



The Rise of Deepfake Crime in 2026

Artificial intelligence has given criminals a weapon that is even more lethal than any virus – and everyone is at risk. take advantage of being able to be quite another person completely. In 2026, deepfake crime is no longer a threat in the future. It comes as today's front page story.

By **Toqeer Zahra** | University of Agriculture, Faisalabad | Published: August 2026

✉ t.zahra@gmail.com | Position: Software Engineer

Introduction

Not so long ago, it was vital to fake a face on video to require a movie studio and a proficient cinematographer. It was once a film studio and proficient cinematographer to fake a face on video, not so long ago. effects team, and weeks of pains taking work. Today it takes a laptop, a free application, and about 10 minutes. The technology which used to create movie magic has got away! the editing suite and landed right into the hands of fraudsters, extortionists, political and other scams. The use of manipulators, and organised criminal networks, and the impact of that is already being felt.

Deep fake crimes are defined as the use of AI-generated synthetic images, audio and video to deceive. What was once labelled a 'withdrawal' now called a 'withdrawal' as curiosity of tech-forums and science-fictional has turned into actual and increasingly endangerment of persons, institutions and public trust. For a country like Pakistan, a nation Spending more money, while engaging in rapid digital transformation with a young, mobile-first population, that is also spending more money. That's a young, mobile first population that's spending more money, while undergoing rapid digital transformation. The stakes are just higher, as still, they are building their digital literacy.

The technology, which made movie magic in the past, has gone astray from the editing room, It was left to criminals to "suite and landed" in the hands of the criminals.

Technology Overview

A deepfake is at its essence a piece of media, whether a video clip, a voice recording, or something else. Photograph: One that is created or altered with the help of computer technology so that it shows something that did not actually happen. The term is derived from the combination of 'deep learning' and 'learning to learn', among other things. The technology is fueled by an AI technique that is powerful enough and "fake". With the advancement of technology, modern deepfakes are being created. Few advances, especially using generative adversarial networks (GANs) and, more recently, diffusion models, have as much potential for future development as the ability to generate images and movie clips. same underlying architecture behind many image generation tools that have become mainstream in recent years.

Not only has there been technical improvement, but what sets 2026 apart from even two years ago is also more than just that. it is democratisation. Once expensive and expert knowledge was needed to use the tools, this is no longer the case. It was about time that hardware became part of consumer smartphones. Mobile applications make it possible to swap by anyone. Face to face with someone in real-time in a video call. Voice cloning platforms can replicate the voice of a specific individual from a sample as short as three seconds, With chilling precision



capturing their accent, cadence and emotional tone. And AI It is now possible to create altogether synthetic footage of a voice saying or doing something. convincingly, quickly and cheaply, things they never said or did. Video calls are part of a vital way of communicating. Many professionals and trust principles are involved in remote business transactions, and there is a trust mechanism.

Social media profiles provide an abundance of video and audio content on LinkedIn, Facebook, YouTube and TikTok. bad actors can harvest to produce believable synthetic replicas of real people. And the individual caution.

Key Findings & Impact

+340% Rise deepfake fraud related incident reports worldwide from 2023 to 2025	\$2.5B Estimated financial losses from synthetic media crime worldwide in 2025	3 sec The minimum amount of audio samples needed to accurately clone a person's voice is now less.	91% Even the newest deepfake detection software is inadequate against the newest generation of tools.
--	--	--	---

The criminal uses of the deepfake technology have spread into several unique and growing categories. The most financially damaging is CEO fraud — also known as The business email compromise has been upgraded to “business video compromise”. In this During video calls, criminals impersonate senior executives to make authorizing transfers. fraudulent transfers. There are already reports from multiple Pakistani businesses about incidents of this nature, with losses ranging from tens of thousands to tens of millions of rupees. The scam works, because it takes advantage of a false assumption that most organisations have never made. formally questioned: that’s convenience of identity when you see a familiar face.

Beyond the boardroom, The videos used against politicians, journalists, business leaders and others that were created were fabricated. Compromising or criminal scenarios are increasingly being circulated by the individual(s) involved. Using social media and encrypted messaging sites. For Woman In Public Life, this Nowadays, the term has assumed a particularly sinister dimension and intimate images, created synthetically, have been used as a harassment & coercion tool. In Pakistan, cyber lawyers report a rise in numbers of cybercrime cases has dramatically increased. this nature though prosecutions are still rare, due to the technical complexity involved in; [And] attributing content to such traces.

Political manipulation via deepfakes is also a growing worry for Pakistan as it strives to navigate. Political manipulation through deepfakes is also a growing concern in Pakistan as it attempts to navigate. A public sphere that becomes more and more digital. Produce political leaders’ speeches in audio files. the fake inflammatory statements, fake videos of government officials taking bribes, and AI generated. press conferences that never took place have all been documented in the region. The these damage reputations, democratic discourse, institutional trust damages In fact, sometimes it is impossible to tell whether the forgery is true or not even after it is discovered. As the saying goes: A lie is half way. around the world before the truth has got its boots on.

There’s an initial response from Pakistani institutions, although it’s sluggish. The Federal Deepfake fraud is an emerging problem for Investigation Agency’s cybercrime team. Although capacity for investigation and prosecution is also limited, category of complaints is. Last updated in 2016, the Prevention of Electronic Crimes Act (PECA), and There are no special provisions in contains for synthetic media. Experts in the field of law have called for Amendments are at various stages of the legislative process, but the process is slow. technology accelerates.



What's Next?

The immediate horizon offers both threat and hope. On the threat side the next generation of The deepfake tool is expected to give the power to produce a video that can be impersonated completely in real time at the meeting of scale meaning a single operator could simultaneously run dozens of fraudulent video calls impersonating different people. On the defensive side, a number of promising approaches are emerging. Digital watermarking embedding invisible, tamper evident information, into digital content. signatures into authentic media at the point of creation could allow recipients to verify that a video/audio clip is authentic. It is made by several major camera manufacturers and smart phone platforms are beginning to implement this at the hardware level though It will still be years before it is widely adopted.

The practical solution in case of Pakistan's tech industry and its broader business community is to relax. The immediate answer for tech industry and business community of Pakistan is to chill out. Can't wait for policy and technology. Organisations need to establish out of band verification protocols a secondary confirmation step, via a separate trusted channel, before an actuation of any high value instruction that is delivered by video or audio only. All of the above, along with banks, telecoms and fintech platforms, should review their video KYC processes against. deepfake attack scenarios. Synthetic threats was to meet the demands of the present-day. Was changed to reflect the requirements of today, including security awareness training. Such threats to media should be part and parcel of employee on boarding process in all organizations. sector.

Pakistan's digital revolution has brought extraordinary However, the opportunity has called for a quick re-negotiation of the dynamics of trust in a connected world. For centuries, visuals were no longer substitutes for faith and belief turned into a burden. Building the awareness, the habits, and the institutions that allow us It's not a technical problem to navigate a world of synthetic media. It is a human one and it starts off with every person realizing that the face on the screen is no longer. proof of anything at all.

About the Author

Toqeer Zahra is a technology and cyber crime correspondent at PakTech Today having more than eight years in the industry. AI and digital security. 3 years experience reporting on digital security, AI and the convergence of those two fields. technology and society in Pakistan. She has explored some of the most important issues for which Pakistan is responsible. cyber crime cases have been seen as an expert commentator on the national media broadcasting.

Keywords: Deepfake; Synthetic Media; AI-Generated Fraud; Cybercrime Pakistan; Voice Cloning; Digital Trust; PECA

References

- [1] Security. Chesney, R. and Citron, D.K. (2019) Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. The University of California, Press. 1753–1820. DOI: 10.15779/Z38RV0D15J
- [2] The use of deepfakes is not limited to creating manipulated video. Deepfakes are not the only application of face manipulation and fake detection, as explored in Tolosana et al. (2020), Deepfakes and Beyond: A Survey of Face Manipulation and Fake Detection. Information Fusion, 64, pp. 131-148. DOI: 10.1016/j.inffus.2020.06.014
- [3] Deloitte & Touche Ltd.
- [4] Federal Investigation Agency Cybercrime Wing (2025) Annual Digital Crime Statistics Report 2025. Islamabad: Pakistan's government.
- [5] Vaccari, C. & Chadwick, A. (2020) Deepfakes and Disinformation: Exploring the Impact of Synthetic Political The video on Deception, Uncertainty, and Trust in News, Social Media + Society, 6(1) is available now. Deception, Uncertainty, and Trust in News, Social Media + Society, 6(1) is out now. DOI: 10.1177/2056305120903408
- [6] Pakistan Telecommunication Authority (2025) Cybersecurity Threat Intelligence Report Q4 2025. Islamabad: PTA.