Chapter 6
Identification of Deepfake Images and Synthetic Media for Forgery Detection

Anand Kumar
Amity Institute of Forensic Sciences, Amity University, Noida, India

Rakshita Gautam
https://orcid.org/0009-0006-2651-7907
Amity Institute of Forensic Sciences, Amity University, Noida, India

Shipra Rohatgi
https://orcid.org/0000-0003-0532-9908
Amity Institute of Forensic Sciences, Amity University, Noida, India

Sachil Kumar
https://orcid.org/0000-0002-2681-3937
Amity Institute of Forensic Sciences, Amity University, Noida, India

ABSTRACT

During past years, the easy accessibility of image editing tools such as Canva, FACEAPP, and CorelDRAW, many deepfake and synthetic images have been generated and circulated across media channels and the internet. Due to the emerging technologies such as Artificial Intelligence (AI) and Image Processing techniques, these tools show a capability of transforming human faces, swapping gender, and modifying other data of the images easily without any professional skills. The deepfake and synthetic images have raised challenges in multimedia and document forensics. Indeed, identifying these images through human eyes is difficult. The application

DOI: 10.4018/979-8-3373-3795-1.ch006

of AI can tackle the problem. Various machine learning and deep learning models, such as GAN, CNN, and RCNN, have demonstrated effective classification accuracy in detecting and localizing image forgeries. The AI model's efficiency is evaluated on diverse datasets like Deepfake TIMIT and Deeper-Forensics-1.0.

1. INTRODUCTION

Advancements in Machine Learning (ML) and Artificial Intelligence (AI) are driving the rapid digitalization of society, ushering in a new era of digital content creation and sharing (Chataut & Upadhyay, 2025; Westerlund, 2019). While the creative and entertainment industries have benefited from the immense potential of AI technologies, their proliferation has also given rise to serious ethical, legal, and security challenges, raising deep concerns about their implications on society, democracy, and the integrity of information (Masood et al., 2023; Mirsky & Lee, 2020; U.S. Department of Homeland Security, 2025). Among the most prominent innovations in this field are deepfakes and synthetic media, which have fundamentally redefined how digital content is generated, manipulated, and perceived (Seow et al., 2022; Malik et al., 2022). Digitally altered images and videos, and audio clips of people are increasingly appearing online, contributing to the rise and spread of synthetic media and a new phenomenon known as deepfakes (Ahmed et al., 2024; Rana et al., 2022).

Synthetic media is a broad term that encompasses various types of content, such as video, text, image, or voice, partially or fully generated using AI (Dehghani & Saberi, 2025). This includes not only deepfakes but also a wide range of other AI-generated content, such as computer-generated imagery, virtual and augmented reality, AI-written music, and synthesized voice or text. Deepfakes or synthetic media represent some of the most impressive advancements in digital content creation, revolutionizing the modalities by which images and videos are conceived, fabricated, and altered (Sandotra & Arora, 2024; Masood et al., 2023). The growing prevalence of digitally manipulated images, audio, and videos featuring real people has given rise to the widespread phenomenon known as deepfakes (Altuncu et al., 2024; Verdoliva, 2020).

The term “deepfake,” a combination of “Deep Learning (DL)” and “fake”, was coined by a Reddit user known as “deepfakes” in 2017 (Westerlund, 2019). Deepfakes are typically created using DL frameworks, especially **Generative Adversarial Networks (GANs)**, where two neural networks compete to produce increasingly realistic synthetic media (Masood et al., 2023; Seow et al., 2022). These technologies can convincingly mimic facial expressions, voice modulations, and even full-body movements, making the resulting media difficult to distinguish