need to consider two main factors in their operational planning: 1) a swift, near-real-time response to deepfake disinformation videos, and 2) creating more familiarity through additional, preferably live video footage of the target of the deepfake responding to and refuting the disinformation personally.

Keywords—deepfakes, disinformation, misinformation, deception, social media, artificial intelligence, image processing, video manipulation.