Chapter 14
The Rising Threat of Deepfake Technology and Frightening Advancements of Social Engineering

Gausiya Yasmeen
https://orcid.org/0000-0002-7853-1376
Integral University, India

Syed Adnan Afaq
Integral University, India

Tasneem Ahmed
https://orcid.org/0000-0003-2702-3168
Integral University, India

ABSTRACT

Advancements in digital technologies have made it difficult to distinguish between real and fake media, leading to privacy and security threats. Deepfake, a combination of deep learning and fake, is a technique used to replace or mask someone else's face in images or videos. Social engineering (SE) attacks exploit human attributes and psychology to bypass technical security measures for malicious acts. Deepfake videos, created using artificial intelligence (AI), pose a significant threat to society, politics, and businesses. Deepfakes pose a significant threat, they can be combated through legislation, regulation, corporate policies, voluntary action, education, training, and the development of technology for deepfake detection, content authentication, and

DOI: 10.4018/979-8-3693-6665-3.ch014

prevention. Common deepfakes include pornographic videos, political deepfakes, financial crimes, and synthetic audio. The paper explores deepfake technology, its benefits, challenges, and detection techniques.

INTRODUCTION

Fake news poses a significant threat to public discourse, human society, and democracy. It spreads quickly through social media, impacting millions of users. YouTube is the second-most popular source of news, highlighting the need for tools to confirm media authenticity. The ease of obtaining and spreading misinformation makes it difficult to trust, leading to harmful consequences for informed decision-making. Today, we live in a "post-truth" era characterized by digital disinformation and information warfare. Technological advancements have enabled the creation of "deepfakes," hyper-realistic videos using artificial intelligence (AI) applications (Rafique et al., 2023). These videos, which can be humorous, pornographic, or political, can be created without the person's consent. The technology's scope, scale, and sophistication make it possible for anyone with a computer to create indistinguishable fakes. In the future, deepfakes may be used for revenge porn, bullying, political sabotage, terrorist propaganda, blackmail, market manipulation, and fake news. This study explores the concept of deepfakes, their origins, their benefits and threats, current examples, and strategies to combat them. It analyzes news articles on news media websites, contributing to the literature on fake news and deepfakes. The research also identifies options for politicians, journalists, and entrepreneurs to combat deepfakes, highlighting the need for further research and understanding.

Deepfake, a blend of deep learning with fake content, involves swapping a person's face to a targeted person in a video or image, resulting in the person acting like the targeted person. This technique has become a public issue, affecting individuals and spreading fake news, fraud, and hoaxes. Researchers are now focused on understanding the insights of Deepfake, which can be used for pornography, political, or bullying without consent (Naitali et al., 2023). Deepfake algorithms use generative adversarial networks to copy movements and facial expressions of individuals, posing threats to political figures, public figures, and celebrities. This technology can also be used to mislead military personnel and cause serious damage. Despite its potential, deep understanding of Deepfakes is crucial for recovery and preventing false news spread. Despite its newness, there is limited resources on this topic. This paper discusses Deepfake technology, its uses, threats, challenges, generation and detection, positive and negative aspects, limitations, suggestions, and future thoughts. Deepfakes are fake motion pictures and images that are produced by using sophisticated artificial intelligence tools to manipulate the original content.