QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 01 (2025)

LEGAL IMPLICATIONS OF DEEPFAKE TECHNOLOGIES IN PAKISTAN'S COURTS

***Asad Ali Arain,**
Department of Law, Dadabhoy Institute of Higher Education, Pakistan
(arainasad481@gmail.com)
****Dr. Tansif Ur Rehman,**
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)

Abstract
The development of deep fake technologies has become one of the major legal dilemmas facing the Pakistani courts, especially on matters of authentication of evidence, privacy, and criminal responsibility. Deep fakes, in which audio, video, or image materials are altered to produce incredibly realistic and yet deceptive images, can also be used to defame, commit fraud, manipulate politics, and even create evidence in a court of law. The virtual evidence technology renders it difficult to establish whether the digital evidence is authentic or not in the eyes of the courts and raises the question of due process and fairness of trial. The current Pakistani laws, including the Prevention of Electronic Crimes Act, 2016, provide minimal details on the way to deal with the crime related to deep fakes, which highlights the shortcomings of the law and control instruments. To overcome these issues, new laws, technological skills in courts, and digital evidence verification guidelines will be needed. This paper explores the legal aspects of deep fakes, discusses the sufficiency of the current laws, and presents the options of how technological protections can be incorporated into the judicial system in Pakistan to provide justice and accountability.

Keywords: challenges, historical context, laws, opportunities, theoretical context

Introduction

One more challenge for the justice system in Pakistan comes in the form of the increasing prevalence of technologies used to make deep fakes. Deep fakes refer to artificial media that is generated using AI and modifies videos, photos, and sounds, thus undermining the credibility of evidence presented in a court. Nazir et al. (2025) suggest that the evaluation of digital evidence in Pakistan reveals that the issues of admissibility and verification persist in the country, and the development of deep fakes only increases the problem. Similarly, Zahoor et al. (2022) state that the use of technological evidence in Pakistani courts has been poor in the past, and present-day structures of the local law are not sufficient to address the sophisticated AI-based manipulations. Inability to verify deep fakes properly endangers the procedural equity and soundness of the court judgments.

New developments are being made in the sphere of forensics, and these developments will probably provide a solution; however, they are not effectively implemented in the Pakistani legal system. AI-based deep fake detection and mitigation methods offered by Nasir et al. (2025) may be applied to offer evidentiary validation in Pakistani courts since the methodology can be employed to identify such a fake. Besides this, Qureshi et al. (2024) multimodal solutions to the issue of deep fakes on social media and the significance of technical literacy and expert testimony in the courtroom.

Besides, juridical processing of modern digital evidence in Pakistan is still in its infancy. Saeed et al. (2022) emphasize that courts need to keep up with the new technologies, such as AI-generated media, to make them admissible and authentic. Similarly, Sohail et al. (2025) suggest that deep fake forensics can safeguard privacy and content validation, and it can be

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 01 (2025)

applied as an effective instrument to minimize evidentiary risks. All these studies together demonstrate that there are more than technical aspects to the legal concerns of deep fakes.

Research Justification

The recent breakthrough of deep fake technologies has posed unprecedented challenges to the Pakistani legal system, and it is crucial to investigate them in terms of their effects on courts. Deep fakes are fake audio, video, or image data that can be utilized to create evidence, slander people, or control the opinions of other people, and thus endanger the integrity of trials and the justice of the court proceedings. Even with such risks, the existing Pakistani laws, such as the Prevention of Electronic Crimes Act, 2016, do not mention deep fakes directly and do not allow for specific instructions on how to prove such veracity in the court.

The study is supported by the fact that courts are more than ever likely to be presented with instances where digital evidence might have been compromised, and this necessitates judges, prosecutors, and lawyers to consider the issue of authenticity and reliability. Policymaking, procedural guidelines, and training of judges can be informed by learning about the legal, procedural, and technological concerns of deep fakes. The study will also come in handy in the identification of loopholes in the existing laws and propose solutions to safeguard the rights of citizens and ensure the integrity of the judicial system, in a comprehensive manner.

Literature Review

The emergence of deep fake technologies has created a major problem for the legal system, especially in digital evidence. Nasir et al. (2025) highlight the significance of AI-based detection and forensic systems to curb the threats of deep fake content in criminal cases. On the same note, Qureshi et al. (2024). Provide a detailed overview of multimodal deep fake detectors in social media, suggesting technical resolutions that can help to prove checks in court. These articles reflect the growing relevance of forensic abilities and technical literacy of legal actors in Pakistan because the traditional evidentiary norms may not be sufficient in responding to AI-edited media. Sohail et al. (2025) also explain that deep fake image forensics has the potential to safeguard privacy and improve content accuracy.

Admissibility and fair process are still important in the Pakistani legal system. Nazir et al. (2025) note that there are doctrinal issues surrounding the admissibility of digital evidence, such as chain of custody, reliability, and the judicial knowledge of technical evidence. These issues are supported by Zahoor et al. (2022), who show that courts do not have uniform guidelines to determine the authenticity of electronic evidence. Hameed et al. (2021) further states that the assessment of modern technological evidence in Pakistani courts has gaps in its system, and that it is crucial that changes are introduced to synchronize the rules of procedures with the realities of modern digital technologies.

Other studies focus on the integration between forensic taxonomy and process innovation. Aoun (2023) addresses the challenges that arise in identifying deep fakes and provides a taxonomy aimed at resolving the issue. Conversely, Rana et al. (2022) discuss the probative value of evidence from electronic devices used in the investigation of criminal acts in Pakistan. The issue of procedural justice is addressed by Gul et al. (2025), who emphasize the importance of judges' training and changes in legal procedures. Saeed et al. (2022) state that judges should be adaptive to assess new devices and techniques. All these sources show that solving the problem of deep fakes in Pakistan needs a multi-dimensional approach combining robust forensic methods with legal reform.

Historical Context of Legal Implications of Deepfake Technologies in Pakistan's Courts

The history of legislation on digital evidence and cybercrime in Pakistan offers a crucial context for comprehending issues brought about by deep fake technologies. Traditionally, the

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 01 (2025)

Pakistani justice system was based on traditional rules of evidence, which were not well-suited to deal with electronically generated content. According to Zahoor et al. (2022), the problem that courts faced is determining the authenticity and reliability of digital evidence, which had lapses in the procedures and constrained the successful prosecution of cyber-enabled crimes. In the same vein, Nazir et al. (2025) point out that the frameworks of digital evidence in doctrines were underdeveloped.

The emergence of advanced AI-based manipulations, including deep fakes, became a crucial change in the history of digital evidence law. Nasir et al. (2025) suggest that AI-generated content detection methods were not actively investigated in Pakistan until recently, indicating a reactive approach of the law instead of a proactive one. Saeed et al. (2022) also note that the judicial system has been slow to adapt to new technologies, and courts have been increasingly aware that expert testimony and technical indications are necessary to analyze electronic evidence. From the discussion presented above, it is clear that even though Pakistan has done well in handling cybercrimes, there is still a lot of work to be done concerning cases of deep fakes.

Theoretical Context of Legal Implications of Deepfake Technologies in Pakistan's Courts

Deep fake technologies are based on the latest artificial intelligence, more specifically, Generative Adversarial Networks (GANs), which can produce audio, video, and images that are very realistic. On theoretical grounds, these technologies undermine the traditional legal definitions of evidence credibility. The assumption that visual and auditory material is real has been historically used by courts; deep fakes have subverted this assumption by ensuring that the fake data are indistinguishable.

Principles of reliability, integrity, and verifiability are the basis of the admissibility of evidence in theory. Deep fakes contradict these principles since they have the capability of altering the context, making up false narratives, and masquerading as individuals without their knowledge. This raises the question of the burden of proof, the question of expert testimony and the fact that one must be technologically savvy as a judge or a legal practitioner.

In addition, deep fakes are set on the edge of the theory of ethics and human rights since they can infringe upon privacy, dignity, and freedom of expression. Theories of legal digital evidence and procedural fairness, and the protection of individual rights, should be revised to encompass synthetic media. The concepts are essential in designing effective legal frameworks. They give instructions on the verification of evidence.

Laws Regarding Deepfake Technologies in Pakistan's Courts

1. **Prevention of Electronic Crimes Act (PECA), 2016:** PECA is the main law regulating electronic crimes in Pakistan, which includes unauthorized access, cyber fraud, data manipulation, digital impersonation, as well as the abuse of electronic records. Parts 21 and 22 make it a criminal offense to copy, modify, or use data unauthorized, potentially applicable in situations of manipulated audio, video, or image content, such as deep fakes. PECA is a broad category, but it does not explicitly define or even address deep fakes or synthetic media, making it problematic to assess manipulated digital evidence in legal practice and courts. This loophole demonstrates the need to implement special procedures and rules in determining the factuality of AI-generated content before it can be accepted in court.
2. **Qanun-e-Shahadat Order, 1984:** Regulates the admissibility and consideration of evidence, including digital and electronic records. The standard of authenticity, reliability and integrity of electronic evidence before the court can receive attention. Courts should ensure that there is an appropriate chain of custody and that digital files have not been

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 01 (2025)

modified or manipulated in any form. Deep fakes are a threat to these principles since today AI is capable of producing content that cannot be perceived as anything but genuine recordings, making it more difficult to judge the content in court and leading to a wrongful conviction or acquittal.

3. **Pakistan Penal Code (Defamation and Privacy):** Sections of the penal code refer to defamation, harassment, and privacy, and can be applied in cases of using deep fakes to destroy the reputation or damage personal rights. These laws include broad-based solutions yet do not outline any procedural steps to be followed by experts in their testimony or technology to verify the content that has been manipulated.
4. **Legislative and Institutional Reforms:** A necessity to explicitly define synthetic media and set admissibility standards of AI-generated evidence is urgent. Developing cyber forensics and preparing judges will enhance judicial capabilities to make the right assessment of deep fakes. This will enable them to make the judiciary responsive in Pakistan.

Challenges for Legal Implications of Deepfake Technologies in Pakistan's Courts

Whether in proving the authenticity or creating fake videos, the use of deep fake technologies is a serious problem for Pakistan's judicial system. Deep fakes can create highly convincing audio, video and image files, and a judge, lawyer or investigator may not be able to determine if the media is genuine or manipulated. In most cases, the traditional ways of forensics wouldn't be able to detect the changes that have been brought about by AI, which is a greater danger in providing false evidence in court. The legal issues of deep fakes are another challenge. The use of synthetic media is not defined and/or regulated in existing legislation (e.g., Prevention of Electronic Crimes Act, 2016). Because of this type of ambiguity, prosecution and defence are more difficult and unclear, as it is not clear in the current laws how deep fakes should be classified. Moreover, the lack of direct punishment imposed when developing or sharing deep fakes minimizes the deterrent impact and lets potential abusers of such technologies get away without any explicit legal punishment. This is further complicated by human rights and privacy issues. Defamation of a person, violation of personal privacy, or any other vulnerable group can be carried out with the help of deep fakes. The courts are left to strike a balance between the necessity to present the evidence and the security of the rights of individuals without procedural guidelines and technological standards.

Lastly, the abuse of deep fakes may negatively affect the confidence of people in the court. Courts are not sure of the standards of procedure and rules of evidence because there are no common law precedents on them. These issues must be tackled through legislative changes, capacity building of technology, and judicial education, such that the integrity of the Pakistani courts is not compromised and that the synthetic media can be dealt with effectively.

Opportunities for Legal Implications of Deepfake Technologies in Pakistan's Courts

Despite the impairments of deep fake technologies, they also offer some exclusive opportunities to the judicial system in Pakistan to modernize and improve its operations. The development and integration of advanced digital forensic tools is one of the major opportunities. Through investing in AI-driven detection software, the courts will have an opportunity to be more certain that the digital evidence is authentic and that any manipulated material will be recognized and excluded during the legal process in courts or the judicial system.

Deep fakes can also provide an opportunity to enhance the training and knowledge in the field of law. Specialized courses on the topics of learning synthetic media, digital forensics, and the analysis of evidence using AI can be valuable to judicial officers, lawyers, and

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 01 (2025)

investigators. The other opportunity is the opportunity to revise and improve legislation. The existing loopholes in Pakistani legislation on synthetic media can be filled with the help of specific legal changes, which offer clear definitions of deep fakes, clear guidelines on admissibility, and clear definitions of penalties in case of abuse. Legal clarity can lessen ambiguity in the judicial process.

Moreover, deep fakes have the power of promoting inter- and international collaboration, since the instances of synthetic media tend to border on cybercrime, privacy breach, and transnational concerns. Through collaboration with the technology experts, law enforcement authorities and international partners, Pakistan can bolster its capacity to effectively address digital threats, while simultaneously protecting the rights of fair trial. In Pakistan's context, the judiciary has the opportunity to turn these threats into opportunities leading to legal, technological, and justice and individual rights. Courts need to be proactive and deal with technology to make them resilient and credible in this era of increasing digital threats.

Discussion

The advent of deepfake technology presents a huge challenge and an opportunity for the judiciary in Pakistan. The creation of deep fakes threatens established ideas of the reliability of AV evidence and has implications for authenticity, chain of custody and procedural fairness. The problem for the courts is the danger of taking the falsified information, which might affect the outcome of the trials, violate privacy or ruin reputations. Existing legislation, such as the Prevention of Electronic Crimes Act, 2016, and the Qanun-e-Shahadat Order, 1984, has a broad-based concept of electronic evidence, but there are no specific rules concerning AI-generated media.

At the same time, the emergence of deep fakes opens up the prospect of changing the judicial process, enhancing digital forensics and developing special education courses to bring up experts in the legal sphere. Legislative changes can define synthetic media, as can be the admissibility criteria, as well as penalties against misuse. Overall, this conversation demonstrates that although deep fakes pose a serious risk to the integrity of evidence and legal assurance, legal and institutional measures can be taken to curb the threat of deep fakes. Pakistan's Judicial system will be able to have the people's trust and will also be able to provide justice.

Conclusion

The integrity of evidence, privacy, and procedural fairness are revolutionary issues facing the Pakistani judicial system due to deep fake technologies. The extremely realistic editing of audio, video, and image materials makes the testing of digital evidence difficult, which poses a threat of false conviction, damaged reputation, and undermined confidence in the courts. The existing legislation, including the Prevention of Electronic Crimes Act, 2016, and the Qanun-e-Shahadat Order, 1984, provides a vague definition of electronic evidence, yet it is not specifically addressed in reference to AI-generated media.

Nevertheless, these obstacles present a chance to change as well to enhance the judiciary in dealing with deep fakes, it is possible to integrate high-tech digital forensic tools, provide explicit legal definitions of synthetic media, and train judges, lawyers, and investigators on dealing with them. Also, the strong inter-agency cooperation and international collaboration could aid effective verification mechanisms. Pakistan courts can protect justice, enforce individual rights, and be credible by being proactive in altering the laws, procedures, and institutional practices to suit the rapidly digital and technologically sophisticated environment.

QUALITATIVE RESEARCH JOURNAL FOR SOCIAL STUDIES
ISSN Online: 3006-4686, ISSN Print: 3006-4678
Volume No: 02 Issue No: 01 (2025)

Recommendations

The following are some of the measures that could be taken in order to address the issue of deep fake technology in the context of the Pakistani legal system. Firstly, certain legislative amendments could be carried out in order to provide a definition for artificial media, stipulate rules concerning its admissibility, and highlight the consequences of producing it. Amendment of the Prevention of Electronic Crimes Act, 2016, and other laws will provide the courts with more direct guidelines and effective prevention of abuse. Second, legal and judicial education programs must be implemented to improve the abilities of judges, lawyers, and investigators to receive AI-produced media, digital forensics, and methodologies of evidence verification. Such programs will assist the legal professionals in critically assessing the digital evidence and making informed decisions.

Third, law enforcement and courts must create special cyber forensic units to deal with deep fake detection and validation. The availability of advanced AI-forensic technologies will ensure that there is an effective assessment of the digital evidence. Finally, inter-agency and international collaboration will be useful in increasing evidence exchange, cross-border cybercrime investigations, and access to technical knowledge. The citizens can also be informed about the dangers of synthetic media through public awareness campaigns.

Research Limitations

There are several limitations that could affect the generalizability of the study results. One, the rapid advancement of deep fake technology makes it a moving target, and it's hard to anticipate everything it can do and the potential legal ramifications at a particular point in time. Secondly, there are few empirical statistics available to determine the use of deep fakes in Pakistani courts, as the number of reported cases is low. Third, all the literature identified is largely theoretical/international and may not accurately reflect the local legal, cultural and institutional environment of Pakistan. Additionally, there was little access to forensic evidence about deep fakes or technology expertise to analyze the evidence in the deep fake, and the feasibility of detection techniques was not assessed. These restrictions highlight the need for further empirical research, case studies, and data-driven analysis to develop robust legal and procedural measures to address deep fakes in Pakistan.

Research Implications

The study has a number of implications for the legal system of Pakistan as well as for policy-making. It emphasizes, legally, the need for law to change and clarify the scope of admissibility of AI-generated evidence, and sanctions against the misuse of AI. The research paper highlights the need for capacity building in the judicial and law enforcement institutions, including special cyber forensic units, training of judges, lawyers, and investigators.

Analyzing the international legal frameworks and their suitability in addressing the synthetic media can lead to an understanding of what changes in the laws and procedures can be made in Pakistan. Research and development of technology should include the creation of improved AI detection mechanisms, guidelines for forensic analysis as well as tools to assist courts in a reliable determination of content manipulation. Moreover, a combination of disciplines (law, computer science, ethics) can develop balancing principles for the admissibility of evidence and the protection of it.

Future Research Directions

The recommendation of future studies of deep fake technologies in the Pakistani judicial system should emphasize both legal and technological aspects. An empirical study about the phenomenon and impacts of deep fakes in courts will be very informative in regard to proposing changes in policies and legislation. A comparison of the international legal

framework and its suitability in addressing synthetic media can give an insight into how the laws and procedures can be changed in Pakistan. Research and development of technology should include the creation of improved AI detection mechanisms, guidelines for forensic analysis as well as tools to assist courts in a reliable determination of content manipulation.

Besides, interdisciplinary research into law, computer science and ethics can come up with principles of balancing admissibility of evidence, privacy, and protection of human rights. Judicial simulations and trainings could be tried out and evaluated as to their effectiveness for improving the knowledge of legal professionals about deep fakes. In general, the direction of future studies should be to develop a holistic evidence-based technique of dealing with synthetic media to make sure that the judiciary system, in Pakistan, continues to be responsive, just, and legitimate in the digital age.

References

Aoun, M. (2023). Deep fake detection in social media forensic taxonomy, challenges, and future directions. *LC International Journal of STEM, 4*(1), 16-26. https://doi.org/10.5281/zenodo.7893258

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

Hameed, U., Qaiser, Z., Qaiser, K. (2021). Admissibility of digital evidence: A perspective of the Pakistani justice System. *Pakistan Social Sciences Review, 5*(4), 518-530. http://doi.org/10.35484/pssr.2021(5-IV)40

Nasir, M., Afzal, A., & Iftikhar, A. Zahra, L., (2025). AI-driven detection and mitigation of deepfake technology in cybercrimes: A forensic approach. *International Journal for Electronic Crime Investigation, 9*(1), 1-16. https://doi.org/10.54692/ijeci.2025.0901/240

Nazir, S., Asif, M., & Khan, A. (2025). Digital evidence in Pakistan: A doctrinal Assessment of admissibility and Reliability in Criminal Trials. *Advance Social Science Archive Journal, 4*(1), 1941-1951. https://doi.org/10.55966/assaj.2025.4.1.0107

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 71*(2), 225-233. https://doi.org/10.7717/peerj-cs.2037

Rana, A., Naul, A. H. K., Gujjar, U. A., & Ahmad, F. Z. (2022). Admissibility and evidentiary value of electronic evidence in criminal cases: A case study of Pakistan. *Journal of Law and Social Policy, 4*(1), 27-50. https://doi.org/10.2139/ssrn.4261350

Saeed, A., Abro, L., & Dastagir, G. (2022). Approach of Pakistani courts regarding admissibility of modern devices or Techniques in Evidence. *Pakistan Journal of International Affairs, 5*(3), 430-440. https://doi.org/10.52337/pjia.v5i4.683

Sohail, S., Sajjad, S., Zafar, A., Iqbal, Z., Muhammad, Z., & Kazim, M. (2025). Deepfake image forensics for privacy protection and authenticity using deep learning. *Information, 16*(4), 270-299. https://doi.org/10.3390/info16040270

Zahoor, R., Arif, S., & Bannian, B. (2022). Digital evidence and its admissibility under Pakistani Law. *Journal of Development and Social Science, 3*(4), 51-60. https://doi.org/10.47205/jdss.2022(3-IV)06