AL-AASAR Journal
Quarterly *Research Journal*
www.al-aasar.com

Vol. 3, No.1 (2026)
Online ISSN: 3006-693X

Print ISSN:3006-6921

ELECTRONIC EVIDENCE UNDER THE QANUN-E-SHAHADAT ORDER, 1984: IS PAKISTAN'S LEGAL FRAMEWORK READY FOR THE AI ERA?

Rimsha Shahid (Advocate)
Email: rimsham257@gmail.com
Aleesha Zafarullah Jathol (Advocate)
Email: zafarullahaleesha@gmail.com
Mahboob Ahmad (Advocate)
Asad Law Associates 41-Muzang Road Lahore
Email: mahboobkharal254@gmail.com

ABSTRACT

Artificial Intelligence (AI) and generative AI and deep fake technologies have revolutionized the way in which electronic evidence is collected and analysed, generating new challenges for today's justice systems. In this study, the authors will critically analyse the existing legal framework to ascertain its readiness to deal with electronic evidence created or manipulated using AI. The study is doctrinal and qualitative in nature and focuses on the Qanun-e-Shahadat Order, 1984, specifically Article 164, and the Electronic Transactions Ordinance, 2002, as well as the Prevention of Electronic Crimes Act, 2016, some relevant developments in Pakistan's judicial history, and the latest international scholarship on AI-generated evidence. The results illustrate that Pakistan has a good legal framework for recognising electronic evidence, but there are significant gaps in the authentication, reliability, provenance of the content generated by Artificial Intelligence, and the chain of custody and forensic verification of such content. The analysis also finds that Article 164 offers technology flexibility, but lacks adequate standards for evaluating the authenticity of digitally created or manipulated apparently authentic material. Additionally, the study reveals that the traditional chain of custody is not enough when the content could have been created by third parties prior to investigators' acquisition. It thus calls for an AI-sensitive framework of evidence, which steers clear of a single-authentication approach and relies on layers of authentication, forensic investigation, expert evidence, and the effective procedural mechanisms to contest disputed digital evidence. The study finds that Pakistan is not legally ill-equipped to deal with electronic evidence, but the present laws and procedures in Pakistan need specific reforms to ensure that the advancement of technology does not compromise evidentiary reliability and the right to a fair trial.

Keywords: Electronic Evidence; Artificial Intelligence; Deepfakes; Authentication; Qanun-e-Shahadat Order, 1984

1. INTRODUCTION

Digital technology has transformed the type of evidence presented in today's legal trials. Emails, text messages, WhatsApp conversations, call-detail records, CCTV recordings, social-media posts, digital photographs, electronic documents, location information, metadata and forensic data are all becoming more common ways of providing evidence to courts. Electronic evidence is generated and preserved via technological systems and can be reproduced, communicated, altered and manipulated without apparent physical markings of alteration. This shift has afforded new avenues to courts and investigators, but also raised challenges with regard to authenticity, integrity, reliability and chain of custody. In the last few years, there are indications that electronic evidence plays a greater role in civil and criminal proceedings, but authentication, forensic verification and uniformity of standards are ongoing challenges in the legal system (Ahmed, 2025; Idrees et al., 2026).

The Qanun-e-Shahadat Order, 1984 (QSO), is the main source of law for evidence in Pakistan, which was passed before the internet, the smartphone, cloud computing and modern digital communication became widely available. However, the QSO does have a significant avenue for technological change in Article 164 which authorizes the introduction of evidence of a kind or form that has since become available through modern devices or techniques in appropriate

cases. This clause has given Pakistani courts the power to keep up with the advance of technology without the need for a separate statute in relation to each and every new piece of equipment or method of evidence. As a result, judicial interpretation has acknowledged the importance of the role of modern electronic technologies in the evidentiary process. The significance of Article 164 is evident and the fact that the traditional proof elements are not the only types of proof in evidence also poses questions regarding consistency and boundaries of judicial discretion in the presence of new technologies.

The Electronic Transactions Ordinance, 2002 (ETO) has also given electronic evidence its due legal recognition in Pakistan. Section 3 of the ETO states that an electronic document, record, information, communication or transaction may not be excluded from being legally recognised, admissible, or having effect or be denied proof or validity, or be denied to be enforced, just because it is in electronic form. The Ordinance also covers the requirements for original form and integrity, which state that electronic material may meet the original documents requirements if there is reliable assurance that the integrity of the electronic material has been maintained since it was created in its final form. The ETO is therefore a significant move away from a paper based legal world to a world of legal recognition of electronic information. But no requirement on the basis of statutory recognition should preclude the need to consider whether a given electronic record is genuine, complete and reliable in the context of a given situation.

Additional important aspect of Pakistan's electronic-evidence is provided by Prevention of Electronic Crimes Act, 2016 (PECA). The Act covers crimes committed against information systems and electronic communications as well as procedures pertaining to the preservation, collection and investigation of electronic information. It has forensic provisions that acknowledge the significance of a technical examination and expert opinion in handling electronically stored material. Thus, the Pakistan legal regime on electronic evidence is not solely reliant on the QSO, but is based on the interaction among all the three, the QSO, ETO, PECA, and the judicial interpretation. Such a combination would also serve as a bedrock for both the acceptance and the assessment of digital information, and the success of such an approach would rely on the methods used to establish its authenticity, to ensure its integrity and to make the connection between the digital information and the facts in dispute evident.

The criterion of admissibility versus evidentiary reliability is thus a key issue in the present research. The electronic record can be legally admissible to be presented in court but may not be admissible to prove facts. The issue of authentication, chain of custody, forensic examination and expert testimony are all factors that have been discussed by Pakistani scholarship and are important in determining the evidentiary value of digital material. However, weaknesses were noted in the handling of electronic evidence in Pakistan by Abbasi et al. (2021), amongst others, in regard to authentication of electronic evidence and expert evidence with regard to electronic evidence, and in recent research, continued procedural and technical difficulties were noted in the handling of electronic evidence. These observations indicate that the issue is not only about recognition of electronic evidence in Pakistan but also to have mechanisms with clarity in the legal system which would determine the trustworthiness of electronic evidence.

This issue gets considerably worse when AI created and/or AI manipulated content starts to rise in popularity. Modern Generative AI systems are capable of generating highly realistic images, videos, voices, documents and written communications. Deepfake technologies can alter the facial appearance and voice of a person, while generative technologies can produce seemingly real communications or a record of events that have never actually happened. This

is therefore a different kind of evidentiary danger than is the typical case of digital alteration. Manipulation can be done in traditional ways, leaving visible flaws and inconsistencies, or by increasingly sophisticated AI tools that can generate synthetic material specifically crafted to look authentic. International studies of deepfakes evidence have therefore exposed significant concerns in relation to the reliability of digital evidence and the capacity of courts to differentiate between authentic and synthetic or manipulated evidence.

Not all electronic evidence is to be considered unreliable because of the advent of AI. A ruling like that would have been unsound both morally and legally. There is risk of AI manipulation of a digitally stored CCTV recording, email or mobile-phone record, but it can still accurately record an event. The question that should be asked is whether the specific evidence has been properly authenticated and whether the integrity of the evidence can be established. The task is no longer just to be able to read the electronic information but now to also verify it using technology. A court must take into greater account not only the source of a digital file but whether the file's content has been altered, synthetically generated or manipulated before being introduced into the evidentiary process itself. The distinction is now at the core of the current debates on the usage of AI-generated evidence and digital forensics.

In particular, Article 164 of the QSO is significant, because the terms “modern devices or techniques” are not technology specific. It proved useful during times of change like the introduction of audio recordings, video recordings and electronic communications to courts. But the same freedom can be limited when technology can record an event as well as a believable representation of an event that never existed. The legal battle thus has a conceptual component. The previous technological developments only necessitated courts to establish whether they can use new forms of information as evidence, while AI will make courts need to consider whether the technological process itself could have given rise to the apparent evidence. This makes it more important to seek out standards of authentication, forensic considerations, and judicial understanding of synthetic media.

In recent years, Pakistan's judiciary has shown strides toward embracing digital technology through various actions. Pakistani case law has accepted the use of modern technological evidence under Article 164 and the Supreme Court has touched upon the significance of electronic evidence and electronic material's legal recognition by the Electronic Transactions Ordinance. Concurrently, judicial treatment centers on the need to examine the authenticity and evidentiary support of such recordings as opposed to presuming that all electronic productions are prima facie evidence. The developing jurisprudence thus offers a balance between the technology and the caution for evidence.

The problem has grown in importance as the judicial institutions in Pakistan are moving to a more technologically sophisticated world. The National Judicial (Policy Making) Committee has issued National Guidelines for the Use of Artificial Intelligence in Judicial Institutions of Pakistan on April, 2026. The guidelines are human-centred, not relying on AI as a tool to replace human activity in the judicial process, and stress the importance of human oversight, transparency, accountability, privacy and security. While these guidelines largely focus on how AI can be used within judicial institutions and not the admissibility of AI generated evidence, the adoption of these guidelines marks AI as an institutional reality in the justice system in Pakistan. Given this development, it is more important than ever to consider whether the existing evidence rules of the country are adequate to deal with evidence created or tampered with in the same technological environment.

This worry is further exacerbated by the larger transformation of the Pakistani judiciary towards digitization. The National Judicial (Policy Making) Committee has also worked

towards the themes of e-filing, digital transformation and technology as an enabler of judicial administration. These developments can lead to more information being entered into the justice system via electronic means and, thus, the significance of valid processes for authenticating digital content. The more widely that courts use digital evidence, the more severe the downstream effects of the shortcomings of digital evidence authentication and forensic integrity. The need for a more efficient justice, in turn, provides an opportunity for digitalization, but with a duty to protect the reliability of the evidence given its technological ease.

Lately, Pakistani scholarship echoes this conflict. Ahmed (2025) notes that Pakistan's courts have increasingly accepted digital evidence as a part of Article 164 but have been hesitant to accept it when there are doubts about its authenticity, chain of custody and forensic evidence. A comparative study of Basit et al. (2026) also suggests that the QSO does not have a specific part that addresses the authentication and forensic integrity of electronically stored information in a comprehensive manner and that there is need for a more detailed legal framework. It is crucial that these studies provide evidence to reveal that there were existing weaknesses in the electronic-evidence system in Pakistan prior to the development of the more sophisticated generative AI. But AI should not be seen as introducing a completely new evidentiary issue – it exacerbates and accelerates issues that are already present in the treatment of digital evidence.

The chain of custody also evolves in the AI era.Chain of custody also transforms in the AI era. In conventional digital-forest Investigation, investigators can prove that a specific device and/or file has been seized, copied, stored and examined in accordance with a prescribed procedure. While this continuity is important, it does not mean that the content itself has to be authentic prior to investigators' acquisition of it. Finally, if an AI-generated video has been produced prior to the seizure of its storage media, then the establishment of an uninterrupted chain of custody after the seizure can't prove that the video actually occurred. Thus, the courts will have to differentiate between file integrity and content authenticity in relation to AI. Technically, a file may not have been changed since it was acquired, but may have been changed in its content from the original. This is one of the biggest hurdles of AI in the realm of traditional electronic evidence.

As AI is more frequently applied to forensic analysis, there is yet another complication. AI could help investigators spot anomalies in a report, identify altered pictures or audio files, and analyse metadata and process vast amounts of digital information. But AI's applications as a forensic tool don't necessarily mean that its conclusions are reliable. When an AI-based forensic system has identified a recording as manipulated it may be necessary for the court to gain an understanding of the system's methodology, training data, error rates, validation procedures and limitations. The reliability of the AI examining evidence can thus be considered an issue in evidence distinct from the reliability of the evidence being examined. Comparative research on AI and electronic evidence similarly suggests that there are new requirements for AI-related evidentiary processes such as authenticity, traceability, explainability and accountability.

The constitutional aspect of the question is also paramount. Evidentiary reliability has strong ties to the right to a fair trial and due process in criminal proceedings. An accused person could be subject to serious penalties if evidence created by AI or manipulated by AI is introduced without proper authentication, and it's not accurate. However, if there's too much doubt about digital evidence due to the fact that it could be manipulated with artificial intelligence, then true evidence could be unnecessarily disregarded. Instead of assuming digital evidence is reliable (or unreliable), the legal dispute is to set procedures in place that allow for proof of

reliability and a challenge to it. This means there is a balance to be struck between innovation and efficiency of evidence and fundamental fairness of procedures.

The literature, however, creates an important foundation and leaves a question unanswered for the specific research. Pakistani scholarship has explored questions of admissibility and jurisprudential status of electronic evidence, the Electronic Transactions Ordinance and problems of authentication and forensic integrity. Deepfakes and AI-generated evidence have been the subject of growing interest in the international literature. There is, however, comparatively limited integrated analysis of the current institutional framework of QSO in Pakistan, which is adapted to the shift from ordinary digital evidence to AI generated and AI manipulated evidence. But, of course, the question isn't just if electronic evidence is admissible under Article 164, but if the same admissibility conditions that are in place now will continue to be adequate when AI can be capable of creating more believable audiovisual and text content. This is the main reason for the present study.

1.2 Statement of the Problem

Pakistan has provided a legal framework for e-evidence under the Qanun-e-Shahadat Order, 1984 (specifically Article 164), the Electronic Transactions Ordinance, 2002 and the Prevention of Electronic Crimes Act, 2016. These instruments, however, have been designed prior to the era of the common use of generative AI and advanced deepfake techniques. While current law allows for the use of evidence created with modern devices, and acknowledges the legal relevance of electronic evidence, it fails to offer clear guidelines on how to determine evidence that has been synthetically produced or manipulated by AI. This uncertainty not only extends to admissibility, but also extends to the authentication, content integrity, forensic verification, expert evidence and allocation of responsibility for reliability. As the Pakistan criminal justice system is already grappling with these issues within the context of traditional digital evidence, the introduction of AI could exacerbate them.Past studies in Pakistan have shown vulnerabilities in the authentication process, chain of custody and forensic expertise even in the domain of traditional digital evidence, which may increase with the advent of AI. Thus the main issue that this study aims to discuss is whether the current Pakistani evidentiary system, particularly Article 164 of the QSO, has adequate mechanisms to handle AI-generated evidence and AI manipulated evidence or whether there is a need for legislative, procedural and forensic reforms to ensure the integrity of the judicial process in the era of AI.

1.3 Objectives of the Study

a) To critically examine the adequacy of the Qanun-e-Shahadat Order, 1984, particularly Article 164, for the admissibility and authentication of electronic evidence in the context of AI-generated and AI-manipulated content in Pakistan.

b) To identify the legal, procedural and forensic gaps in Pakistan's existing framework for evaluating the authenticity and reliability of AI-related electronic evidence and propose appropriate directions for legal reform.

1.4 Research Questions

a) To what extent does the Qanun-e-Shahadat Order, 1984, particularly Article 164, adequately address the admissibility and authentication of AI-generated and AI-manipulated electronic evidence in Pakistan?

b) What legal, procedural and forensic gaps exist in Pakistan's current framework for establishing the authenticity and reliability of AI-related electronic evidence, and what reforms are required to address them?

1.5 Significance of the Study

It is a valuable study to understand the impact of the rise in electronic evidence in the modern adjudication process and how AI is making it increasingly easier to make up and manipulate digital evidence. Its key contribution is to shift the focus from the relatively settled issue of the admissibility of electronic evidence in Pakistan to the more challenging issue of the sufficiency of current standards of authentication and reliability if electronic evidence can be created or manipulated with the help of artificial intelligence. The study provides a comprehensive overview of the Qanun-e-Shahadat Order, 1984, the Electronic Transactions Ordinance, 2002, PECA, and the recent judicial developments and emerging issues related to AI, all in one analytical framework, which has been missing in the previous studies. It might also help judges, lawyers, prosecutors, investigators, digital-forensic experts and policymakers be able to differentiate between electronic admissibility, file integrity and substantive authenticity. The study is timely as Pakistan's judiciary has recently issued national guidelines related to the use of Artificial Intelligence stressing over human oversight, transparency, accountability, privacy and security. The study will help inform the creation of more effective authentication protocols, enhanced forensic guidelines, and improved expertise and judicial handling of synthetic media and AI-generated evidence. Finally, the study aims to develop a legal framework that doesn't dismiss technological evidence simply because it's technologically complex, but that also doesn't let seemingly convincing digital evidence come to a court's thinking without proper evidence that it's authentic and reliable.

1.6 Limitations and Delimitations of the Study

This study focuses on qualitative doctrinal and comparative analysis of electronic evidence as per Pakistani laws and therefore does not test AI-detection technologies, perform laboratory experiments on deepfakes, or gather primary data from judges, lawyers, investigators or forensic experts. New technologies, judgments, laws and institutional policies may also be developed since the research is conducted, making the field of AI a rapidly evolving one. The study is intentionally limited to electronic evidence that can be found in the context of AI generated or AI manipulated digital evidence, and specifically to the issue of admissibility, authentication, integrity, reliability, chain of custody and forensic verification in the context of the Qanun-e-Shahadat Order, 1984. The study is mainly analytical with emphasis on the QSO and its interaction with the Electronic Transactions Ordinance, 2002 and PECA and some selected foreign approaches, which are employed for the purpose of comparison and reform. While the study does not seek to be exhaustive of all facets of AI regulation, data protection, IP and cybercrime or algorithmic decision-making, where these provisions have a direct impact on the evidentiary status of AI-generated or AI manipulated material, they are discussed.

2. Literature Review

With the growth of digital communications, mobile technology, social media and cybercrime investigations, there has been considerable development in the literature involving electronic evidence in Pakistan. The early focus was on the acceptance of electronic records by the courts because of the question of whether they were admissible; later, there has been greater discussion of reliability and authenticity, chain of custody, and the probative value of the records. This change is significant because the acceptance of electronic evidence does not imply that any electronic record is reliable. In this context, Ahmed (2025) analyzes how Pakistani courts have been accepting digital evidence with the judicial interpretation of Article 164 of the Qanun-e-Shahadat Order, 1984 (QSO) and has found that the courts have begun to accept digital evidence but still make distinctions between its admissibility and evidentiary value. Likewise, Idrees et al. (2026) point out that challenges for authentication, chain of custody and consistency in judicial practice remain. From the literature, it is therefore

concluded that the main challenge now in Pakistan is not the admissibility of digital evidence in court, but rather establishing its authenticity and reliability.

Article 164 of the QSO is important for the courts in that it gives the court the flexibility to accept evidence presented in a modern way or by a modern device or technique. This has helped the Pakistani courts to keep track of the technological advancements without need for creating a new evidentiary provision for each new technology. According to Ahmed (2025), judicial interpretation of Article 164 has played a major role in the development of the concept of digital evidence in civil and criminal trials. The courts have also been able to adapt to technology, as Siddiqui et al. (2025) maintain, in the context of audio, video and other electronically created materials. The flexibility of Article 164 also brings another problem, however, as suggested in the literature, the Article creates a gateway for technologically produced evidence, but not a specific methodology for the evaluation of whether the evidence has been technologically produced or manipulated or altered by AI. This will become even more significant when digital technologies will no longer be used to record information, but to produce synthetic information.

Another important part of the electronic-evidence framework of Pakistan is the Electronic Transactions Ordinance, 2002 (ETO). The ETO provides statutory recognition for electronic documents, records, communications and transactions and does not create a basis for denying that these are legally valid or admissible just because they are in electronic form. The literature has broadly accepted the ETO as an important move towards the modernization of Pakistani law with regards to electronic transactions and electronic records. Legal recognition does not, however, mean proof of authenticity. However, Jan (2025) suggests that statutory recognition of electronic evidence is not enough as courts must also be able to establish the integrity and reliability of an electronic record. This is especially important for evidence that relates to artificial intelligence as a synthetically created electronic record may meet the formal definition of an electronic record but lack any actual information. The ETO thus offers a valuable legal framework, however, it is not enough to solve the evidentiary issues raised by AI-generated content.

The Prevention of Electronic Crimes Act, 2016 (PECA) also enhances the legal structure of Pakistan by providing provisions regarding the investigation, preservation and collection of the electronic information and emphasises the need for forensic examination. Generally, PECA is seen as a prerequisite to the cybercrime and electronic-evidence regime in Pakistan. For example, Ullah et al. (2025) suggest that the increasing significance of electronic evidence in cybercrime prosecutions is due to the growing complexity and sophistication of the crimes themselves, but that problems in technical competence and in evidentiary processes can impact the outcome of a successful prosecution. Idrees et al. (2026) also point to the interplay between the QSO and the PECA and forensic process as a key aspect of the developing regime of electronic-evidence in Pakistan. The findings of these studies suggest that Pakistan has some laws on digital evidence; however, they are interrelated but not a single law dedicated to the authenticity of AI-generated or AI-manipulated evidence.

One of the common issues in the Pakistani literature is the issue of authentication. Digital evidence can be duplicated, transferred and altered without the obvious physical evidence of change that can occur with traditional evidence. Courts therefore must determine the source of the evidence, how it was gathered and whether it was properly recorded and whether the contents of the evidence were altered. Nazir et al. (2025) point out that the current method of digital evidence in Pakistan has some flaws, notably authentication and chain of custody. Similarly, Ahmed (2025) argues that courts have become more demanding for having a sufficient evidentiary basis to allow a substantial probative value for electronic material. The

reason these findings are significant is that they highlight the vulnerability that AI enhances: Investigators might acquire a perfectly preserved electronic file with its contents being artificially generated or manipulated before that file was acquired.

Chain of custody has therefore become more and more of a focus. Traditional forensic science relies on establishing a chain of custody between the original source of evidence, the time of its collection, how the evidence has been stored, transferred, and presented in court. While this is still vital in the digital world, the era of AI has created a difference between what's happening within the file versus the content's authenticity. According to Idrees et al. (2026), the chain of custody and standardized forensic procedures continue to be crucial in Pakistan. In a comparative study of Pakistan and United Kingdom, Basit et al. (2026) also mention the requirement of establishing stricter rules and regulations on authentication and forensic integrity. They conclude that the only way to determine if the content is a real event, is to have an evidentiary chain after it has been collected. This difference is critical in the case of deepfake videos, cloned voices and fake snapshots.

The increasing importance of expert evidence over the years also is evident in the literature about digital forensics. The authors of Usman (2022) believe that digital evidence has technical attributes of which not all can be properly assessed using traditional evidence-based techniques and this would require suitably-trained forensic professionals to evaluate digital evidence effectively. The argument is further boosted in the case of generative AI. It may be possible for a judge to notice that a video shows a certain person but it does not necessarily mean that the face or voice is a synthetic one. The analysis of technical aspects can involve the study of metadata, file structure, compression methods, source data, digital signature, digital provenance records, and more. The problem is not only to generate electronic evidence, but to craft technical knowledge to lead the court to a proper understanding of the origin and integrity of the evidence.

This conversation has been greatly enriched by recent international scholarship, which has focused on the manipulation of AI-generated and AI-manipulated evidence. It is important to distinguish between acknowledged and unacknowledged evidence that is created with AI assistance, according to Grossman and Grimm (2025). Acknowledged AI-generated evidence refers to evidence that either the use of AI was disclosed or it was not disputed, while unacknowledged AI-generated evidence is evidence that is apparently real but upon which there is a dispute. This difference is significant in evidence cases: the two scenarios raise different legal problems. If the AI involvement is recognized, the court might need to assess the trustworthiness and pertinence of the AI process primarily. The issue that arises when the manipulation of AI is denied is whether the evidence is genuine or not. However, Grossman and Grimm (2025) suggest that conventional rules for authentication might need to be adapted with care as generative AI can create synthetic evidence, including text, images, audio and audiovisual content, which can be very hard to tell apart from authentic evidence.

As deepfakes have gotten more sophisticated, there has been more general concern of visual and audiovisual evidence being unreliable. Photographs and video recordings can come from sources of different reliability and images can be altered, deepfaked and digital images might have an uncertain source, notes Hak (2024). He highlights the possible applications of metadata analysis and digital signatures, as well as the possibility of the watermark and digital forensics when original documents are still available. But Hak (2024) also acknowledges that without the original materials it is much more difficult to be authenticated. In the context of the country this discovery has direct implications for Pakistan as screenshots, compressed videos, forwarded social media content and copied videos may end up in courts without the original

source file or complete metadata information. Under these circumstances, the conventional notions of the trustworthiness of visual evidence become problematic in an increasing way.

But the systematic literature on deepfakes adds to growing worries about the justice system's capacity to differentiate between real and fake evidence. The systematic review by Westerlund et al. (2024) revealed an increasing number of potential risks in deepfake research, such as the falsification of evidence, manipulation, and the undermining of legal and law-enforcement systems regarding evidence, evidence sources, and trust in evidence. The review also revealed that technological approaches to detection are often not up to speed with developing and proliferating the technologies of deepfakes. This is of special concern for courts, as it makes the assumption that technological experts can always detect fabricated content question. Perhaps this is because the technology to create generation is advancing faster than the technology that can detect it – if that is the case, then requiring expert verification may not be the whole solution.

Research on humans' ability to recognize deepfakes provides support to the problem. Recent research shows that even ordinary viewers aren't always good at spotting whether the source of an AV stream is a real or fake entity. This has a very important impact on the proceedings of the courts, as judges, lawyers and witnesses could be faced with very convincing electronic documents even before they have been scientifically proven as authentic. Grossman and Grimm (2025) thus stress the potential for unreliability of AI-generated evidence, while the National Center for State Courts (2025) suggests that the court needs to ask a series of questions about the origin, process, chain of custody and potential for manipulation of digital evidence. It is becoming more and more clear in the literature that visual realism is not in itself proof of authenticity.

One of the key advancements is that AI detection solutions aren't a one-size-fits-all solution. Detecting a GenAI system is a rapidly evolving process, and detection systems can give false positives and false negatives. Thus, a court merely seeking the opinion of an AI detector about whether a video is fake will be substituting one technological uncertainty with another. Hak (2024) and Grossman and Grimm (2025) have advocated for a more holistic view, which includes the verification of sources, forensic examination of the evidence, and the analysis of its context and circumstances in which the evidence was generated and collected. The growing body of literature then argues for a multi-layered approach to authentication and not relying on any single technical cue.

There has also been a start in the literature on approaches to digital evidence based on "provenance." Provenance mechanisms do not try to verify authenticity once a dispute has become an issue; instead they aim to establish the history of a digital content from its start. Verifiable provenance, such as through metadata, cryptographic signatures, content credentials and others, can be used to claim the origin of content and that it has not been modified after the fact. But, provenance mechanisms are not foolproof. Metadata may be deleted or altered and not all digital content is created in a system that can generate reliable digital provenance information. So it's important to remember that provenance is not an absolute certificate of authenticity, but rather one of the elements that can be used to support that authentication.

Another theme that has been highlighted in the literature is the process of the creation of AI-generated evidence. Grossman and Grimm (2025) contend that there should be practical solutions to address acknowledged and disputed AI-generated evidence in the courtroom. The National Center for State Courts (2025) also lists questions about the origin, chain of custody, modifications and context of the production of AI evidence that courts should address when considering the evidence. What is important is this literature for Pakistan, and that evidentiary

reform cannot be just limited to statutory definitions. Practical protocols have also been needed for judges, lawyers, prosecutors and forensic experts to detect, question and scrutinize evidence suspected as AI-generated.

The literature also associates AI-generated evidence to the right to fair trial. The introduction of false "evidence" as "evidence" could result in dire consequences for an accused person who is charged on the basis of an untrue fact. On the other hand, if the courts become too wary of digital evidence because of the potential for AI manipulation, then actual evidence could be unnecessarily cumbersome to use. The right legal strategy needs balance, then, to respond to such a situation. The evidentiary system should offer tools to allow parties the ability to question the authenticity of digital evidence and for courts to consider conflicting technical arguments. The relevance of this concern is greater in Pakistan where the reliability and contestability of the evidence is given a greater significance under Article 10-A of the constitution.

It is known from the literature that Pakistan is thus encountering two interrelated, yet distinct, issues. The first is an ongoing issue relating to the authentication, integrity and chain of custody of traditional electronic evidence. The second is a novel AI-specific issue that includes evidence which can be faux or malformed. In the study of the first problem, scholarly work in Pakistan has made immense strides in the field of Article 164, electronic transactions, cybercrime law and digital forensics. There has been more literature to emerge internationally, however, around the second issue – especially in the field of deepfakes, synthetic media and AI-generated evidence. Together, Grossman and Grimm (2025), Hak (2024), and Westerlund et al. (2024) prove that the court must reconsider the notion of authenticity of audiovisual and digital evidence in the era of AI.

The critical issue in Pakistan is thus the convergence of the current electronic-evidence regime with the new emerging issue of AI-produced evidence. Claiming that Pakistan does not have any law regarding electronic evidence is not correct as QSO, ETO and PECA provide an important legal basis. The more defensible research gap is that these laws were not explicitly written to address the context of artificial intelligence producing highly convincing synthetic evidence, and that Pakistan has just started to systematically focus on this issue in scholarship. Some of the existing research has explored Article 164, admissibility, reliability, chain of custody and forensic evidence, and international scholarship is beginning to focus on the deepfakes and AI-generated evidence. The question that remains unanswered is whether existing evidence-based framework of Pakistan can bridge these two aspects into a comprehensive evidence-based authentication and reliability regime in the era of AI? In the present study, Article 164 and other applicable legal mechanisms are critically reviewed in the context of artificial intelligence generated and artificial intelligence manipulated electronic evidence, including issues of authentication, forensic verification, chain of custody and fair-trial issues.

3. METHODOLOGY

3.1 Research Design

The research method followed in this study is doctrinal legal research with qualitative approach to study the sufficiency of the legal provisions of Pakistan on electronic evidence in the era of artificial intelligence. A doctrinal approach is suitable because it is a study of interpreting existing legal provisions, inconsistencies and whether the existing evidentiary rules are adequate for the evidence produced by AI and the evidence created by AI. The study is not based on surveys, interviews or statistical analysis, but rather the legislation, judicial decisions, policy documents, and scholarly literature are studied and evaluated critically.

3.2 Sources of Data

This research is mostly based on primary and secondary legal sources. Primary sources are the Qanun-e-Shahadat Order 1984 (Article 164), Electronic Transactions Ordinance 2002, Prevention of Electronic Crimes Act 2016, relevant constitutional provisions and a number of judicial decisions made in Pakistan regarding electronic evidence. Secondary sources are peer-reviewed research articles, legal scholarship, comparative studies and authoritative reports from 2020-2026. Comparative perspectives are offered through the lens of international literature on deepfakes, AI-generated evidence and digital authentication.

3.3 Analytical Framework

The analysis follows four interrelated dimensions of electronic evidence: admissibility, authentication and reliability and forensic integrity. The admissibility refers to the availability of electronic and AI based evidence is allowed in court before the existing law of Pakistan. Authentication looks for methods to determine if evidence is what it represents itself to be. Reliability is an issue whether or not the evidence can be reasonably relied upon and forensic integrity is an issue about preservation, handling and chain of custody. These dimensions are analysed specifically with regard to AI generated content and AI manipulated content.

3.4 Comparative Legal Analysis

A comparative legal method is used, but not extensively, to explore the reaction of other jurisdictions to AI evidence and deepfakes. International scholarship and legal changes from other jurisdictions—including the United Kingdom and the United States—are selected to reveal new strategies for authentication, provenance, forensic validation and judicial protections. These are not considered to be directly applicable to Pakistan but are brought to light as principles which could be applied to legal reform in Pakistan.

3.5 Data Analysis Procedure

Collective legal and scholarly material is analysed by themes and from a critical legal perspective. Relevant provisions of the evidence law of Pakistan are first identified and interpreted. Second, judicial methods of dealing with electronic evidence are explored to see how courts have dealt with authenticity, reliability and modern technological evidence. Third, there are opportunities identified to address unique challenges arising from the evidence created by AI and manipulated by AI. Finally, the current regulatory framework in Pakistan is examined to see if any further reforms are needed in legislative, procedural or forensic measures to meet these challenges.

3.6 Linking to Research Objectives

The methodology is directly related to the two research objectives. The first objective is covered by examining Article 164 and related evidence requirements and Article 168, which focuses on the admission and authentication of AI-related electronic evidence. The second objective, which is related to legal, procedural and forensic gaps, and potential reform, is analysed through forensic standards, chain of custody, reliability and comparative approaches. This approach allows the analysis to flow logically from the current legal landscape to the areas of weakness and possible solutions.

4. Data Analysis

4.1 Analytical Framework

The analysis is presented directly related to the two research objectives and two research questions of this study. This is a doctrinal legal study, so the “data” are statutory provisions, judicial interpretations and interpretations of law, and the development of law in relevant comparative jurisdictions, rather than numerical data or survey data. Four dimensions—admissibility, authentication, reliability, and forensic integrity—are examined as they are

connected to each other. This is because the legality of electronic evidence does not imply that a specific digital record is authentic or correct. In recent times, Pakistan's scholarship also referred to the continuing weaknesses of the country in relation to digital evidence, which are identified as "authentication," "chain of custody," "forensic verification," and "technical capacity" (Ahmed, 2025; Nazir et al., 2025; Idrees et al., 2026).

4.2 Objective One: Adequacy of Article 164 for AI-Generated and AI-Manipulated Evidence

The first one explores the issue of the admissibility and authentication of electronic evidence in the age of artificial intelligence, specifically the Qanun-e-Shahadat Order, 1984, Article 164. Article 164 empowers courts to permit the use of evidence obtained by the use of modern devices or methods, thus providing the evidentiary system in Pakistan a good amount of technological flexibility. The provision has played a crucial role in the recognition of evidence created using modern communication and recording media in the courts. Judicial analysis of the article in the last few years has made it an important legal basis for admitting digital evidence in Pakistan (Ahmed, 2025; Siddiqui et al., 2025).

But here, the analysis shows that the concept of technological admissibility does not coincide with the concept of technological authentication. Article 164 does not provide specific guidelines on what constitutes non-authentic evidence created with modern technology, such as AI-generated and AI-manipulated evidence. This separation is important where technology can not only record an event, but can also produce a realistic image of an event that never actually happened. An ordinary description of electronic evidence can also be a synthetic voice recording or an AI-generated photo or video that is entirely fake. Thus, the requirements of Article 164 are flexible with regard to the form of evidence but offer rather little guidance with regard to the authenticity of its content.

This is in sync with the recent study conducted in Pakistan. Nazir et al. (2025) point to confusion regarding authentication needs and chain-of-custody procedures, while Ahmed (2025) notes that the courts remain very focused on authentication and forensic verification in evaluating digital evidence. Likewise, Siddiqui et al. (2025) state that the enabling policy principle is outlined in Article 164, but there are practical challenges related to the authenticity of digital evidence, forensic analysis and the judicial comprehension of new digital technologies. The limitation is not, however, in Article 164's technological neutrality but in the lack of detail procedural standards that go with the technological neutrality.

4.2.1 Article 164 and the Problem of AI-Generated Content

The present analysis also shows that, with the language of Article 164, the legislator was primarily concerned with allowing evidence gathered with the new technologies, but not with evidence that would be synthetically generated by an Artificial Intelligence system. This separation establishes a new type of evidence. Typically, in traditional digital evidence, technology is used to record or store information. Generative AI can be an active generator of the information.

For instance, in an authentic CCTV system, an event happens in front of a camera, and it is recorded. An AI system, on the other hand, can create a video in which an individual seems to be doing an action that never actually took place. The evidentiary risks are quite distinct, both are electronic files. The former asks, “did the recording undergo changes?”; the latter asks the former question, “was the event described really happen?” So to treat them both with the same authentication method would be insufficient.

The analysis concludes, therefore, that Article 164 is still a legally relevant, but still technologically incomplete provision. The flexibility must be preserved but specific rules for AI-generated and AI-manipulated content must be provided.

4.3 Authentication: From Digital Origin to Content Authenticity

The most important vulnerability found in the analysis is authentication. Traditional authentication attempts are those that aim to prove that evidence is the evidence that the party claiming to have it is claiming. In digital cases, this can include the source device, account, sender, recipient, file history or other identifying factors. But with AI, the evidentiary issue is different – there can be real content on a device or account that is fake.

If it is a content that has been created or manipulated using artificial intelligence, it does not necessarily mean that it is a genuine human communication if it can be proven that it came from a certain phone. Similarly, it was not enough to prove that a video file had come from a specific camera to prove that the information contained in the video is authentic.

This results in a distinction between source authentication and content authentication in the analysis. Content authentication refers to ensuring that the content of a digital information record reflects what it claims to reflect, while source authentication concerns the origin or provenance of a digital information record. While a significant amount of existing scholarship has been devoted to source authentication, chain of custody and forensic preservation, content authentication is also a critical concern due to the advent of generative AI (Nazir et al., 2025; Jan, 2025).

4.4 Reliability and Probative Value

The analysis further shows that it is not correct to equate "admissibility" with "probative value." The evidentiary value of an electronic record has been preserved, but it will be subject to the same rules of production, preservation and verification that apply to all other electronic records. According to Ahmed (2025), Pakistani courts have become more accepting of digital evidence and have been skeptical about giving it any weight unless it is properly authenticated and supported by forensics.

This prudent stance is more defensible in the AI age. Apparently realistic digital evidence can be fabricated; courts should not accept this as a trustworthy piece of evidence without question. Meanwhile, the fact that AI tools can generate evidence shouldn't lead to the assumption that all electronic records are suspect. This would make it impossible to use many categories of authentic digital evidence.

So a proper way is to assess the reliability of the evidence. Courts should take account of where the material came from, how it was created, how it was preserved, metadata, the history of the device it was on, a forensic examination and corroborating evidence, as well as any signs of manipulation. This is neither a case of technological naivety nor of technological scepticism.

4.5 Chain of Custody and Forensic Integrity

Chain of custody is the second big problem that was found during the analysis. There are wide-spread concerns regarding the lack of expertise in documenting, preserving and transferring digital evidence in Pakistan (Nazir et al., 2025; Idrees et al., 2026). Basit et al. (2026) also highlight the importance of better rules and regulations that ensure the forensic integrity of electronically stored information.

However, in the AI world, the chain of custody needs to be examined more closely. A chain of custody after a device has been seized indicates that the file has been preserved and handled correctly, however, does not necessarily mean that the content was authentic prior to the seizure. The device may have been created days or months prior to investigators getting their

hands on it. The chain of custody can be perfect and the evidence can be false if the fabricated file is later stored without any changes.

So two distinct integrity questions are identified:

1) Are there any changes to the digital file since acquisition?
2) Content authenticity: Authenticity of the content prior to acquisition?

Pakistan's current framework would be more suitable to respond to the first question as compared to the second. The second question is becoming more critical with the use of AI.

4.6 Role of Digital Forensic Experts

The results also suggest that there is no hope of relying solely on judicial observation or general witness evidence for authentication in the age of AI. Digital evidence is inherently technical and AI-generated evidence is even more technical. Digital forensic evidence needs specific processes of recovery, preservation, analysis, and presentation as digital information may not be directly perceived by the eyes and hands of humans like in the case of any other type of evidence (Yaseen et al. 2025).

Consideration of metadata, file structures, source information, compression characteristics, editing traces, and device records and other technical indicators may be required by forensic experts. But the fact that an opinion is of a high technological level should not automatically ensure its finality. The methodology and expertise of the experts should stay open for discussion and should be evaluated for reliability and limitations.

This analysis also bolsters the idea of more independent and appropriately qualified digital-forensic experts in situations where the evidence is AI-generated and disputed. This aligns with suggestions made by Nazir et al. (2025) for the development of forensic capacity and training of specialists as reforms needed in Pakistan's digital-evidence regime.

4.7 Finding in Relation to Research Question One

The first research question is: How well does the Qanun-e-Shahadat Order, 1984 (article 164) provide for Admissibility and Authentication of AI-generated and AI-manipulated electronic evidence in Pakistan?

The analysis suggests that the law under Article 164 is a valuable albeit limited legal basis. The technology neutral language will enable courts to admit evidence created using new technologies, and this cannot be discarded. But the provision doesn't include specific enough standards for identifying authentic electronic evidence from AI-generated or AI-manipulated documents.

So, in the balance, Article 164 is pretty good on basic admissibility and pretty bad on authentication and reliability for AI. What is missing is not the ability of courts to evaluate electronic evidence, but a clearer definition of the standards that courts should apply to determine the authenticity of technologically complex evidence.

4.8 Objective Two: Legal, Procedural and Forensic Gaps

The second objective investigates the current weak points of the Pakistani legal, procedural and forensic system and the improvements needed to correct these weaknesses. The analysis shows that these deficiencies are present at three interrelated levels: legal standards, procedural mechanisms and institutional capacity.

4.8.1 Legal Gap

A key legal challenge is the lack of a dedicated legislation on AI-generated evidence and AI-manipulated evidence. The QSO acknowledges evidence that is generated using modern devices, and the ETO provides a legal recognition of electronic records. Both frameworks, however, do not delineate synthetic media in detail nor provide a specific authentication process.

This is in line with the recent Pakistani scholarship. Jan (2025) points out some ambiguities in terms of authentication and technical requirements, and Basit et al. (2026) state that there is an inadequate dedicated system in Pakistan for ESI and forensic integrity. The findings are even more relevant to AI, as synthetic content demands more than traditional electronic proof of origin.

4.8.2 Procedural Gap

The second loophole relates to the lack of uniform laws that govern how a court would handle evidence that was created by artificial intelligence. There is a lack of specific guidance on the procedures to follow if one party says that a photograph, audio recording or video has been generated using AI.In the current system, there is insufficient guidance on how authenticity should be challenged when a photograph, audio recording or video is reported to be AI-generated.

A more matured procedure might involve the party relying on the disputed AI related evidence to trace the evidence back to its origin, identify its source, preserve the original file in existence (if applicable) and provide relevant forensic data. There should also be a meaningful opportunity for the opposing party to examine the authenticity through its own means.

This will enhance procedural fairness without automatically prohibiting electronic evidence.

4.8.3 Forensic Capacity Gap

The third gap is in forensic capacity. But even the best crafted legal rule is of little use if investigators and the courts are lacking in qualified experts and reliable digital forensic labs. The researchers Nazir et al (2025) mention the lack of forensic facilities and lack of technical training as significant hindrances to digital evidence adjudication. Similarly, Yaseen et al. (2025) highlight the need for digital-forensic capacity in the investigative framework in Pakistan.

This is heightened by AI, as some digital-forensic techniques aren't always effective at spotting advanced synthetic material. Pakistan needs sustained investments in forensic skills, new tools, norms and training in deepfake and synthetic media analysis.

4.9 AI Detection Tools: A Limited Solution

The analysis refutes the notion that Pakistan will be able to address the deep fake issue by buying AI-based detection software. The detection technologies themselves are rapidly changing and their reliability could fluctuate based on the type of content, generation model and technique of manipulation. So, the output of an AI detector shouldn't be assumed to be automatically correct by a court.

Rather, the use of AI detection should be combined with multiple layers of authentication such as provenance, metadata, forensic examination, source verification, and corroborating evidence. This is more in keeping with the general rule of evidence that reliability should be proved by looking at the cumulative effect of all the circumstances.

4.10 Fair-Trial Implications

The analysis also shows that there is a direct link between AI-related electronic evidence and procedural fairness. Nazir et al. (2025) have foreseen the flaws in the procedures for collecting digital evidence as a threat to the right of fair trial under Article 10-A of the Constitution. The concern is even more relevant in the context of AI, as evidence that is often technically complex might be challenging for the accused to comprehend or dispute without the help of AI.

The consequences are that the defendant may be at a significant disadvantage if the prosecution produces a deep fake video as evidence that it is authentic and the defence has no access to any forensic assistance. On the other hand, if courts discard the true electronic evidence simply due

to the fear of AI manipulation, the prosecution evidence or defence evidence is not allowed to be legally used and this is an unnecessary loss.

The right reform should, therefore, be contestability. Parties should be reasonably provided with the technical information and expertise to challenge disputed digital evidence.

4.11 Finding in Relation to Research Question Two

The second research question is: What are the gaps in the existing legal, procedural and forensic framework in Pakistan regarding the authenticity and reliability of electronic evidence pertaining to AI and what changes are needed to fill these gaps?

The results indicate three major gaps, namely the absence of AI-specific authentication standards, insufficiently standardized procedures for questioning the authenticity of digital data and a lack of forensic and technical capacity. The current system is not ready for advanced AI-based evidence, as it is weak and lacks capacity-building resources.

The analysis thus calls for specific changes, not for the replacement of the entire evidentiary system. Pakistan should also maintain the technological flexibility of Article 164 alongside the introduction of more robust authentication requirements and uniform forensic processes, with also greater resources for experts to be easily available and specific protection for parties contesting AI-generated evidence.

4.12 Overall Findings

The four main findings of the analysis are: The first is that Article 164 offers a foundation – but not a sufficient one – for the AI era. It allows for the use of technologically generated evidence, while failing to distinguish between normal electronic evidence and evidence generated or manipulated by AI. Second, authentication is gaining significance over mere admissibility, as AI-generated evidence can be convincing, yet may not relate to a genuine occurrence. Thirdly, chain of custody is not sufficient as preserving a file after it has been acquired does not prove that it was authentic prior to acquisition. Fourth, legal reform needs to go hand in hand with forensic and institutional reform as, without the presence of qualified experts, with standardized procedures and reliable forensic infrastructure, courts cannot evaluate the evidence created by AI.

The overall findings suggest that Pakistan's legal framework is prepared to a certain extent but not fully ready to address the challenges of the AI era. The country has a valuable statutory framework with the QSO, ETO and PECA and Article 164 provides courts with a certain degree of technological flexibility. But the authentication, chain of custody, forensic capacity, and procedural consistency as problems have been consistently identified by recent scholars in Pakistan (Ahmed, 2025; Jan, 2025; Nazir et al., 2025; Idrees et al., 2026). This does not take away the relevance of this existing system, but rather brings to light the moment when general rules on the admissibility of digital evidence are no longer enough. The best solution is thus to design an evidence-based framework that remains technology neutral, but also establishes more robust guidelines for evidence provenance, authenticity of content, evidence forensics, expert evidence and procedural challenges.

5. DISCUSSION

The results of this current research prove that the law in Pakistan is somewhat ready but not adequately ready for the evidentiary issues faced due to artificial intelligence. The analysis does not justify the simple equation that Pakistan doesn't have a mechanism to deal with electronic evidence. On the contrary, the Qanun-e-Shahadat Order 1984 (QSO) especially Article 164 and the Electronic Transactions Ordinance 2002 and the Prevention of Electronic Crimes Act 2016 offer a valid and useful basis for recognition and use of electronic evidence. The issue is what happens between the general technological recognition and the evidentiary

issues posed by AI-generated and AI-manipulated content. This trend is similar to the one noted by Ahmed (2025), who has noted that Pakistani courts are more accepting of digital evidence but still give significant weight to the need for authentication, forensic verification and the chain of custody. It also complements the findings of Basit et al. (2026) that current framework is not sufficiently detailed in terms of authentication and forensic integrity of electronically stored information for Pakistan.

5.1 Article 164 Provides Flexibility but Not a Complete AI-Evidence Framework

The first important point is that of the sufficiency of Article 164. The provision has been pivotal in enabling the Pakistani Court to tackle with technological advancements due to its wide language, which is capable of yielding evidence generated by modern devices and techniques. The current research is therefore not for the purpose of abolishing Article 164 just because it is not up-to-date with the modern day of artificial intelligence. One of its strengths is that it is technologically neutral. Similarly, Ahmed (2025) shows that the Pakistani courts have found a way to acknowledge digital evidence without specific provisions in the technology itself in Article 164.

But the results showed that there exist a definite limitation with the flexibility of Article 164. The provision mainly addresses the issue of whether court can consider 'technological generated evidence' but does not sufficiently address the ever-challenging question of court authentication of the content presented to it. Among AIs, this difference is very important. As a technological device can no longer just capture or store an event, AI can create an entirely artificial representation of an event. Thus, the evidentiary problem has escalated from the technological admissibility to the technological authenticity.

This discovery is in line with the general literature. While Siddiqui et al. (2025) acknowledge that the significance of Article 164 cannot be overstated in the context of criminal justice in the commonwealth state of Pakistan, they also highlight the ongoing challenges and issues related to technological evidence. Similarly, Basit et al. (2026) find that the current QSO framework does not have adequate measures in place to verify authenticity or to ensure forensic integrity regarding electronically stored information. In an effort to further this argument the present study showed that, indeed, things get worse when the electronic material is synthetically created.

5.2 The Central Problem Has Shifted from Admissibility to Authentication

An important discovery of this study was that the issue of admissibility is no longer the most challenging evidentiary question. Pakistan already has in place systems to present the electronic evidence in the court. The more serious question is whether the evidence is of sufficient authenticity and strength of proof.

This discovery is corroborated by a significant amount of literature in Pakistan. The courts in Pakistan are more inclined to accept digital evidence but are uncertain about its probative value if there is any doubt about authentication and forensic analysis, Ahmed (2025) states. In another study, Nazir et al. (2025) highlight two additional challenges in Pakistan's digital-evidence system: the absence of authentication and chain of custody. The results presented here are not in contradiction with the existing works, but only strengthen them and show that the problem of authentication is significantly more complex with the help of AI.

It's simple because. Traditional digital evidence includes proving the origin of a specific message, from a specific account or the origin of a specific recording, from a specific device. But it's not enough to have a real device or account for the content to be real, in the case of AI-generated content. Fake voice recording can be installed on a real mobile phone. AI can create images and post them to a legitimate social media account.AI can create images and then post

them to a legitimate social media account. Footage can be manipulated in a true CCTV storage system.

As such, there is a growing need for courts to separate source authentication from content authentication. The primary focus of source authentication is identifying the origin of the material, and the primary focus of content authentication is determining whether the material actually is a representation of reality. The findings indicate that the current framework in Pakistan is more effective in dealing with the former, than the latter.

5.3 AI Has Changed the Meaning of Authenticity

The findings also bolster the point that the concept of "authenticity" has fundamentally shifted as a result of AI. A historical electronic record had the potential to be challenged as it could have been edited, copied, or fabricated. AI brings a new and more advanced option — the content can be created in a manner that is coherent from a technical perspective, visually convincing, and hard for the average person to see through.

Grossman and Grimm (2025) present a valuable framework to consider when discussing this issue, which highlights the difference between recognized AI-generated evidence and unrecognized AI-generated evidence. If there is recognition of the use of AI, the court can assess the credibility of the AI process and its applicability. If the evidence is denied to be genuine, however, the court must first decide if the evidence is genuine at all before it can decide if it is the work of AI. The results of the present study validate this separation in the context of Pakistan as it shows that not all evidentiary disputes should be dealt with in the same manner when it comes to AI.

This difference may be of great relevance to Pakistani courts. Where an AI system has produced an image, the key issues might include the purpose of the image being offered, the accuracy and reliability of the image. When one party alleges a purportedly genuine video is a deepfake, the court is asked with a different sort of question: what does it take for a video to be considered authentic? The same approach for both situations as "electronic evidence" is too simplistic a treatment.

5.4 The Findings Confirm the Importance of Forensic Verification

The study also reveals that the verification of electronic evidence should increasingly be the focus of the processing of disputed electronic evidence for forensic purposes. The observation aligns with those of Usman (2022), who stressed the significance of expert evidence for the assessment of digital evidence, and Idrees et al. (2026), who stated that one of the ongoing challenges in Pakistan's digital evidence framework is the forensic verification of digital evidence.

The need to have forensic expertise increases significantly when the AI-generated content is included. If your manipulated photo or video is obvious, a judge may be able to identify the manipulation, but if the photo or video is a high-quality fake, they will likely not pick up on the manipulation. Therefore, a forensic analysis might be necessary to investigate metadata, source information, file structure, compression style and editing history.

The results also suggest, however, that the use of a forensic expert should not always be considered conclusive. Opinion of an expert is itself evidence and can be judged in its reliability based on the methodology employed, the skills and knowledge of the expert and the limitations of the technology. In the context of using AI applications as evidence, Grimm et al. (2021) stress the need to assess the validity and reliability of the applications. This is especially crucial when AI tools are employed to gauge an evidence's authenticity.

5.5 Chain of Custody Is Necessary but No Longer Sufficient

The literature and findings are quite consistent on the critical importance of chain of custody. The preservation and handling of electronic evidence are critical issues that have been raised by Nazir et al. (2025) and Idrees et al. (2026) in the context of Pakistan. A similar call for better and more standardised methods of preserving the forensic integrity of digital evidence is made by Basit et al (2026).

The present study argues, however, that there is another type of distinction that is of special relevance in the context of AI. A chain of custody may be able to prove that a file has not been modified since it was collected but cannot necessarily prove that it was authentic before it was collected. Chain of custody creates continuity and handling and content authentication creates a determination of authenticity of the information contained in the file.

This separation reveals a weakness in the approach of using traditional digital-forensics method. Imagine that investigators confiscate a device with a deepfake video on it and then successfully preserve and transfer it.Suppose investigators are able to confiscate a device with a deepfake video on it, and then to successfully preserve and transfer it. Even if the chain of custody is flawless, the video could still show an event that never occurred. So, AI would need a model of evidence in which chain of custody was a part of the evidence for authentication, not an authentication solution.

5.6 The Findings Support a Layered Authentication Model

Based on the study findings, there is a need to shift towards a multi-level authentication system instead of a single test or technological indication in Pakistan. This type of a model would take into account the nature of the evidence, the context in which it was produced, the original device, the metadata, the evidence source, the chain of custody, the forensic examination process, the evidence source, and the corroborating evidence and expert testimony.

This is aligned with Hak (2024) who states that provenance and the metadata and forensic examination are important in assessing image-based evidence. It's also in line with Grossman and Grimm (2025), who warn of the danger of simply asking a technical question about deepfake detection. Reliability of AI generated evidence should be assessed not only in terms of technical attributes, but also in relation to its context.

This would be more suitable option for Pakistan where not all the courts would have access to advanced AI-detection technology. A multi-layered structure enables courts to rely on more than one type of evidence and not require that it all be based on a single software tool. It can also help prevent over-reliance on automation systems for detection.

5.7 AI Detection Technology Cannot Be the Sole Solution

The other significant discovery is that Pakistan cannot address the issue just through the judicial system by incorporating AI detection software. As the generative AI evolves quickly, detection tools are evolving even faster and may now become obsolete. An effective detector for synthetic media of one generation might not be as effective for newer systems.

Similarly, Grossman and Grimm (2025) highlight the challenges of detecting a deepfake and the challenge of distinguishing real content from fake content. The message to Pakistan is that AI detectors shouldn't be absolute measures of authenticity, but rather additional forensic tools. This is significant as it could lead to a new type of evidentiary error if the AI detection becomes too prevalent. Courts could refuse to accept true evidence as fake or accept fake evidence as true, depending upon whether a detector misidentifies it as a fake or fails to detect manipulation. It is therefore best to use automated tools, in conjunction with expert examination, provenance information and contextual corroboration.

5.8 The Findings Reveal a Forensic Capacity Problem in Pakistan

The second aim of the study was to identify the gaps in the law, procedure and forensic aspects. The results show that the issue is definitely not solely a legislative one. The reforms may be effective, even if Pakistan did change the QSO tomorrow, if the courts, investigators and forensic laboratories were not able to put the new standards into practice.

This is an indication of the need for technical skills and forensic capability, which are still weak areas, as noted by Ahmed (2025), Nazir et al. (2025), and Idrees et al. (2026). Institutional problem is escalating to an urgency with the technologically sophisticated digital manipulation. Statutory reform is therefore required, and special training of judges, prosecutors, defence advocates, investigators and digital-forensic experts is needed in Pakistan. Judges should not be made into computer scientists. Instead, judicial actors must be technologically literate enough to appreciate what the forensic experts are saying and to find any flaws in their methodology and to assess if the two opposing expert opinions are sufficiently backed-up.

5.9 Implications for Fair Trial and Due Process

The results also have important implications for the rights to fair trial. The issue of AI-generated evidence is not just a technical one as the quality of evidence can directly impact criminal proceedings. If someone is guilty because fabricated audio, video or images are believed to be real, then an accused individual may be convicted for an event that never really happened.

Meanwhile, too much doubt regarding electronic evidence could lead to the other issue. Even if there is genuine evidence, it could be disallowed because of the theoretical possibility of its manipulation by AI. The results thus support a balanced approach that balances the potential for manipulation with appropriate questioning and not blanket rejection.

Disputed AI-produced evidence poses substantial risks of unfair prejudice, as Grossman and Grimm (2025) point out, while Dalal et al. (2025) argue that judges should proactively manage alleged deepfake evidence. Their method is for the courts to make serious attempts to resolve the authentication quandaries before the evidence in question is permitted to unduly influence the fact-finding. This helps establish procedural processes for Pakistan which allow parties to raise issues of authenticity at an appropriate stage and which enable courts to direct the appropriate forensic examination before giving substantive weight.

5.10 Comparison with Existing Literature

The present results generally corroborate, but do not contradict, the previous results, and at the same time extend the literature in an important dimension. In Pakistan, any of the studies mentioned above – Ahmed (2025), Nazir et al. (2025), and Idrees et al. (2026) – have highlighted issues related to authentication, reliability, chain of custody and forensic capacity. Basit et al. (2026) also states that the standards for electronically stored information should be more clear and coherent in Pakistan. The findings of the present study are consistent with these studies, but it is a different problem, in different scale and nature, due to the advent of the generative AI.

Likewise, there has been an increase in the literature surrounding deepfakes and evidence created by AI. Grossman and Grimm (2025) highlight the difference between acknowledged and unacknowledged AI-generated evidence and Dalal et al. (2025) stress proactive judicial control over disputed deep fake evidence. The present research seeks to bring these insights to the context of Pakistan and to ask whether the Article 164 and related legislation can survive this stark and obvious ‘evidence environment’.

The novelty of the present study, thus, is linking two areas of scholarship that have traditionally been independent of each other – namely, Pakistani scholarship on electronic evidence, and international scholarship on AI-generated evidence. The results in this study show how the

weaknesses which were identified in the traditional electronic-evidence framework in Pakistan become more significant with the creation of synthetic evidence.

5.11 What Legal Reform Should Look Like

The findings neither advocate any change in Article 164 nor call for a new evidence law. It would be overreacting to respond like this. The better option is to follow the targeted reform and procedural clarity.

First, the QSO needs to establish the evidentiary treatment of AI-generated and AI-manipulated content. The bill should address common and AI-generated evidence and disputed AI-generated evidence.

Second, Pakistan has to have more specific requirements for authentication. These should take into account: source verification; provenance; metadata; forensic examination; expert testimony and corroborating evidence.

Third, the law should make it clear what the relationship is between chain of custody and content authenticity. Keeping an evidentiary chain should not be regarded as proof of authenticity of the content itself, but it should still be considered as an essential part of a system of proving authenticity.

Fourth, procedural rules should include a process to question and, if required, request to have the evidence, which might have been produced by an AI system, forensically tested, prior to its substantial evidentiary weight.

Last but not least, institutional investment is necessary to support legal reform. The effective working of the revised legal framework requires digital-forensic laboratories, expert accreditation and judicial training and technical capacity.

5.12 Overall Discussion

The overall conclusions reflect that Pakistan is not legislatively under-equipped to deal with electronic evidence but it is not ready for the electronic evidence in the age of artificial intelligence. The QSO, ETO and PECA has set a very good basis and Article 164 has given Pakistani courts much flexibility in admitting technologically generated material. However, the advent of generative AI reveals the shortcomings of a model based on the premise that electronic technology was primarily a mechanism for recording, storing or conveying information. Authenticity can now be made challenging with the ability of AI to recreate realistic representations of people, events and communications.

The results thus justify the move from an admissibility-oriented to an authentication- and reliability-oriented approach. It is not as if courts should be cynical about technology. It implies that courts are entitled to insist that the evidence show higher evidence of the technology's characteristics that could lead to synthetic generation or manipulation. The literature can be used to support this direction: Pakistani literature shows an emphasis on authentication, forensic integrity and technical capacity (Ahmed, 2025; Nazir et al., 2025; Idrees et al., 2026); but international literature highlights the necessity of a proactive and differentiated judicial approach towards AI generated evidence (Grossman & Grimm, 2025; Dalal et al., 2025).

The main question is not whether Pakistan should embrace or reject evidence relating to AI. The crux of the matter is whether Pakistan can set up a legal mechanism that can differentiate technologically advanced evidence that can be trusted by a judge from technologically advanced evidence that can appear to be trusted by a judge. The results indicate that the current process could continue to be based on Article 164, albeit with improved authentication rules and greater forensic measures, and with a greater focus on the ability to handle challenges to disputed AI-generated evidence and to the reliability of the evidence produced. If these are not undertaken, the flexibility of the current evidentiary regime could become its biggest liability

as a measure meant to keep up with the changing times may allow for more and more elaborate synthetic evidence to be admitted into court proceedings without adequate methods to determine its authenticity.

6. CONCLUSION

The result of this study is that the current legal regime in Pakistan is somewhat ready for the AI era of electronic evidence however is not fully equipped. The most important laws regarding electronic evidence such as the Qanun-e-Shahadat Order 1984, Article 164, the Electronic Transactions Ordinance 2002, and the Prevention of Electronic Crimes Act 2016 were prepared prior to the advent of electronic technology that could produce highly realistic synthetic images, videos, voices and documents by artificial intelligence. The results illustrate that the authentication of any electronic evidence, its reliability, provenance and forensic integrity are the current major hurdle, rather than the basic admissibility of the evidence. While Article 164, in its wording, does give some technological flexibility, it does not give adequate standards to determine what constitutes genuine electronic evidence and what constitutes AI-generated or manipulated material.

The study also reveals that chain of custody alone will not prove to be a sufficient measure to establish the authenticity of digital content since a perfectly preserved file can be created prior to its entry into the chain of custody. Considering these issues, Pakistan should opt for specific rather than general law reforms, such as the establishment of a benchmark for presenting evidence generated by AI, a protocol for rebutting evidentiary material produced by AI, and the capacity of digital forensic experts that can be mobilised when necessary for both prosecution and defence to challenge the authenticity of AI-generated materials.

Hence, in the light of the study, it is suggested that Pakistan should stick to the technological flexibility of Article 164 and evolve an evidence-based framework of AI that will be based on provenance, forensic evidence, expert opinion, corroboration and procedural fairness. The ability of Pakistan's legal system to keep pace with the AI era will not be an issue of simply being able to accept and recognize electronic evidence, but it will be whether it can be able to distinguish between genuine digital evidence and the one that appears to be genuine.

REFERENCES

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). (Tahdhib al-Afkar)

Ahmed, F. A. (2025). Jurisprudential status of digital evidence in Pakistan while courts' interpretation of Article 164, Qanun-e-Shahadat Order, 1984.

Ahmed, 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**. (XLSLOT88)

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.

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**. (Policy Journal of Social Science Review)

Grossman, M. R., & Grimm, P. W. (2025). Judicial approaches to acknowledged and unacknowledged AI-generated evidence. *Science and Technology Law Review, 26*(2).

Hak, J. W. (2024). The authentication of image-based evidence. In *Image-based evidence in international criminal prosecutions: Charting a path forward*. Oxford University Press.

Idrees, R. Q., Hussain, N., & Shahid, A. (2026). Electronic evidence in Pakistan: Admissibility, reliability, and judicial practice.

Idrees, R. Q., Hussain, N., & Shahid, A. (2026). *Electronic evidence in Pakistan: Admissibility, reliability, and judicial practice*. **Journal for Current Sign**. (Current Sign Review)

Jan, A. (2025). Digital evidence in Pakistan: A doctrinal assessment of admissibility and reliability in criminal trials.

Law & Justice Commission of Pakistan. (2026). *National Guidelines for the Use of Artificial Intelligence in Judicial Institutions of Pakistan*. (LJCP)

Nazir, S., Asif, M., & Khan, A. U. (2025). Digital evidence in Pakistan: A doctrinal assessment of admissibility and reliability in criminal trials.

Pakistan. (1984). *Qanun-e-Shahadat Order, 1984*. Ministry of Law and Justice, Pakistan Code.

Pakistan. (2002). *Electronic Transactions Ordinance, 2002*. Ministry of Law and Justice, Pakistan Code. (Pakistan Code)

Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016*. Ministry of Law and Justice, Pakistan Code.

Siddiqui, K. M., Rehman, T. U., & Siddiqui, I. K. (2025). Use of Article 164 Qanun-e-Shahadat Order, 1984 in criminal justice system of Pakistan.

Siddiqui, K. M., Rehman, T. U., & 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. (JALT)

Ullah, Z., Ullah, M. K., & Abbas, H. (2025). The impact of digital evidence laws on cybercrime prosecution in Pakistan.

Usman, M. (2022). Digital evidence: Testimony of expert witness in Pakistani law.

Westerlund, M., et al. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*.