REVIEW OF CRIME, PEACE AND SOCIETY
ISSN (O): 3079-6105, ISSN (P): 3079-6091
Vol. 3, No. 8, 2026, 425-440

AI-GENERATED FORGED DOCUMENTS: THE ROLE OF FORENSIC EVIDENCE AND LEGAL CHALLENGES IN PAKISTAN

Fatima Aslam[1], Rehan Issa Afridi[2]

Abstract

The rapid development of Artificial Intelligence (AI), particularly generative AI, has transformed the creation, manipulation and dissemination of digital documents and simultaneously created new challenges for the legal regulation of forged and synthetic documents in Pakistan. This study critically examines the existing legal framework governing AI-generated forged documents, with particular focus on the Pakistan Penal Code 1860, Electronic Transactions Ordinance 2002, Qanun-e-Shahadat Order 1984 and Prevention of Electronic Crimes Act 2016. The study explores how existing laws may apply to AI-assisted forgery while identifying gaps relating to attribution, authenticity, admissibility, reliability and evidentiary weight of AI-generated material. It further examines the role of digital and forensic evidence, including metadata, file structures, timestamps, digital signatures, device information, editing histories, chain of custody and expert testimony, in establishing the origin and integrity of questioned documents. The study finds that although existing legislation can address several forms of unlawful conduct involving forged electronic documents, Pakistan lacks a comprehensive and coordinated framework specifically addressing the distinctive challenges created by generative AI. Particular difficulties arise in identifying the person responsible for AI-generated material, assessing the reliability of AI-detection technologies, preserving digital evidence and ensuring consistent judicial treatment. The study therefore emphasises the need for technology-neutral legal provisions, strengthened digital-forensic infrastructure, clear authentication standards, specialised training for judges, prosecutors and investigators, improved chain-of-custody procedures, greater reliance on corroborative forensic evidence and enhanced international cooperation. It concludes that an effective legal response should balance technological development with the protection of authenticity, evidentiary integrity, privacy, due process and fair-trial rights.

Article History
Received 22 September 2026
Accepted 14 October 2026
Published 20 October 2026
Corresponding Author*
OPEN ACCESS
Keywords
Artificial Intelligence; AI-Generated Forgery; Digital Evidence; Digital Forensics; Electronic Documents.

1.0 Introduction

Artificial Intelligence (AI) has rapidly transformed the creation, processing, reproduction and dissemination of digital information. Generative AI can now produce or manipulate highly realistic text, images, signatures, audio, video and documentary material. Although these technologies have legitimate administrative, educational, commercial and legal applications, they have simultaneously created new opportunities for deception, fraud and digital forgery. The legal significance of this development is particularly important because synthetic material may be sufficiently convincing to challenge ordinary methods of visual or documentary verification. Recent Pakistani scholarship similarly identifies deepfakes and AI-generated material as creating serious questions concerning authenticity, privacy, criminal responsibility and the reliability of evidence before courts (Arain & Ur Rehman, 2025; Laghari et al., 2025).

[1] Lecturer Law, Hajveri Law College, Times University Multan. fatimaaslam757@gmail.com
[2] Lecturer Law, Hajveri Law College, Times University Multan. Rehanissaafridirahi@gmail.com

AI-generated forged documents are particularly concerning where they are used to make false claims, alter contractual arrangements, obtain financial advantages, create false records, impersonate individuals or institutions, or influence judicial proceedings. A synthetic document may reproduce the appearance of an official certificate, invoice, identity document, academic record, contract or signature while concealing the fact that it has been artificially generated or substantially altered. The increasing accessibility of generative technologies also lowers the technical and financial barriers traditionally associated with sophisticated forgery. Consequently, distinguishing genuine material from artificially generated or manipulated material has become an important legal issue involving authenticity, reliability, admissibility and evidentiary weight (Arain & Ur Rehman, 2025).

The issue is especially significant in Pakistan because the country's legal framework already recognises electronic transactions and electronic evidence, but many of the principal legal instruments were developed before the current generation of generative AI. The Pakistan Penal Code 1860, Electronic Transactions Ordinance 2002, Qanun-e-Shahadat Order 1984 and Prevention of Electronic Crimes Act 2016 (PECA) provide different legal mechanisms relevant to forgery, electronic records, evidence and cybercrime. However, the emergence of AI creates questions concerning authorship, attribution, authenticity and the evidentiary treatment of synthetic material. Pakistani research has observed that existing digital-evidence rules face difficulties concerning authentication, preservation, forensic capacity and judicial interpretation (Usman & Ahmad, 2021; Ullah et al., 2025).

Digital forensic evidence is therefore central to the investigation of suspected AI-generated forgery. Forensic examination may consider metadata, file structures, timestamps, digital signatures, device information, editing history, communication records and other digital traces. Such evidence can assist investigators and courts in determining whether a document has been altered, where it originated and whether the material is consistent with the circumstances alleged by a party. Nevertheless, the rapid development of AI means that forensic detection should not be treated as infallible. The reliability of forensic tools, preservation of evidence, chain of custody, expert competence and judicial scrutiny remain essential to ensuring that technological evidence does not itself become a source of injustice (Usman, 2022; Neik Ch et al., 2025).

2.0 Research Objectives

1. To examine the existing legal framework for AI-generated forged documents in Pakistan.
2. To identify the main challenges in detecting and dealing with AI-generated forged documents in Pakistan.
3. To suggest legal and practical recommendations for addressing AI-generated forged documents in Pakistan.

3.0 Research Questions

1. What is the existing legal framework for AI-generated forged documents in Pakistan?
2. What are the main challenges in dealing with AI-generated forged documents in Pakistan?

3. What legal and practical measures can be recommended to address AI-generated forged documents in Pakistan?

4.0 Emergence of AI-Generated Forged Documents and the Evolving Nature of Digital Fraud

AI-generated forged documents represent a new stage in the development of digital fraud because artificial intelligence can reproduce the appearance and structure of documentary material with comparatively little technical expertise. A forged certificate, invoice, identity document, academic record, contract or signature may be generated or altered rapidly and repeatedly. The accessibility of such technologies reduces some of the barriers that previously made sophisticated forgery more difficult. The resulting legal problem is therefore not merely whether a document appears genuine, but whether its origin, production process and integrity can be independently established (Laghari et al., 2025).

The production of AI-generated material can be automated, modified repeatedly and combined with other cyber-enabled techniques. A forged document may be used together with impersonation, phishing, identity theft, social engineering or fraudulent online communications. This means that an apparently isolated document may form one part of a broader scheme involving several digital actions. The investigation must consequently examine the circumstances in which the document was generated, transmitted, possessed and used rather than focusing only on the appearance of the document itself (Hadi & Butt, 2025).

The consequences extend beyond individual fraud because widespread uncertainty about digital authenticity can weaken confidence in electronic records used by courts, government departments, banks, businesses and educational institutions. There is also a reverse risk: genuine material may be rejected simply because an opposing party alleges that it was AI-generated. This creates a dual evidentiary danger in which fabricated material may be accepted while genuine material may be unfairly discredited. A reliable legal response therefore requires standards capable of distinguishing technological suspicion from demonstrated manipulation (Ahmad et al., 2024).

AI-generated documents may also be used to obtain financial benefits, fabricate professional or educational credentials, establish false identities, support fraudulent claims and manipulate institutional records. Their misuse can therefore affect both private transactions and public administration. Because AI systems can generate large volumes of content quickly, traditional investigative approaches that depend heavily on manual inspection may become increasingly inadequate. The legal system must consequently develop approaches that combine documentary examination with digital investigation and technological verification (Raza et al., 2025).

Digital forensic investigation must evolve alongside AI-enabled fraud. Investigators may need to examine metadata, file structures, timestamps, device information, editing histories, communication records, source information and other digital traces. These methods can assist in reconstructing the history of a questioned document and identifying inconsistencies. At the

same time, forensic conclusions must be approached carefully because technical indicators may be incomplete or manipulated. The reliability of forensic methodology, evidence preservation and expert competence remains central to a fair determination of authenticity (Qureshi et al., 2024).

5.0 Legal Framework Governing AI-Generated Forgery and Digital Documents in Pakistan

Pakistan does not have a single comprehensive statute specifically dedicated to AI-generated document forgery. Instead, the relevant legal response is distributed among traditional criminal law, electronic-transactions legislation, evidence law and cybercrime legislation. The Pakistan Penal Code 1860 can address conduct involving false documents and forgery, while the Electronic Transactions Ordinance 2002 recognises electronic records and signatures. The Qanun-e-Shahadat Order 1984 provides the principal evidentiary framework, and PECA 2016 addresses several forms of electronic criminal conduct. The fragmented nature of this framework makes coordinated interpretation particularly important as AI-generated material becomes more common (Ashraf, 2025).

5.1 Pakistan Penal Code 1860

The Pakistan Penal Code 1860 remains relevant where AI is used to create, alter, possess or use a false document. The decisive legal questions ordinarily concern whether the statutory requirements of forgery, making a false document or fraudulent use are satisfied and whether the necessary intention can be established. AI does not by itself remove criminal responsibility; rather, it changes the method through which the false material may be produced. The difficult issue is attribution because an automated system may perform the immediate generation while a human actor may have initiated, directed or used the process for an unlawful purpose (Bilal & Khan, 2022).

5.2 Electronic Transactions Ordinance 2002

The Electronic Transactions Ordinance 2002 provides legal recognition to electronic records, communications and signatures and is therefore important where a questioned document exists entirely in digital form. Recognition of an electronic record, however, is distinct from proof of authenticity. In an AI-forgery case, investigators and courts may need to determine the source of the record, its integrity, the identity of the person responsible for its creation or alteration and whether its digital history is consistent with the account presented in court. The legal significance of electronic form therefore depends upon reliable proof of provenance and integrity (Idrees et al., 2025).

5.3 Qanun-e-Shahadat Order 1984

The Qanun-e-Shahadat Order 1984 provides the central evidentiary framework for civil and criminal proceedings in Pakistan. Article 164 is particularly relevant because it permits courts

to receive evidence made available through modern devices and techniques. In AI-generated document cases, however, admissibility does not necessarily resolve questions of reliability or evidentiary weight. The court must still consider whether the material is authentic, how it was obtained, whether it has been preserved properly and whether the circumstances surrounding its production make it sufficiently trustworthy (Siddiqui et al., 2025).

5.4 Prevention of Electronic Crimes Act 2016 and AI-Assisted Digital Fraud

PECA 2016 may become relevant where an AI-generated document forms part of electronic fraud, impersonation, unlawful manipulation or another offence falling within the Act. Its importance lies in addressing harmful electronic conduct even though it was enacted before the widespread adoption of modern generative AI. This creates a technology-neutrality problem: the technology may be new while the underlying conduct resembles an existing offence. Effective enforcement therefore requires investigators and prosecutors to identify the statutory elements of the offence and establish how the AI-generated material was connected with the accused (Saleem et al., 2022).

5.5 Constitutional Safeguards, Privacy and Fair Trial

Constitutional safeguards must remain relevant throughout investigation and prosecution of AI-generated forgery. Articles 4, 9, 10-A and 14, among others, protect lawful treatment, security, fair trial and dignity, while digital investigations may involve extensive examination of personal devices and private information. The use of automated detection systems also creates a risk if technological conclusions are treated as unquestionable. A fair process therefore requires proportional investigation, protection of privacy and a meaningful opportunity for the accused to challenge the reliability and methodology of digital evidence (Abbasi et al., 2021).

6.0 The Role of Digital and Forensic Evidence in Detecting AI-Generated Forgery

Digital and forensic evidence is increasingly important in establishing the origin, authenticity and integrity of electronic documents. AI-generated forgery may leave few obvious visual indications, making technical examination especially valuable. Investigators may analyse metadata, file characteristics, device information, digital signatures, editing histories and related digital records. Such evidence can help reconstruct the circumstances surrounding a questioned document and can provide a more reliable basis for judicial assessment than appearance alone (Khan & Bhatti, 2023).

6.1 Digital Forensic Examination of Electronic Documents

Digital forensic examination involves the systematic acquisition, preservation, analysis and interpretation of information from digital devices and files. In document cases, examination may include file properties, metadata, creation and modification dates, embedded information,

document structure and different versions of a file. Comparison with an authentic document can reveal inconsistencies that justify further investigation. The forensic process should nevertheless distinguish between an electronic document and a fraudulent document, because digital existence alone does not establish falsity (Salam et al., 2022).

6.2 Metadata and Digital Traces as Forensic Evidence

Metadata can provide information about the creation, modification, storage and transmission of a digital file. Software information, timestamps, device identifiers and editing history may assist investigators in reconstructing the sequence of events surrounding a document. Nevertheless, metadata is not automatically conclusive because it may be altered, removed or affected by ordinary software operations. It should therefore be examined together with other digital traces, documentary evidence and surrounding circumstances before a conclusion about authenticity is reached (Malik et al., 2024).

6.3 AI-Detection Tools and Forensic Authentication

AI-detection tools can assist forensic experts in identifying synthetic or manipulated content, but their results should not automatically be treated as conclusive proof. Detection systems may produce false positives or false negatives, particularly when generative technologies change rapidly. Courts should therefore consider the scientific basis of the tool, its known limitations, the data used for analysis and whether its conclusion can be independently verified. Explainability is also important because judicial decision-makers must be able to understand why a technological system produced a particular result (Khalid et al., 2024).

6.4 Chain of Custody and Preservation of Digital Evidence

The evidentiary value of digital material depends substantially upon proper preservation and handling. Investigators should document how evidence was collected, transferred, stored and examined and should preserve original devices and files where practicable. Forensic copies should be created through appropriate procedures and every significant handling stage should be recorded. Weak chain-of-custody practices may permit challenges concerning alteration, contamination or substitution of evidence and may consequently reduce the reliability of an otherwise relevant digital record (Ullah et al., 2025).

6.5 Expert Testimony and Judicial Assessment of Forensic Findings

Expert testimony may be required when the authenticity of a digital document depends upon specialist technological knowledge. An expert can explain the examination methodology, the technical indicators identified and the limitations of the conclusions reached. The ultimate assessment remains with the court, which should consider the expert's qualifications, methodology, underlying material and consistency with other evidence. Expert evidence is therefore most useful when it assists the court without replacing judicial evaluation of the facts (Usman, 2022).

7.0 Challenges in the Authentication and Admissibility of AI-Generated Evidence

The growing availability of AI-generated material creates significant challenges for authentication and admissibility. A digital document may appear genuine while containing fabricated information, and courts must determine whether the material is relevant, authentic, reliable and sufficiently connected to the dispute. Pakistani evidence law has developed mechanisms for electronic material, but the rapid evolution of generative AI creates factual situations that may not have been contemplated when existing rules were developed (Ahmed, 2025).

7.1 Difficulty in Establishing Authenticity and Origin

Authenticity is particularly difficult where a synthetic document appears to have been created by a person, company or public institution. Possession of a file does not necessarily prove that the possessor created it, and a person may have received or downloaded material without knowing that it was fabricated. Investigators may therefore need to establish source, device history, communications, accounts, timestamps and circumstances of acquisition. Establishing origin becomes a central component of proving both falsity and responsibility (Muhammad, 2025).

7.2 Reliability and Accuracy of AI-Detection Technologies

Detection technologies introduce their own evidentiary risks. A detector may incorrectly classify genuine content as artificial or may fail to recognise sophisticated manipulation. The rapid development of generative models means that a method that performs well against one generation of systems may become less reliable against another. Courts should consequently treat automated results as technical indicators requiring contextual evaluation rather than as independent substitutes for comprehensive forensic proof (Shah et al., 2025).

7.3 Integrity, Preservation and Chain of Custody

Digital evidence can be altered without producing the obvious physical signs associated with traditional documentary manipulation. Files can be copied, metadata can be changed and several versions of the same material can exist simultaneously. Investigators should therefore preserve original evidence where possible, generate forensic copies under controlled procedures and document each stage of examination. Proper preservation strengthens the credibility of digital evidence and enables the court to assess whether the material presented is substantially the same as the material originally obtained (Gul et al., 2025).

7.4 Legal Uncertainty Regarding Admissibility

A further difficulty is the absence of detailed statutory criteria specifically designed for AI-generated documentary evidence. Existing rules may provide a legal route for admitting

electronic material, but they do not necessarily answer every question about AI-generated provenance, automated detection, synthetic signatures or the evidentiary weight of machine-generated content. This uncertainty may lead to inconsistent judicial approaches. Clearer standards would improve predictability while preserving the court's authority to evaluate evidence according to the circumstances of each case (Hameed et al., 2021).

7.5 Risk of Misleading Evidence and Violation of Fair Trial Rights

Highly convincing fabricated material can undermine a fair trial by creating a false appearance that an innocent person created or communicated a particular document. The opposite problem is equally serious: genuine evidence may be rejected merely because a party raises an unsupported allegation that it was generated by AI. Both risks require judicial caution because technological uncertainty should not be converted into either automatic acceptance or automatic rejection. The evidentiary process should instead permit meaningful challenge, corroboration and reasoned judicial assessment (Rana et al., 2022).

8.0 Gaps in Pakistan's Legal System and Challenges in Prosecution of AI-Generated Document Forgery

AI-generated document forgery exposes several weaknesses in Pakistan's existing criminal justice framework. Traditional offences may cover much of the underlying unlawful conduct, but successful prosecution requires investigators to identify the perpetrator, preserve relevant evidence, establish that the document is false and prove the required mental element. These requirements become more difficult where the material was created through automated systems, stored on foreign platforms or transmitted through multiple accounts and devices (Adil, 2024).

8.1 Absence of Specific Legal Provisions Addressing AI-Generated Forgery

A significant legislative gap is the absence of a comprehensive provision expressly dealing with AI-generated or AI-assisted document forgery. Existing criminal and cybercrime laws can potentially apply when their elements are fulfilled, but they do not expressly explain issues such as synthetic signatures, automated document generation or AI-assisted attribution. Pakistan could adopt a technology-neutral legislative approach under which unlawful conduct remains punishable regardless of whether the false document was produced manually, digitally or through AI, while aggravated circumstances could be recognised where appropriate (Zakir et al., 2024).

8.2 Investigative and Forensic Limitations

Effective prosecution also depends on the institutional capacity of law-enforcement and forensic agencies. Shortages of specialised personnel, advanced tools, standardised procedures and technical training can weaken the investigation of sophisticated digital manipulation. The problem becomes more complex when evidence is held by foreign cloud

providers or platforms outside Pakistan. Strengthening digital-forensic infrastructure and integrating forensic expertise into criminal investigations are therefore necessary to ensure that technological evidence can be collected and interpreted effectively (Neik Ch et al., 2025).

8.3 Evidentiary and Prosecutorial Challenges

Prosecutors must establish more than the falsity of a document where the applicable offence requires proof that the accused created, possessed, transmitted or used it with the necessary criminal intention. A strong case may require a combination of device examination, metadata, communications, account records, file histories, expert testimony and other corroborative evidence. Defence counsel may challenge the reliability of detection systems, expert qualifications, preservation procedures and the connection between the accused and the questioned material. Consistent prosecutorial and judicial training is therefore essential to improve both conviction quality and protection of fair-trial rights (Basit et al., 2026).

Conclusion and Recommendations

The emergence of AI-generated forged documents represents an important development in digital fraud and presents substantial challenges for Pakistan's legal and criminal justice system. Generative AI has weakened traditional assumptions that appearance is a reliable indicator of authenticity. Although Pakistan already has laws dealing with forgery, fraud, electronic transactions, cybercrime and evidence, these laws were not designed around the full range of contemporary generative-AI techniques. The central task is therefore to adapt existing legal principles without creating uncertainty or unnecessarily restricting legitimate technological use.

Digital and forensic evidence should remain at the centre of the response to AI-generated forgery. Metadata, file analysis, device examination, source verification, digital signatures and other technical methods can assist in establishing authenticity and integrity. At the same time, no automated detection result should automatically be treated as conclusive. Reliable preservation, chain of custody, expert interpretation, corroborating evidence and careful judicial reasoning are necessary to prevent technological tools from becoming a source of evidentiary injustice.

The principal legal problem is not simply the absence of an offence labelled AI forgery. The deeper problem is the absence of a sufficiently detailed and coordinated framework for attribution, forensic examination, authentication and assessment of AI-assisted material. Pakistan should therefore adopt a technology-neutral approach that focuses on unlawful conduct while recognising the special evidentiary characteristics of synthetic documents. Such an approach would be more sustainable than legislation tied to a particular AI technology that may quickly become obsolete.

1. Introduction of Specific Legal Provisions for AI-Generated Forgery

Pakistan should clarify through legislation how existing forgery, fraud and cybercrime offences apply to AI-assisted and AI-generated documents. Any reform should recognise that the use of AI does not remove criminal responsibility where the statutory elements of an offence are established. Where necessary, aggravated forms of AI-enabled fraud should be identified while legitimate AI use remains outside criminal liability.

2. Enhancement of Digital Forensic Infrastructure

Pakistan should strengthen digital-forensic laboratories and investigative institutions through modern equipment, secure evidence-storage facilities and appropriate analytical systems. Training should cover document forensics, metadata analysis, digital authentication, device examination and synthetic-content detection. Stronger infrastructure would reduce reliance on ad hoc investigation and improve the quality of evidence placed before courts.

3. Development of Standards for Authentication of AI Evidence

Clear legal and technical standards should be developed for authenticating AI-generated or AI-manipulated evidence. Courts should consider provenance, integrity, acquisition method, chain of custody, forensic methodology, reliability of detection systems and expert qualifications. Standardised procedures would promote consistency among investigators, prosecutors and courts.

4. Training of Judges, Prosecutors and Investigators

Specialised continuing education should be provided to judges, prosecutors, police officers and forensic personnel concerning AI-generated content and digital evidence. Judicial officers should understand both the capabilities and limitations of generation and detection systems. Investigators and prosecutors should receive practical training in lawful acquisition, preservation, analysis and presentation of digital evidence.

5. Strengthening Chain-of-Custody Procedures

Pakistan should adopt uniform procedures for seizure, preservation, transfer, examination and storage of digital evidence. Original devices and files should be preserved wherever practicable, forensic copies should be created for examination and every transfer or analytical stage should be documented. These procedures would strengthen evidentiary integrity and reduce challenges based on alleged alteration or contamination.

6. Greater Reliance on Corroborative Forensic Evidence

AI-detection results should ordinarily be assessed together with other evidence rather than in isolation. Courts and investigators should consider metadata, device logs, digital signatures, communications, file histories, account records and expert testimony where available. A multi-layered approach can reduce false positives and provide a stronger factual basis for determining authenticity.

7. Strengthening International Cooperation

AI-generated documents may be created, stored and transmitted through foreign platforms and cloud services. Pakistan should strengthen mechanisms for obtaining electronic evidence from foreign service providers and cooperating with other jurisdictions in cross-border investigations. International cooperation can assist in identifying perpetrators, tracing digital activity and preserving evidence located outside Pakistan.

8. Safeguarding Constitutional and Fair-Trial Rights

Any legal or technical response to AI-generated forgery must remain consistent with dignity, privacy, due process and fair-trial protections. AI-detection systems should not be treated as unchallengeable authorities. Accused persons should have a meaningful opportunity to contest the methodology, reliability and factual basis of forensic evidence.

9. Continuous Review of AI and Digital-Evidence Law

Pakistan should establish a continuing review mechanism involving legislators, judges, lawyers, forensic experts, technology professionals, academics and law-enforcement agencies. AI develops faster than ordinary legislative cycles, making periodic review necessary. Continuous evaluation would allow legal rules, forensic standards and judicial guidance to respond to emerging forms of synthetic evidence before technological problems become entrenched.

References

Zakir, M. H., Bashir, S., Zahoor, S., Shahzad, F., & Khan, S. H. (2024). Evolving trademark laws in a global context: A comparative study of China and Pakistan. *Migration Letters, 21*(4), 985–994.

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

Usman, M. (2022). Digital evidence: Testimony of expert witness in Pakistani law. *Majallah-e-Talim o Tahqiq, 4*(1).

Ullah, Z., Ullah, M. K., & Abbas, H. (2025). The impact of digital evidence laws on cybercrime prosecution in Pakistan. *ACADEMIA International Journal for Social Sciences, 4*(4), 5517–5527. https://doi.org/10.63056/ACAD.004.04.1373

Siddiqui, K. M., Ur Rehman, T., & Siddiqui, I. K. (2025). Use of Article 164 Qanun-e-Shahadat Order, 1984 in criminal justice system of Pakistan. *Journal of Applied Linguistics and TESOL*. https://doi.org/10.63878/jalt2346

Shah, G., Ali, Z., & Tahir, M. (2025). Artificial intelligence integration in Pakistan's legal system: Enhancing access to justice, judicial transparency, and legal efficiency. *Federal Law Journal, 4*(1), 87–101.

Saleem, H., Jan, J., & Areej, A. (2022). Cyber crimes trends in Pakistan: Analyzing the legal framework and enforcement challenges. *Society, Law and Policy Review, 1*(1), 10–22. https://doi.org/10.62585/slpr.v1i1.21

Salam, M. H. u., Arif, S. M. A. W. K., & Rathore, S. A. (2022). An appraisal on digital forensic and computer tools involved in investigation process: The case of Pakistan. *Annals of Human and Social Sciences*. https://doi.org/10.35484/ahss.2022(3-III)21

Raza, M., Farooq, U., Moroojo, M. Y., Ali, J., & Shabbir, T. (2025). AI-driven journalism in Pakistan: Legal constraints and future directions. *ACADEMIA International Journal for Social Sciences, 4*(2), 1929–1944. https://doi.org/10.63056/ACAD.004.02.0297

Rana, A. A., Naul, A. H. K., Gujjar, U. A., & Zulfiqar, F. (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.

Qureshi, S. M., Saeed, A., Almotiri, S. H., & Ahmad, F. (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

Neik Ch, S., Azhar, S., & Niazi, A. (2025). Forensic evidence under domestic law: An efficient substitute to ocular account in Pakistani courts. *ACADEMIA International Journal for Social Sciences, 4*(2). https://doi.org/10.63056/ACAD.004.02.0190

Muhammad, O. (2025). AI-generated deepfakes and the crisis of legal authenticity: Reconstructing evidentiary standards in the digital age. *Sarhad Journal of Legal Studies, 1*(1), 1–15.

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. *Sensors, 24*(2), 433. https://doi.org/10.3390/s24020433

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

Khan, M. S., & Bhatti, S. H. (2023). Digital evidence and Pakistani criminal justice system: A review article. *Journal of Social Sciences Review, 3*(1), 489–498. https://doi.org/10.54183/jssr.v3i1.198

Khalid, Z., Iqbal, F., & Fung, B. C. M. (2024). Towards a unified XAI-based framework for digital forensic investigations. *Forensic Science International: Digital Investigation*.

Jan, J., Saleem, H., & Areej, A. (2022). Cyber crimes trends in Pakistan: Analyzing the legal framework and enforcement challenges. *Society, Law and Policy Review, 1*(1), 10–22. https://doi.org/10.62585/slpr.v1i1.21

Idrees, R. Q., Kiyani, S., & Fatimah, R. (2025). Artificial intelligence and intellectual property laws in Pakistan. *Regional Lens, 4*(2), 8–18. https://doi.org/10.62997/rl.2025.42054

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

Hadi, S., & Butt, T. A. (2025). A critical analysis of copyright laws for regulating the legal framework for artificial intelligence. *Qlantic Journal of Social Sciences and Humanities, 6*(1), 359–370. https://doi.org/10.55737/qjssh.vi-i.25334

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

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing reality from AI: Approaches for detecting synthetic content. *Computers, 14*(1), 1.

Bilal, H., & Khan, M. A. (2022). Cyber crime legislation in Pakistan: A critical analysis from Islamic law perspective. *Al-Idah, 40*(2). https://doi.org/10.37556/al-idah.040.02.0802

Basit, A., Dharalah, A. A., Kausar, Z., & Ansari, A. A. (2026). A comparative study of admissibility and authenticity of electronic evidence in context Pakistan and the United Kingdom. *Policy Journal of Social Science Review, 4*(3), 141–150.

Ashraf, M. (2025). Legal framework of artificial intelligence in Pakistan and its regularisation: A comparative analysis and its development with cognitive suggestions. *Advance Social Science Archive Journal, 4*(1), 4562–4595. https://doi.org/10.5281/zenodo.17494761

Abbasi, H., Rafique, S., & Badshah, S. N. (2021). Critical analysis of Pakistani law of electronic evidence from the perspective of Sharīʿah and English law—Recommendations for Pakistan. *Tahdhib-al-Afkar, 8*(1).

Arain, A. A., & Ur Rehman, T. (2025). Legal implications of deepfake technologies in Pakistan's courts. *Qualitative Research Journal for Social Studies, 2*(1), 14–20. https://doi.org/10.63878/qrjs1131

Adil, K. (2024). Digital forensics and criminal investigations in Pakistan. *Research Society of International Law Pakistan*.

Ahmed, R. N., & Fatima, S. (2025). Establishing AI regulations and a legislative framework for Pakistan. *Review of Education Administration and Law, 8*(3), 431–445. https://doi.org/10.47067/real.v8i3.443

Ahmed, I. (2025). Digital evidence in Pakistan: Legal framework, forensic challenges, and judicial reliability. *Contemporary Journal of Social Science Review, 3*(1), 12–20. https://doi.org/10.63878/cjssr.v3i1.1579

Ahmad, F. A. (2025). Jurisprudential status of digital evidence in Pakistan while courts' interpretation of Article 164, Qanun-e-Shahadat Order, 1984. *Pakistan Journal of Law, Analysis and Wisdom, 4*(10), 15–30.

Ahmad, J. B., Hussain, M. A., & Mir, H. A. (2024). Developing a legal framework for digital policy: A roadmap for AI regulations in Pakistan. *Law and Policy Review, 3*(1), 162–188. https://doi.org/10.32350/lpr.31.08

Zakir, M. H., Bashir, S., Zahoor, S., Shahzad, F., & Khan, S. H. (2024). Evolving trademark laws in a global context: A comparative study of China and Pakistan. *Migration Letters, 21*(4), 985–994.

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

Usman, M. (2022). Digital evidence: Testimony of expert witness in Pakistani law. *Majallah-e-Talim o Tahqiq, 4*(1).

Ullah, Z., Ullah, M. K., & Abbas, H. (2025). The impact of digital evidence laws on cybercrime prosecution in Pakistan. *ACADEMIA International Journal for Social Sciences, 4*(4), 5517–5527. https://doi.org/10.63056/ACAD.004.04.1373

Siddiqui, K. M., Ur Rehman, T., & Siddiqui, I. K. (2025). Use of Article 164 Qanun-e-Shahadat Order, 1984 in criminal justice system of Pakistan. *Journal of Applied Linguistics and TESOL*.

Shah, G., Ali, Z., & Tahir, M. (2025). Artificial intelligence integration in Pakistan's legal system: Enhancing access to justice, judicial transparency, and legal efficiency. *Federal Law Journal, 4*(1), 87–101.

Saleem, H., Jan, J., & Areej, A. (2022). Cyber crimes trends in Pakistan: Analyzing the legal framework and enforcement challenges. *Society, Law and Policy Review, 1*(1), 10–22. https://doi.org/10.62585/slpr.v1i1.21

Salam, M. H. u., Arif, S. M. A. W. K., & Rathore, S. A. (2022). An appraisal on digital forensic and computer tools involved in investigation process: The case of Pakistan. *Annals of Human and Social Sciences*. https://doi.org/10.35484/ahss.2022(3-III)21

Raza, M., Farooq, U., Moroojo, M. Y., Ali, J., & Shabbir, T. (2025). AI-driven journalism in Pakistan: Legal constraints and future directions. *ACADEMIA International Journal for Social Sciences, 4*(2), 1929–1944. https://doi.org/10.63056/ACAD.004.02.0297

Rana, A. A., Naul, A. H. K., Gujjar, U. A., & Zulfiqar, F. (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.

Qureshi, S. M., Saeed, A., Almotiri, S. H., & Ahmad, F. (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

Neik Ch, S., Azhar, S., & Niazi, A. (2025). Forensic evidence under domestic law: An efficient substitute to ocular account in Pakistani courts. *ACADEMIA International Journal for Social Sciences, 4*(2). https://doi.org/10.63056/ACAD.004.02.0190

Muhammad, O. (2025). AI-generated deepfakes and the crisis of legal authenticity: Reconstructing evidentiary standards in the digital age. *Sarhad Journal of Legal Studies, 1*(1), 1–15.

Malik, A. W., Bhatti, D. S., Park, T.-J., Ishtiaq, H. U., Ryou, J.-C., & Kim, K.-I. (2024). Cloud digital forensics: Beyond tools, techniques, and challenges. *Sensors, 24*(2), 433. https://doi.org/10.3390/s24020433

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

Khan, M. S., & Bhatti, S. H. (2023). Digital evidence and Pakistani criminal justice system: A review article. *Journal of Social Sciences Review, 3*(1), 489–498. https://doi.org/10.54183/jssr.v3i1.198

Khalid, Z., Iqbal, F., & Fung, B. C. M. (2024). Towards a unified XAI-based framework for digital forensic investigations. *Forensic Science International: Digital Investigation*.

Idrees, R. Q., Kiyani, S., & Fatimah, R. (2025). Artificial intelligence and intellectual property laws in Pakistan. *Regional Lens, 4*(2), 8–18. https://doi.org/10.62997/rl.2025.42054

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

Hadi, S., & Butt, T. A. (2025). A critical analysis of copyright laws for regulating the legal framework for artificial intelligence. *Qlantic Journal of Social Sciences and Humanities, 6*(1), 359–370. https://doi.org/10.55737/qjssh.vi-i.25334

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

Ghiurău, D., & Popescu, D. E. (2024). Distinguishing reality from AI: Approaches for detecting synthetic content. *Computers, 14*(1), 1.

Bilal, H., & Khan, M. A. (2022). Cyber crime legislation in Pakistan: A critical analysis from Islamic law perspective. *Al-Idah, 40*(2). https://doi.org/10.37556/al-idah.040.02.0802

Basit, A., Dharalah, A. A., Kausar, Z., & Ansari, A. A. (2026). A comparative study of admissibility and authenticity of electronic evidence in context Pakistan and the United Kingdom. *Policy Journal of Social Science Review, 4*(3), 141–150.

Ashraf, M. (2025). Legal framework of artificial intelligence in Pakistan and its regularisation: A comparative analysis and its development with cognitive suggestions. *Advance Social Science Archive Journal, 4*(1), 4562–4595. https://doi.org/10.5281/zenodo.17494761

Arain, A. A., & Ur Rehman, T. (2025). Legal implications of deepfake technologies in Pakistan's courts. *Qualitative Research Journal for Social Studies, 2*(1), 14–20. https://doi.org/10.63878/qrjs1131

Ahmad, J. B., Hussain, M. A., & Mir, H. A. (2024). Developing a legal framework for digital policy: A roadmap for AI regulations in Pakistan. *Law and Policy Review, 3*(1), 162–188. https://doi.org/10.32350/lpr.31.08

Ahmad, F. A. (2025). Jurisprudential status of digital evidence in Pakistan while courts' interpretation of Article 164, Qanun-e-Shahadat Order, 1984. *Pakistan Journal of Law, Analysis and Wisdom, 4*(10), 15–30.

Adil, K. (2024). Digital forensics and criminal investigations in Pakistan. *Research Society of International Law Pakistan*.

Abbasi, H., Rafique, S., & Badshah, S. N. (2021). Critical analysis of Pakistani law of electronic evidence from the perspective of Sharīʿah and English law—Recommendations for Pakistan. *Tahdhib-al-Afkar, 8*(1).

Primary Pakistani Legal Sources

Constitution of the Islamic Republic of Pakistan, 1973.
Pakistan Penal Code, 1860.
Qanun-e-Shahadat Order, 1984.
Electronic Transactions Ordinance, 2002.
Prevention of Electronic Crimes Act, 2016, as amended.