REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 4, 2026, 549-555

Deepfake Technology and the Integrity of Digital Evidence in Pakistan: A Critical Analysis of Evidentiary Challenges, Legislative Gaps, and the Right to a Fair Trial

Muhammad Afzal[1], Dr. Tansif Ur Rehman[2]

Abstract

With all the above in today's legal environment, a new challenge is the deepfake technology that is being developed by artificial intelligence or deep learning and is a serious threat to digital evidence integrity. The evaluation of digital proof in the legal trials since its inception in Pakistan has been a matter of concern of authenticity, acceptability and verification of the audio-visual evidence produced by Artificial Intelligence. The existing laws and legislations, for instance, Qanun-e-Shahadat Order 1984 and Prevention of Electronic Crimes Act 2016 provide some guidance on the issues of deepfakes. The author in this article, assess the implications of Deep Fakes on the Pakistani evidence Law, explore the lacunas and recommend legislative and forensic changes to ensure safeguarding of right to a fair trial and integrity of the judicial processes.

Article History
Received 15 June 2026
Revised 25 June 2026
Accepted 14 July 2026
Published 20 July 2026

OPEN ACCESS

Corresponding Author *

Keywords
Deepfakes, Digital evidence, laws, Pakistan, theoretical context

Introduction

AI's fast-paced development has drastically reshaped global digital communication and media creation. A particularly troubling trend is the creation of deep fakes, which are fake audio, video or image produced with AI and a neural network that is realistic. Deepfakes are okay in the entertainment and educational sphere but not with regard to privacy, democracy and judicial integrity. Public profile due to the wide spread of the altered media, identity theft and the creation of criminal evidence. In Pakistan, deepfakes made the legal and proof availing challenging , whereas courts are increasingly relying on electronic evidence such as CCTV footage, mobile records, and social media posts.

The main procedures governing the admissibility and verity of electronic evidence in Pakistan are as follows: the Qanun-e-Shahadat Order (QSO) 1984 and the Prevention of Electronic Crimes Act (PECA) 2016. But these laws were drafted prior to the advent of cutting-edge AI-synthetic media and thus offer inadequate guidance on authentication and forensic validation of deepfakes. Not having specific legal standards to identify tampered digital evidence may affect the right to a fair trial and public confidence in the trial system. The article explores the implications of deepfakes within the current evidence law regime in Pakistan and recommends necessary changes in the law to cope with the new technological and forensic challenges.

Research Justification

[1] Department of Law, Dadabhoy Institute of Higher Education, Pakistan (afzalabbasi715@gmail.com) (+923700930490)
[2], Teaching Associate, Department of Sociology, University of Karachi, Pakistan; and Visiting Faculty, Department of Law, Dadabhoy Institute of Higher Education, Pakistan (tansif@live.com) (https://orcid.org/0000-0002-5454-2150)

The global adoption of deepfake technology has had an impact on the legal and evidential landscape, particularly in areas where electronic evidence is central to the process, such as the EU. The existing legislations and statues in Pakistan, such as QSO 1984 and PECA 2016, are weak enough to address the issues raised by AI-generated synthetic media. This research is justified because digital contents can be manipulated and it may jeopardize the procedural fairness, accuracy of the justice and public trust in the justice. The research analyzes the lacunae of law, highlights the challenges in adducing evidence and proposes amendments to the law and forensic science related to deep fake evidence in Pakistan.

Literature Review

However, the rise of generative AI is making synthetic media a huge problem for digital forensics. More efficient deep learning models are continually being developed to detect manipulated video content to help combat malicious deepfakes (Qadir et al., 2024). But as technology becomes increasingly sophisticated, we are now in an endless arms race of sorts to detect the newest innovations (Babaei et al., 2025). In order to address this issue across different platforms, forensic experts are heavily relying on multimodal identification techniques to identify fakes before they can be sold as genuine media (Qureshi et al., 2024).

But the issue is not simply about the technology, it's also a huge conundrum for legislators. From the research presented this is clear, our regulations are riddled with loopholes and we badly need solid legal definitions of synthetic media that address the unknowns (Birrer & Just, 2024). We also can't simply rely on software to save us as algorithmic detection often does not provide the level of certainty that a strict legal framework requires (Jacobsen, 2024). Worse, these digital dupes pose a genuine threat to personal freedom and so it's time to turn a critical eye towards the current privacy and cybercrime laws to ensure that people's basic rights are properly safeguarded (Laghari et al., 2025).

The final problem is what happens if these fakes get to trial. In Pakistan, where the process of obtaining evidence is particularly laborious, the reliability of the court record is entirely undermined if the evidence is AI generated, and the rights to fair trial are at great risk (Abdullah et al., 2026). Hence, it is decisive to re-imagine the approach toward cybercrime prosecutions to certify that digital proof is properly handled in a fair manner to sanctuary the justice system (Gul et al., 2025). With the "noise" generated by synthetic media, courts will have to start drafting rules from scratch such as changing the burden of proof in the statutory rules, for instance, in QSO (Ullah et al., 2025).

Historical Context

The idea of a deepfake was introduced in the late 2010s with the progress of AI technologies such as deep learning and Generative Adversarial Networks (GANs). Originally created for research and entertainment, the technology quickly progressed to create videos, audio and images that are very believable. In recent years, with a number of incidents involving manipulated digital content in politics, celebrity impersonation and online fraud, this has grown into an issue of concern in the international sphere. The rise of digital media in the communication and legal investigation arena created problems for courts in different jurisdictions concerning the verification and credibility of electric testimony. As the use of electronic evidence is increasing in Pakistan, both Qanun-e-Shahadat Order 1984 and Prevention of Electronic Crimes Act 2016 have posed certain legal and forensic problems with

the use of AI-generated media.

In this context, the law and forensic practices lack in certain areas in Pakistan including the QSO1984 and PECA 2016. The Qanun-e-Shahadat Order does not mention about verification of synthetic media or deepfakes, there is no legislation in Pakistan regarding this. A lack of robust forensic systems, judicial training and consistent judicial procedures for verification are highlighted as significant limitations on the right to a fair trial and the integrity of evidence. There is a risk of violation of the right to fair trial and evidence integrity due to the lack of uniformity of procedures and protocols for verification, the quality of the forensic infrastructure and the training of judges.

Theoretical Context

Both deepfakes and evidence laws are based on concepts of evidence authenticity, reliability and admissibility in legal proceedings. Traditional evidence theory is based on the assumption that the audiovisual recordings are objective representations of facts and events. However, it is this idea that is being challenged by the capabilities of deep fake technology which can create extremely realistic fake content that is nearly indistinguishable from the real thing. As digital content becomes more easily created with AI, it is having a profound impact on digital proof verification systems, diminishing the evidentiary value of online content and public confidence in electronic evidence.

Under the QSO 1984, electronic evidence in Pakistan is only admissible if the court permits it and if the evidence can be proven to be reliable by any forensic procedures in place. Theoretical arguments center around whether the existing concepts of the law are sufficient to address the manipulation of media using synthetic techniques and whether new rules be adopted for evidentiary value of the content generated by use of AI. The significance of digital forensic authentication, expert testimony, and Chain of Custody procedures in order to preserve the integrity of evidence in the age of AI has been emphasized by scholars.

Relevant Laws

1. Qanun-e-Shahadat Order 1984: The modern electronic and scientific evidence can be admitted to court according to Article 164. It does not contain specific rules relating to artificial media created by AI however, which means that judges are left without any specific rules to determine whether digital audio-visual recordings are genuine or manipulated by deepfake technology.

2. Expert Opinion and Digital Forensics: The Electronic Document and Electronic Evidence Regulations of 2019 permit expert evidence from electronic documents; however, Pakistan still does not have any standardized methods for identifying deepfakes. Lack of a shared standard in technique may lead to conflicting expert opinions regarding the crime, which may cause confusion in court proceedings.

3. Electronic Transactions Ordinance 2002: The ETO is a system for electronic documents and signatures, but does not cover generative AI manipulation or synthetic media. It fails to provide a legal way to ensure the integrity of AI-manipulated digital documents.

4. Prevention of Electronic Crimes Act 2016: PECA outlaws cyber crimes such as identity theft, online fraud and electronic defamation. It does not, however, explicitly outline definitions and criminal penalties for creation and dissemination of deepfakes, which means there is a need for legislation changes and greater forensics readiness.

5. The rules of burden of proof and presumption of truth (Articles 117-129): If the party alleging the deep fake bears the burden of proof, then they have to prove something in an unreasonably high standard. Striking a balance between admissibility of electronic evidence and fairness of the procedure is difficult in the absence of a legal presumption of proactive forensic validation of digital media.

Challenges

The legal system in Pakistan is facing new challenges due to the use of deepfake technology, particularly regarding the provenance and trustworthiness of digital testimony. Deepfakes can create videos, images, and audio that are indistinguishable from the real thing with the ability of AI. This is a particular issue given the increasing use of digital evidence by the courts in Pakistan, including CCTV footage, mobile videos and social media posts.

The QSO 1984 recognizes that electronic evidence can be used in limited circumstances, but makes no specific reference to AI generated or manipulated media or offers any detailed procedures for the authentication of deepfakes. Similarly, PECA 2016 deals with various cybercrimes but does not contain specific provisions dealing with deepfake technology. The major problem is there is no proper Digital Forensic Infrastructure in Pakistan and no trained Digital Forensic (DF) experts who can be able to identify the manipulated content. Faulty forensic assessment can affect the fairness of trials and accuracy of judicial decisions.

But deepfakes also offer a chance to make positive changes to the legal and tech systems in Pakistan. Relevant legislation might also be modified to create specific rules and regulations regarding deepfakes and offenses concerning deepfakes, and electronic authentication. Up-to-date forensic laboratories, AI detection tools, and judicial training are other investments that can improve the judicial system's ability to manage synthetic media and maintain the integrity of electronic evidence.

Opportunities

While there are potential dangers of deepfakes, the increasing presence of this technology can offer opportunities for legal, technological and institutional development in the justice system in Pakistan. It is now widely recognized that AI-powered synthetic media has brought a need for improved Digital Forensic skills, and the need to adapt the laws of evidence. This will enable Pakistan to enhance the existing laws of deep fake under QSO 1984 and PECA 2016.

As awareness of the deepfake challenges grows, investment in state-of-the-art forensic labs, deepfake tech detection software, and deepfake tech judicial training may also be on the rise. Digital evidence trust in court can be enhanced with new digital verification methods, such as metadata review, which incorporates AI-powered detection software.

Further, through scholarly research and collaboration with other countries in the field of cybercrime law, Pakistan will be able to develop an elaborate law, geared towards the world's technological progress. These modifications could enhance the transparency of the judicial system, protect rights to a fair trial, and increase public confidence in judicial proceedings and the responsible use of new AI tools. These changes can also help to educate judges, lawyers, and investigators about deepfakes and help them to have a uniform method for dealing with disputed digital evidence. This would enhance the legal reaction to new AI issues in general.

Discussion

In the modern era of technologically driven society, deepfake technology has emerged as a significant issue in the context of the reliability and admissibility of evidence in the Pakistani legal system. The existing law is limited and provides certain guidance on AI generated synthetic media and electronic authentication process like the Qanun-e-Shahadat Order 1984 and the Prevention of Electronic Crimes Act 2016. There is no specific legislation, forensic facilities or judicial experience to decrease the likelihood manipulated evidence will affect the process of court cases. Meanwhile, these barriers also offer opportunities for change in the law, technology and institutions. The mechanisms in Pakistan to validate the forensic verification process and enact laws on deepfakes are very important; to preserve evidence and ensure a fair trial.

Conclusion

This deep faking technology is destined to destroy the integrity, authenticity and reliability of e-evidence in Pakistan's legal system. Although digital evidence and cybercrime are addressed by existing legislation, such as the Qanun-e-Shahadat Order 1984 and the Prevention of Electronic Crimes Act 2016, these laws are not adequate to address the issues presented by synthetic media generated by AI. No specific law, forensic structure and authentication law to protect the right to fair trial and judicial accuracy. Thus, Pakistan needs to take a holistic approach towards legal reforms, enhance forensic skills and update the process of evidence gathering to address the challenges that are posed by the use of deep fakes in the digital era.

Recommendations

The need is to formulate comprehensive laws in Pakistan and control deepfake technology and fake media created using AI. The Qanun-e-Shahadat Order 1984 and the Prevention of Electronic Crimes Act 2016 should be amended in having clear definition of deepfakes, guidelines for admissibility of electronic evidences and procedure for authentication of digital proofs. Lastly, the Government should establish high-tech digital forensic lab and give specific training to the judges, lawyers, prosecutors and police on AI-based evidence and cybercrimes investigation.

In addition, Pakistan needs to implement the modern technologies like AI based deepfake detection software, metadata verification system, secure chain of custody protocols etc. to ascertain the authenticity of evidence. Educational institutions and research institutions should promote the research of the synthetic media and cyber law. International cooperation and policy development can also help Pakistan to adapt its legal framework with the new international standards for digital evidence and artificial intelligence.

Research Limitations

The insights highlights the significance of the challenges of a deep fake in Pakistan and the necessity of legal and institutional reforms to combat it. The outcomes of this research can be used as an input in debates regarding the Artificial Intelligence, Cybercrime and the evidentiary law and it may also contribute to the caveats of Prevention of Electronic Crimes Act 2016 and Qanun-e-Shahadat Order 1984. The result might be applied to designing efficient forensic methods and regulations for the future use by other stakeholders such as the police, justice systems and the government in authentication of digital evidence. Furthermore, it suggests future research directions on the governance of artificial

intelligence, studying digital crimes and safeguarding fair trial rights in the technologically and legally dynamic context in Pakistan.

Research Implications

The findings underscore the pressing need to tackle the emerging challenge of deep fakes in Pakistan and the importance of legal and institutional responses to counter this emerging threat. The study contributes to the existing academic debate on the laws related to artificial intelligence and cybercrime laws by highlighting the omissions in Qanun-e-Shahadat Order 1984 and Prevention of Electronic Crimes Act 2016. The result could be applied to design efficient future forensic methodologies and regulations to be followed by various stakeholders such as the police, the justice systems, and the government in the authentication of digital evidence. Moreover, the research provided guidance for the future work of governing AI, exploring digital crimes and guaranteeing fair trial rights in the technologically and legally evolving environment of Pakistan.

Future Research Directions

Going forward, it is essential to develop specific systems of Deepfake detection, regulation and adjudication in Pakistan and in the courts. There is a need of empirical studies to have an understanding of the interpretation of judges and legal practitioners in the context of Qanun-e-Shahadat (1984) and Prevention of Electronic Crimes Act 2016 in relation to AI-generated media. Future studies on how AI can be used for forensic analysis, blockchain-based verification systems and metadata authentication techniques could help to improve the trustworthiness of evidence. Comparative law studies, such as research on the EU, the US and India can also be helpful to find out what constitutes best practice in the area of regulating synthetic media. Furthermore, the interdisciplinary research and study of legal, computer science, ethics, and other areas are significant in order to build up strong governance mechanisms for AI in the judicial field.

References

Abdullah, H. O., Darwaish, M. I., Chaudhry, M. J., & Ehsan, M. (2026). AI generated evidence in the courtroom: Deepfakes, evidentiary authenticity, and the threat to fair trial rights in Pakistan. *Journal of Global Social Transformation*, 2(5), 224–242. https://doi.org/10.71317/jgst.2.5.2026.499

Babaei, R., Cheng, S., Duan, R., & Zhao, S. (2025). Generative artificial intelligence and the evolving challenge of deepfake detection: A systematic analysis. *Journal of Sensor and Actuator Networks*, 14(1), 17–38. https://doi.org/10.3390/jsan14010017

Birrer, A., & Just, N. (2024). What we know and don't know about deepfakes: An investigation into the state of research and regulatory landscape. *New Media & Society, 27*(12), 6819-6838. https://doi.org/10.1177/14614448241253138

Gul, S., Ahmad, F., & Ahmad, R. (2025). Digital evidence and procedural fairness: Reforming cybercrime prosecution in Pakistan. *Journal for Social Science Archives*, 3(2), 544–554. https://doi.org/10.59075/jssa.v3i2.260

Jacobsen, B. N. (2024). Deepfakes and the promise of algorithmic detectability. *European Journal of Cultural Studies*, 28(2), 419–435. https://doi.org/10.1177/13675494241240028

Laghari, A. R., Basit, A., & Ahmad, W. (2025). Deep fakes and the right to privacy: A legal analysis under Pakistan's data protection and cybercrime frameworks. *Academia International Journal for Social Sciences, 4*(4), 1915–1926. https://doi.org/10.63056/ACAD.004.04.1040

Qadir, A., Mahum, R., El-Meligy, M. A., Ragab, A. E., AlSalman, A., & Awais, M. (2024). An efficient deepfake video detection using robust deep learning. *Heliyon*, *10*(5), e25757. https://doi.org/10.1016/j.heliyon.2024.e25757

Qureshi, S. M., Saeed, A., Almotiri, S. H., Ahmad, F., & Al Ghamdi, M. A. (2024). Deepfake forensics: A survey of digital forensic methods for multimodal deepfake identification on social media. *PeerJ Computer Science*, 10, e2037. https://doi.org/10.7717/peerj-cs.2037

Ullah, M. A., Abbas, A., & Sarwar, M. W. (2025). Reassessing the burden of proof under Pakistan's Qanun-e-Shahadat Order, 1984: A doctrinal analysis. *Global Political Review*, 10(3), 95–103. https://doi.org/10.31703/gpr.2025(X-III).09