



DOI: [10.71317/jgst.2.5.2026.499](https://doi.org/10.71317/jgst.2.5.2026.499)

Journal of Global Social Transformation

Journal homepage: <https://rjsaonline.org/index.php/JGST>



AI Generated Evidence in the Courtroom: Deepfakes, Evidentiary Authenticity, and the Threat to Fair Trial Rights in Pakistan

Hafiz Omer Abdullah¹, Muhammad Imran Darwaish², Dr. Mazhar Jamal Chaudhry³, Mohsin Ehsan⁴

¹ Lecturer, Department of Law & Criminology, University of Sahiwal

Email: omerabdullah@uosahiwal.edu.pk

² Advocate High Court Lahore, Visiting Lecturer, Himmayat-ul-Islam Law College Lahore

Email: imrandarwaish@gmail.com

³ Lecturer in Law and Policing, Department of Law and Policing, York Business School, York St John University, York, England

Email: mazharjamal2003@yahoo.com

⁴ LL.M Punjab University, MSc Criminology Punjab University, Deputy District Attorney, Law Department Punjab

ARTICLE INFO	ABSTRACT
Submission: April 19, 2026 Revised: May 03, 2026 Accepted: May 16, 2026 Available Online: May 30, 2026 Keywords: Deep fakes, Digital Evidence, Authenticity, Admissibility, Forensic Readiness, Procedural Safeguards, Fair Trial, Pakistan Corresponding author: Hafiz Omer Abdullah Email: omerabdullah@uosahiwal.edu.pk	The current study focused on implications of artificial intelligence generated deep fakes on authenticity and admissibility of digital evidence and safeguarding of fair-trial rights in Pakistan. It examined the relationships among perceived deep fake threat, institutional/forensic readiness, legal-procedural protections, and authenticity/confidence in admissibility and fair-trial protections. The positivist philosophy and deductive method were used in this study, along with quantitative cross sectional explanatory design. A self-structured five-point Likert scale questionnaire was used to gather data with 300 respondents, which comprised judges, judicial officers, practicing advocates, public prosecutors, investigators, cybercrime officers and digital-forensic experts. The data were analyzed by SPSS software on frequencies, percentages, mean, standard deviation, and Pearson correlation and regression analysis. The results showed a very high perception of the threat from deep fakes, including fabricated evidence, incorrect decisions by judges, and falsified recordings of real evidence. Institutional and forensic readiness was considered to be low, due to lack of training, access to qualified experts, laboratory capacity and lack of validated detection tools. The results of the regressions confirmed the significant negative effect of perceived deep fake threat on authenticity and the admissibility of confidence. In contrast, there was a significant increase in evidentiary confidence of institutional and forensic readiness. Legal-procedural protections had a significant positive impact on perceived fair trial protections, and authenticity and admissibility confidence significantly contributed to perceptions of procedural fairness. There was support for all four research hypotheses. The study found that the visual realism method was no longer sufficient in determining the authenticity of digital evidence. Pakistan needed evidences-driven guidelines for AI, certified forensic labs, expert training, preservation of original documents and metadata, clear expert reporting, de/judicial examination, and sound judgments. For the purposes of maintaining digital evidence and assuring fair trial rights, a multi-layered technical capacity and procedural protections were required.

Introduction

Artificial intelligence (AI) has revolutionized the methods by which digital information is generated, edited, written, stored and shared. Generative AI systems can generate written text, images, audio and video content that is remarkably similar to that of humans. One of the most important types of AI-generated content is deep fakes. Deep fakes are machine-learning systems that are used to produce or manipulate audiovisual content, causing one person to look like another and do something they didn't actually do, or to say something they didn't say, or to be present at an event where they were not (Qin & Chen, 2025).

Deep fake" is derived from the fusion of "deep learning" and "fake." The initial deep fakes relied on generative adversarial networks. These systems are composed of two adversarial neural networks – a generator that creates synthetic content and a discriminator which looks to determine whether the content is real or fake. The more the generator is trained, the more it can produce realistic outputs. Deep fake technology today also uses diffusion models, auto encoders, transformers, facial-reenactment systems, lip-synchronization applications, and voice-cloning technologies (Paris, 2021).

There are not only harmful uses of synthetic media, but also beneficial ones. In filmmaking, education, historical reconstruction, advertising, accessibility, artistic expression, and safeguarding personal identities, AI-generated content can be utilized. But the same technology can be used to perpetrate fraud, harassment, political misinformation, sexual exploitation, extortion, false confessions, identity theft, and tampering with the judicial process (State v. Ahmed Omar Sheikh, 2021). The legal issue is when a fake or altered document is knowingly passed off as a true record of a true event.

Digital evidence is becoming more and more critical in court proceedings. CCTV footage and mobile-phone recordings are routinely turned over in criminal proceedings and civil proceedings, as are social media videos, call recordings, screenshots, emails, surveillance images and electronically stored information. In the past, it was thought that AV was very persuasive due to the apparent representation of reality. In the absence of any indicators of editing or tampering, judges and fact-finders generally believed that a recording would be reliable (Murray, 2025).

This has been significantly undermined by the advent of deep fake technology. The high resolution recording, the realistic voice or the apparent background has lost its independence with regard to authenticity. Reconstructed content can be created with realistic visual and auditory features. This means that courts are left with a challenging task to differentiate between real recordings, conventional edit recordings, and manipulated recordings by AI and completely fabricated synthetic media (Shirish & Komal, 2023).

This happening was termed a crisis of legal authenticity by Muhammad (2025). His work showed that traditional evidentiary frameworks are undermined by deep fakes, novel privacy and reputational injuries are caused by these images, and platforms lack accountability and international oversight. He suggested implementing a regulatory regime on the basis of authenticity infrastructure, platform gate keeping and cross-border legal harmonization (Singh & Dhumane, 2025).

Researchers explored deep fakes' impact on International and Pakistani justice systems. His research described the various possibilities of using synthetic media in fabricated criminal allegations, false confessions, voice-cloning fraud, sexual exploitation, political disinformation and evidentiary manipulation. It also noted that there are significant gaps in the current legal system, forensic institutions, training of the judiciary and procedures of collecting digital evidence in Pakistan (Llorente, 2024; Giangiacomo, 2025).

Combining the two studies indicates that there are two evidentiary threats with deep fakes. Firstly, fake information can be introduced and used as a true document. A convincing but false video can result in wrongful conviction, false civil liability, reputational damage or an unjust judicial order. Second, authentic evidence could be thrown out if the accused or another interested party claims it is AI-generated. This is referred to as the "liar's dividend." It gives people the benefit of the public awareness that recordings can be manipulated (Lin, 2025).

It is not the automatic rejection of digital evidence that's the right legal answer. Electronic recordings are invaluable in modern times when establishing facts. Likewise, when it comes to the audiovisual evidence, a court should not believe it simply because it looks real (Sughra Bibi v. State, 2018). There is a need to consider evidence of provenance, metadata, chain of custody, cryptographic integrity, forensic findings, contextual consistency, expert evidence, and corroborating information to implement a balanced approach in evaluation of the evidence in court (Liu et al., 2023).

Deep fakes also bring considerable concerns for fair trial. If the original file, source device, forensics method, or software is no longer available, a party may not be able to rebut the evidence produced by AI. This means that less-wealthy litigants would not be

able to challenge technical evidence, whereas more affluent accused may be able to secure advance assistance in the field of forensic science. Proprietary detection systems can come up with results without revealing their method. This situation can have a detrimental effect on equality of arms, the presumption of innocence, and the right to present a defense and challenge adverse evidence (Khan, Usman, & Amjad, 2023).

Both of the two source papers make in-depth doctrinal and comparative discussions, and neither documents the perceptions of the professionals responsible for the collection of electronic evidence quantitatively. There is scant empirical evidence that reflects whether current laws and institutions are effective in addressing AI-generated evidence in Pakistan. The present study attempts to fill this gap in research with a quantitative analysis of deep fake threat, institutional readiness, legal-procedural safeguards, and authenticity and admissibility confidence, and fair-trial protection (Khan & Usman, 2023).

Background of the Study

The use of photographs, recordings and digital documents were evidentiary and created in an era when more sophisticated manipulation of these was relatively more difficult, expensive and visible. The traditional methods of authentication were often through witness evidence, chain of custody, identification of the recording device or examination of the physical characteristics (Khan, Usman, & Amjad, 2020). The impact of digitalization was that evidence changed in nature because it became possible to reproduce information without quality loss. Metadata, file systems, storage devices, and cryptographic hashes, as a result, were important tools for proving integrity (Maqsood Alam v. State, 2024). Generative AI has brought a new major shift, as manipulation could be happening at the level of content creation itself (Khan & Jiliani, 2023).

A file can have a valid chain of custody and a stable hash value yet still be synthetic. Hashed verification will only be able to verify that the file is a true copy of the original file obtained by the investigator, not that the event in question did actually happen. The file might be a “made up” file created before it was saved to the device. Courts are therefore required to make a distinction between file integrity and factual authenticity (Hui et al., 2025).

Technologies have been created to detect inconsistencies in the movement of the face, light, shadowing, lip synching, voice patterns, pixel distribution, and artifacts created by the face model. However, there are limitations to detection systems. They may not perform as well if the content is compressed, cropped, re-recorded, filtered, or produced by a model they did not learn. An opponent could also edit content in a particular way so as to evade recognition (Gupta & Fatunmbi, 2024).

The law is therefore not able to rely on just one technological solution. There must be several means of verification in order to be able to reliably assess the courtroom, such as provenance analysis, examination of the metadata, investigation of the source device, contextual corroboration, witness statements, expert evaluation and consideration of uncertainty – the latter being transparent (Gregory, 2024).

The courts of Pakistan have started accepting electronic records and evidence generated with modern devices. Under the general provisions of Article 164 of the Qanun-e-Shahadat Order 1984, evidence obtained by means of modern devices or techniques is admitted. The Prevention of Electronic Crimes Act, 2016 deals with different types of illegal electronic activity (Mkpo, 2025). Both approaches, however, do not provide a detailed procedural requirement that is specifically geared towards AI-produced audiovisual evidence (Ghiurău & Popescu, 2025). However, effective implementation of comprehensive legislation requires the presence of trained investigators and competent forensic examiners, accredited laboratories, judicial education, prosecutorial expertise, and access to technical assistance from the defence, and secure evidence-preservation systems. The current study, therefore, analyzes legal rules and institutional readiness as a whole (Furizal et al., 2025).

Statement of the Problem

AI generated deep fakes pose a risk to the integrity of digital evidence and the courts’ role of discovering the truth. They can be used to make confessions, fake witnesses, fake surveillance, manipulate the statements of political or religious leaders; impersonate victims and fabricate evidence against an innocent person. Meanwhile, the advent of deep fakes can mean that the truth is undermined by false evidence being challenged as having been manipulated.

The current laws of Pakistan have acknowledged electronic evidence, but they don’t have detailed rules on its authenticity, admissibility, forensic techniques, burden of proof, expert disclosure and procedural challenges in relation to AI. Thus, different judges may hold different views on the same audiovisual evidence. Original files or metadata may not be preserved and parties may not have equal access to forensic expertise.

The problem does not exist just in terms of legislative language. On the institutional front, Pakistan also has challenges, such as the lack of AI-forensic capacity, disparity in the availability of specialized laboratories, limited training of judges, failure to have a uniform evidence-preservation procedure, and uncertainty over the efficacy of detection tools.

These issues are located in the source papers through the use of doctrinal and comparative analysis. They lack quantitative data on the perceived seriousness of the threat or effectiveness of current responses from professionals. Therefore empirical studies are needed to explore the effect of perceived deep fake threat, institutional preparedness, and legal-procedural safeguards on the trust in the evaluation and protection of digital evidence and the right to a fair trial.

Purpose of the Study

This study aims to explore the legal and institutional issues arising from AI evidence in Pakistani courts on a quantitative basis. It examines the impact of perceived deep fake threat, institutional and forensic preparation and legal-procedural protections on the confidence of authenticity and admissibility of digital evidence. The study also explores if confidence in the evidence-evaluation contributes to perceived protection of right to a fair trial.

Research Objectives

The study has four research objectives:

1. To examine the effect of perceived deep fake threat on confidence in the authenticity and admissibility of digital evidence.
2. To determine the effect of institutional and forensic readiness on confidence in the authenticity and admissibility of AI-susceptible evidence.
3. To evaluate the effect of legal-procedural safeguards on perceived protection of the right to a fair trial.
4. To examine the effect of authenticity and admissibility confidence on perceived protection of the right to a fair trial.

Research Questions

1. What effect does perceive deep fake threat have on confidence in the authenticity and admissibility of digital evidence?
2. To what extent does institutional and forensic readiness influence confidence in evaluating AI-susceptible evidence?
3. What effect do legal-procedural safeguards have on perceived protection of the right to a fair trial?
4. How does authenticity and admissibility confidence affect perceived fair-trial protection?

Research Hypotheses

H1: Perceived deep fake threat has a significant negative effect on confidence in the authenticity and admissibility of digital evidence.

H2: Institutional and forensic readiness has a significant positive effect on confidence in the authenticity and admissibility of AI-susceptible evidence.

H3: Legal-procedural safeguards have a significant positive effect on perceived protection of the right to a fair trial.

H4: Confidence in the authenticity and admissibility of digital evidence has a significant positive effect on perceived protection of the right to a fair trial.

Significance of the Study

The study is important because it uses doctrinal legal analysis and quantitative evidence. The majority of the legal research on deep fakes focuses on potential damage and calls for law reform. Less research compares the perceptions of professionals involved in the admission, challenge, examination and evaluation of digital evidence.

Study may highlight areas for specialized judicial training and/or guidance for judges. It could contribute towards judicial academies to create programs on deep fake creation, metadata, chain of custody, uncertainty of the facts, expert evidence, and liar's dividend.

The study could help advocates and public prosecutors understand the procedural principles required to present or refute evidence that is subject to AI. It can, perhaps, encourage more interest in the original files, the original source, the disclosure, the methodology of the experts, and corroboration.

The results could highlight evidence acquisition and preservation gaps, forensic referral and documentation issues for investigation agencies. So, investigators need to retain the digital material to them so it can be reviewed and questioned later.

The study can be used to support investment in forensic institutions in validated tools, trained staff, accreditation, quality assurance and transparency reporting. It can also bring attention to the necessity to express technical uncertainty in language communicable to judges and lawyers.

The study could serve as an empirical ground for the reform of the Qanun-e-Shahadat Order, PECA, rules of criminal procedure and judicial practice directions for the policy makers. It will aid in differentiating between proposals that can be substantiated by professionals and those that are simply fantasies.

Accused persons, complainants and litigants will have less risk of wrongful verdicts due to improved procedures with regard to digital evidence. In doing so, the study helps to enhance judicial accuracy, institutional legitimacy, and public trust in judicial processes.

Delimitations of the Study

The study was limited to judges, advocates, prosecutors, investigators, cybercrime officers and digital forensic experts in Pakistan. It was particularly focused on AI-generated or manipulated images, videos and audio recordings which are or may be used in judicial proceedings. The study assessed the level of legal, procedural, institutional and forensic preparedness, but it was not a trial of deep fake detection software itself. The applications of AI were limited to evidentiary matters, and general applications in legal research, automated case management, predictive justice, and administrative decision making were considered provided they dealt with evidentiary issues. The study focused on the aspects of authenticity, admissibility, forensic readiness, procedural safeguards, and fair-trial rights, while political misinformation, platform regulation, and national security were dealt with only when they are directly related to judicial evidence.

Limitations of the Study

The study relied on self-reported data which could have been affected by social-desirability, professional caution and respondents' technical understanding. Participants may have given their opinions about forensic procedures without having dealt with a case involving a deep fake. The cross-sectional design did not draw causal inferences over time and recent changes in technology may have influenced the continued significance of the findings. Difficult access to judges, investigators, forensic experts, and lengthy schedules and institutional restrictions, along with the use of purposive selection of specialized respondents, reduced the generalisability of the results. Moreover, perceived fair-trial protection was measured, not actual judicial results; therefore, the study's results should be interpreted in conjunction with future analyses of cases, experiments, interviews, and forensic performance evaluations.

Literature Review

Nature and Development of Deep fake Technology

Deep fakes are AI-based created or manipulated media. They can swap out one face for another or mimic voice inflections, change lip motion, rework facial expressions or even create fake personas and fictional people and situations altogether. Early deep fakes were developed with the help of generative adversarial networks. It was an artificial content that was generated, and a discriminator that tried to detect whether the content was genuine. There was a competition between two systems that enhanced the realism of the resulting outputs (Cornacchia & Scollo, 2025).

Still further improvement of synthetic-media quality has been achieved using diffusion models. The systems start with a visual noise and over time synthesize detailed images or videos based on patterns learned. Voice-cloning technologies emulate pitch, accent, rhythm and emotion through audio samples (Khan, Abd Elrhim, et al., 2021). The availability of these systems has greatly improved. Advanced programming skills or complex equipment are no longer necessary to ensure that the synthetic content is believable. This accessibility helps to open up legitimate creative possibilities, but also reduces the barriers to evidentiary manipulation (Chesney & Citron, 2019a).

Types of Deep fakes Relevant to Courts

In identity-swap videos, the face or the appearance of a person is swapped with another. Such videos might falsely show an accused person at the time and place of an offence in criminal proceedings. Facial-reenactment deep fakes alter facial expressions or movements of the original person (Pakistan Telecommunication (Re-organization) Act, 1996). They might be used to make false impressions of speech, emotion or behavior. Lip-synchronization systems are systems that adjust lip movements to fit artificial sound. These systems can produce seeming convincing speeches, admissions, threats, or agreements (Apolo & Michael, 2024; Code of Criminal Procedure, 1898).

Voice-cloning technology is the technology that replicates an individual's voice. It can be used to make telephone calls, to give authorization instructions, threats, confessions or financial transactions. Synthetic-person technology is a technology which produces synthetic individuals that are not actually persons (Payment Systems and Electronic Fund Transfers Act, 2007). These identities can be utilized to make false witnesses, social media profiles, transaction records or digital communications. AI-generated documents and screenshots can also be created that mimic real correspondence, financial data, online conversations or official records (Ahmed & Chishti, 2022).

Deep fakes and the Collapse of Visual Trust

The convincing power of audiovisual evidence has traditionally been based on the assumption that such evidence captured what really happened. While it was possible to edit traditional recordings, the manipulation of large quantities of recordings was often complex to perform and left behind visible marks. Deep fakes disrupt this association between what's seen and what's not. Synthetic recordings can duplicate natural lighting, facial expressions, sound, background detail and emotions. Manipulation may not be obvious to the untrained eye (Bernacka, 2025).

Muhammad (2025) argued that the justice system can no longer depend upon visual trust. The realism of an item must be substantiated by evidence of source, history, technical characteristics and surroundings (Khan, Jillani, Abdelrehim Hammad, et al., 2021). This doesn't mean that 100% distrust of digital evidence is necessary for this development. Instead, it demands measured self-assurance. The level of authentication should be commensurate with the importance, the questionable nature and technical susceptibility of the evidence (Casey, 2020).

Authenticity of Digital Evidence

The legal procedure by which evidence is accepted as what the one who presented it claimed. The traditional evidence was authenticated by the testimony of the person who had recorded it, identification of the recording device, and the chain of custody (Electronic Transactions Ordinance, 2002). When determining whether AI-generated evidence is admissible, courts took into account who created the file, the device AI was using, the original version of the file, evidence of editing of the file, available metadata, and cryptographic hash values (Qanun-e-Shahadat Order, 1984, arts. 73-78). They also analyzed if the chain of custody had been documented, forensic analysis had been performed and that the recording had been consistent with the other evidence available (Qanun-e-Shahadat Order, 1984, art. 164). It was essential that the opposing party be able to examine the file without the assistance of the opposing party. It was important to have the ability for the opposing party to examine the file without the assistance of the opposing party in order to have transparency and procedural fairness. However, the absence of metadata and/or a faulty chain of custody did not constitute proof of fabrication, and authenticity was evaluated based on a full analysis of the circumstances (Abdelrehim Hammad et al., 2021).

File Integrity and Factual Authenticity

File integrity should not be confused with factual authenticity. The hash value can be used to show that a file has not been modified since it was acquired. It is unable to certify that the original content is authentic at the time of its creation (Qanun-e-Shahadat Order, 1984, art. 59). For instance, a video can be taken from a suspect's device, its hash value recorded, and an exact duplicate will be made. The process verifies the examined copy to be the same as the acquired file. The suspect, however, if he or she had made the video with AI before, then it will still be a synthetic video (Ishtiaq Ahmed Mirza v. Federation of Pakistan, 2019). The courts should therefore take into account not only the integrity of the process used to manage the evidence but also the authenticity of what is being represented. Provenance systems that document the creation and editing timeline of digital content could help this investigation (Chesney & Citron, 2019b).

Reliability of Deep fake-Detection Tools

Deep fake detectors look for patterns in digital content that are linked to its artificial production. They can analyze facial characteristics, flipping, lighting, shadows, head movements, sound frequency, compression patterns, pixel distribution or even model-specific artifacts. The accuracy of detection isn't guaranteed or automatic. Content generated by newer models might not be recognized by the detector trained on older models (Kashif Anwar v. Aga Khan University, 2013). Resizing, compression, cropping, filtering, social-media processing, and screen recording can all cause performance to drop after the process. The courts should thus not accept the probability score of a detector as final evidence (Muhammad Ammar Shafi v. State, 2025). Expert testimony should provide an explanation of how the method was performed, the training conditions, the validation (if applicable), known limitations, error rates, and alternative interpretations. There should be sufficient information provided to the opposing party to challenge the analysis. Where a proprietary company refuses to provide useful information about its technology, the court must determine whether a reliance on the opinion formed as a result will prevent procedural fairness (Ferguson, 2018).

Pakistan's Existing Legal Framework

There are general provisions in Pakistan's legal system that can be invoked for the actions involving deep fakes. The Pakistan Penal Code could deal with fraud, defamation, forgery, criminal intimidation and more. PECA 2016 could be relevant to certain types of identity misuse, dignity related harm, unauthorized conduct and cybercrime (Shafqat Masih v. State, 2021). The main frame of evidence is derived from the Qanun-e-Shahadat Order. The existence of evidence provided by modern devices or techniques is recognized in Article 164. The definition of deep fakes is not specific to AI, and there is no standardized process for the authentication of synthetic evidence under the law (Prevention of Electronic Crimes Act, 2016). There is no AI-specific terminology, which can cause uncertainties in charge formulation, investigation, expert evaluation and judicial decision. Common legal analogies to editing, spoofing, impersonation or forgery may apply (Ghani et al., 2025).

Theoretical Foundation

The study is guided by legal authenticity theory, procedural-justice theory and institutional-readiness theory. Legal authenticity theory acknowledges that the ability of judicial systems to link evidence to its claimed origin and significance relies on stable ways to do so (Amar Yasir Ali v. State, 2013). Traditional markers of authenticity are undermined in the deep fakes and new combinations of technical and procedural verifications are needed. According to the theory of procedural justice, fairness, transparency, neutrality, participation, and opportunity to challenge the unfavorable material are important. Legal validity of the AI evidence relies not just on the accuracy of the evidence but also on the understanding and contestability of the evidence by each party (Khan, Khan, & Khan, 2022). The institutional-readiness theory offers an explanation in terms of the infrastructure, competence, policy and resource requirements, and the extent of coordination, that are necessary for an organization to effectively manage technological change. Legislation is not enough to help courts tackle deep fakes evidence (Hausknecht, 2025).

Research Gap

A series of studies examined reviewed showed that there are significant legal, evidentiary, ethical and procedural concerns with the use of AI-generated deep fakes. But most of the earlier studies used doctrinal, comparative and descriptive approaches without quantitatively analyzing the issue of professional preparedness. There wasn't much empirical research into the understanding of deep fake threats by Pakistani judges, advocates, prosecutors, investigators, cybercrime officers, and forensic experts (Asfandiyar v. Kamran, 2016). The previous studies also yielded only partial information on institutional capacity and forensic preparedness, authentication process and the state of the legal protection. Furthermore, the correlation between the assessment of evidence produced by AI and the perception of fair-trial rights was under explored. In order to fill this gap, the present study aimed to test four hypotheses with a structured quantitative model based on the perceptions of legal and forensic professionals in Pakistan.

Conceptual Framework

The conceptual framework comprised three independent variables: perceived deep fake threat, institutional and forensic readiness and legal-procedural safeguards. The likelihood of a deep fake was predicted to impact professional trust of the authenticity and admissibility of digital evidence. Better forensic institutions, tested technologies and professional expertise were expected to enhance the confidence in the evaluation of evidence, in contrast. Legal-procedural safeguards were also likely to have positive effects on participants' perceptions of the protection of fair-trial rights. Authenticity and admissibility confidence was used as an intermediate outcome and predictor, while perceived fair-trial protection was used as the final dependent variable (Horsman, 2021).

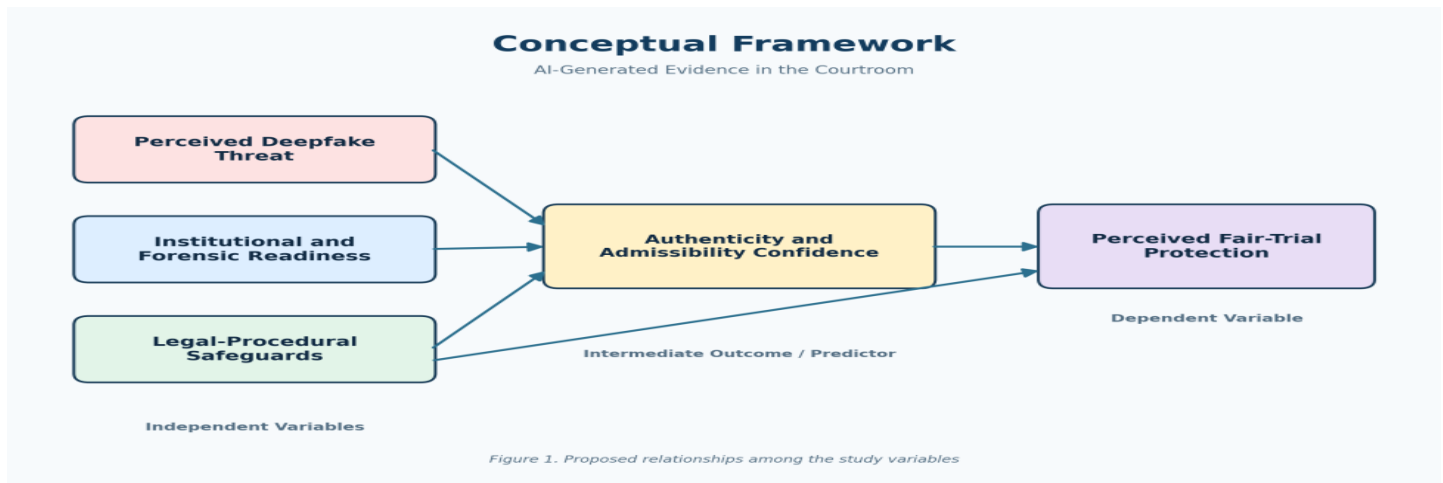


Figure 1

Research Methodology

The research methodology explained the systematic process undertaken to explore the legal and institutional issues surrounding AI-produced evidence for the courtroom. It presented the research philosophy, methodology, research design, population, sampling process, instrument, data collection process, and statistical analysis methods. The selected methodology enabled the researcher to convert the main theoretical concepts into measurable variables. It also offered a framework for examining the connection between the perceived threat of deep fakes, institutional preparedness, legal-procedural protections, evidentiary certainty, and fair-trial protections. As such, the methodology guaranteed a logical alignment of research goals, research questions, research hypotheses and statistical procedures (Javaid & Saleem, 2025).

Research Philosophy

The study was done with the positivist research philosophy as it focused on measurable relationships between clearly defined variables. Professional perceptions on threats from deep fakes, institutional preparedness, evidentiary protection and fair-trial protection were quantified using a structured questionnaire that could be used for a positivist approach. It was assumed that these constructs can be operationalized by observable statements and numerical answers. This philosophy also included the need to use objective statistical techniques to analyze patterns and test the proposed hypothesis. So, in the positivist view, it was suitable to have a basis for creating findings that were systematic, measurable, and could be empirically verified (Juefei-Xu et al., 2022).

Research Approach

The study was deductive research in which the hypotheses were formulated based on the legal arguments, theories and institutional recommendations that were identified in the literature. Four hypotheses were advanced to investigate the hypothesized relationships between the main research variables. To test for statistical support of these theoretically postulated relationships quantitative data were collected. The deductive method allowed the researcher to make a logical progression from general concepts and propositions to specific empirical tests. It thus helped to maintain a consistency in the literature review, conceptual framework, research questions, hypotheses and procedures for data analysis (Khan, 2018).

Research Design

This study employed a quantitative, cross-sectional, and explanatory survey design to examine professional perceptions of generated evidence using AI. The quantitative design enabled the variables to be measured numerically in terms of responses on a 5-point Likert scale. The cross-sectional element enabled data to be gathered from judges, advocates, prosecutors, investigators, cybercrime officers and forensic experts within a specific time frame. The explanatory component allowed the researcher to conclude the direction and intensity of the relationship among the Independent, Mediating and Dependent variables. This design proved to be suitable as it allowed descriptive analysis, hypothesis testing, comparison between professional groups, and statistical explanation of the proposed conceptual model (Khan, 2022).

Target Population

The target population consisted of professionals who were directly involved in the presentation, challenge, investigation, examination or evaluation of evidence in the justice system in Pakistan. It comprised judges and judicial officers, practicing advocates, public prosecutors, criminal investigators, cybercrime officers and digital-forensic experts (Khan, 2023). These professional groups were chosen because they had direct involvement with the admissibility and authentication of electronic and audiovisual evidence. The respondents had to have some experience in the relevant field of practice to be able to have some knowledge of a legal process, criminal investigation or forensic practice. This population allowed the study to gain insightful feedback on the threats from deep fakes, readiness of institutions, evidence protection, and protection of the right to a fair trial.

Sample Size

A sample of 300 respondents will be selected.

Category	Proposed sample
Judges and judicial officers	45
Advocates	105
Public prosecutors	45
Investigators and cybercrime officers	60
Digital-forensic experts	45
Total	300

Sampling Technique

For this study, use of proportionate stratified sampling was used when reliable lists of professionals exist. A representative sample of the population was taken by dividing it into professional strata. Specialized forensic experts and cybercrime officers were chosen using purposive sampling as they form a small and limited and hard-to-reach population.

Research Instrument

The two source papers along with the supporting legal materials, research objectives, research questions, research hypotheses and conceptual framework were used in developing a self-structured questionnaire. The instrument included demographic details about professional role, gender, age, qualification, experience, province, taking part in digital-evidence training, and experience with disputed or suspected AI-generated evidence, as well as access to forensic assistance (Khan, 2024a). The substantive part consisted of five constructs: perceived deep fake threat, institutional and forensic readiness, legal-procedural safeguards, authenticity and admissibility confidence, and perceived fair-trial protection (Khan, 2024b). The questionnaire consisted of statements about fabricated evidence, forensic expertise, validated tools, chain of custody, traceability of documents, independence of the examination, equality of arms, and judicial neutrality. The statements were rated on a 1-5 Likert scale where 1 indicates strongly disagree and 5 indicates strongly agree. With the use of this instrument, the researcher was able to gather standardized quantitative data and analyze the perceptions of professionals with AI-generated evidence and fair-trial protection from a statistical perspective.

Data-Collection Procedure

The researcher obtained ethical approval and necessary permissions. An information sheet was providing information about the purpose of the study, the voluntary nature of the study, confidentiality protections, and respondent rights. Questionnaires were sent by e-mail and in print, if applicable. Participants were asked not to share any information that could be considered confidential or identifiable information of the case. Completed questionnaires were reviewed for missing items, multiple completions, ineligible respondents, and time spent on the completion of the questionnaire.

Data-Analysis Techniques

Collected data were then coded, entered, screened and analyzed using SPSS and an appropriate program of structural equation modeling. Frequency, percentage, means, standard deviation and confidence intervals were computed to describe respondents' characteristics and perceptions of the variables in this study. The reliability and validity of the measurement model examined using

Cranach's alpha test, composite reliability test, average variance extracted test, confirmatory factor analysis test and test of discriminant validity. Pearson correlation and multiple regressions were used to investigate the nature, strength and predictive power of relationships between variables (Khan & Hussain Shah Jillani, 2019). Where appropriate, structural equation modeling and bootstrapped indirect-effect analysis were used to assess statistical significance at .05 level, as well as effect sizes and confidence intervals.

Data Analysis

Table 1: Demographic and Professional Characteristics of Respondents (N = 300)

Variable	Category	Frequency	Percentage
Professional role	Judges and judicial officers	45	15.0
	Practising advocates	105	35.0
	Public prosecutors	45	15.0
	Investigators and cybercrime officers	60	20.0
	Digital-forensic experts	45	15.0
Gender	Male	213	71.0
	Female	87	29.0
Age group	21-30 years	54	18.0
	31-40 years	111	37.0
	41-50 years	84	28.0
	Above 50 years	51	17.0
Highest qualification	Bachelor's degree	48	16.0
	Master's/LL.B. degree	144	48.0
	MPhil/LL.M. degree	78	26.0
	PhD/doctoral degree	30	10.0
Professional experience	1-5 years	72	24.0
	6-10 years	93	31.0
	11-15 years	69	23.0
	More than 15 years	66	22.0
Digital-evidence training	Yes	171	57.0
	No	129	43.0
Experience with disputed audiovisual evidence	Yes	186	62.0
	No	114	38.0
Experience with suspected AI-generated evidence	Yes	117	39.0
	No	183	61.0
Access to forensic assistance	Adequate access	99	33.0
	Limited access	132	44.0
	No access	69	23.0

The distribution of professionals by profession is presented in table 1 and indicated that practicing advocate was the largest group with 35.0% of the total sample. 71.0% of the respondents were male and 29.0% were female. The age group of 31-40 years accounted for the highest proportion and nearly half of the respondents had a Master's or LL.B. qualification. The majority of the respondents were professionals with six to 10 years or more of work experience. 57.0% had taken part in training on digital evidence

but only 39.0% had seen suspected AI-generated evidence. In addition, 67.0% said that they had limited or no access to forensic assistance, thus highlighting an important institutional capacity gap.

Table 2: Descriptive Analysis of Perceived Deep fake Threat

Indicator	N	Mean	SD
Deep fakes increase the risk of fabricated courtroom evidence	300	4.46	0.67
Deep fakes may contribute to wrongful judicial decisions	300	4.38	0.71
Deep fake allegations may create doubt about genuine recordings	300	4.29	0.76
Conventional authentication is insufficient for AI-susceptible evidence	300	4.15	0.81
Deep fakes reduce confidence in audiovisual evidence	300	4.21	0.74
Overall perceived deep fake threat	300	4.30	0.61

Table 2 shows that the average mean score of perceived deep fake threat is very high with an overall mean score of 4.30 and standard deviation of 0.61. The highest consensus was related to the possibility that deep fakes may be used as falsified evidence in court ($M = 4.46$). Respondents were also strongly convinced that deep fakes might be a cause of misjudgments in the judicial process. However, the mean for the adequacy of conventional authentication was relatively low (but high) indicating questions about the sufficiency of current procedures among professionals. Results indicated the broad concern with the impact synthetic media has on the reliability of the evidence.

Research Objective Two

Table 3: Descriptive Analysis of Institutional and Forensic Readiness

Indicator	N	Mean	SD
Qualified AI-forensic experts are sufficiently available	300	2.48	1.02
Forensic laboratories possess adequate detection tools	300	2.39	1.04
Legal professionals receive sufficient deep fake training	300	2.34	1.01
Suspected evidence can be examined without unnecessary delay	300	2.51	0.98
Forensic reports clearly explain methods and limitations	300	2.73	0.96
Overall institutional and forensic readiness	300	2.49	0.82

As can be seen in Table 3, the perception of institutional and forensic readiness was perceived as low with an overall mean of 2.49. The lowest mean was related to availability of professional training on deep fake evidence ($M = 2.34$), followed by the adequacy of forensic detection tools ($M = 2.39$). Confidence in reporting clarity for forensic reporting was moderate, with a mean of 2.73, giving a little higher level of confidence than for infrastructure and training. In general, participants felt the justice system was under-prepared to investigate complex AI-generated evidence.

Research Objective Three

Table 4: Descriptive Analysis of Legal-Procedural Safeguards

Indicator	N	Mean	SD
Original digital files and metadata should be preserved	300	4.51	0.61
Chain-of-custody procedures should be strictly documented	300	4.47	0.64
Opposing parties should receive access for independent examination	300	4.42	0.69
Courts should conduct authentication hearings for disputed evidence	300	4.36	0.72
Judicial decisions should explain the treatment of AI evidence	300	4.39	0.68
Overall legal-procedural safeguards	300	4.43	0.55

Table 4 shows that there is very strong support for the legal-procedural safeguards with the overall mean score being 4.43. The mean for preservation of original digital files and metadata was the highest at 4.51. The chain of custody and separate evaluation of

the opposing party were also rated very highly. The findings demonstrated that transparency in the authentication and disclosure of evidence, preservation, and judicial reasoning are all crucial for the realization of fair-trial rights when evidence involves AI.

Research Objective Four

Table 5: Descriptive Analysis of Evidentiary Confidence and Fair-Trial Protection

Indicator	N	Mean	SD
Courts can make reliable authenticity decisions when safeguards are followed	300	3.76	0.83
Forensic examination improves the accuracy of admissibility decisions	300	3.92	0.78
Independent expert challenge strengthens evidentiary confidence	300	4.08	0.73
Reliable authentication protects parties from prejudicial evidence	300	4.16	0.70
Transparent evidence evaluation strengthens fair-trial protection	300	4.19	0.68
Overall authenticity, admissibility and fair-trial confidence	300	4.02	0.62

The overall level of confidence in the contribution of reliable evidence evaluation to fair-trial protection is high ($M = 4.02$) (see Table 5). Both M and SD were highest for the statement that transparent evidence evaluation enhanced fair-trial rights ($M = 4.19$). The reliability of authentication was also seen as safeguarding litigants against prejudicial and fabricated evidence. While trust in courts' current capacity to make reliable authenticity decisions was relatively low, it was still high. The results indicated that with the appropriate forensic and procedural safety measures implemented, professional confidence could be enhanced.

Research Hypothesis Testing

Hypothesis One

Table 6: Regression Effect of Perceived Deep fake Threat on Authenticity and Admissibility Confidence

Predictor	B	SE	β	t	p	95% CI for B
Constant	5.041	0.174	—	28.97	<.001	[4.699, 5.383]
Perceived deep fake threat	-0.421	0.051	-0.432	-8.27	<.001	[-0.521, -0.321]
R	R²	Adjusted R²	F(1, 298)	p	Decision	
.432	.187	.184	68.39	<.001	H1 supported	

As indicated in Table 6, perceived deep fake threat negatively and significantly influenced confidence in authenticity and admissibility ($\beta = -.432$, $t = -8.27$, $p < .001$). Perceived threat was found to be significantly related to evidentiary confidence ($r = -0.421$) with a one-unit increase in perceived threat corresponding to a 0.421-unit decrease in evidentiary confidence. The model accounted for 18.7% of the variance in authenticity and admissibility confidence. The coefficient had a negative sign and the p value was less than .05, so H1 was accepted.

Hypothesis Two

Table 7: Regression Effect of Institutional and Forensic Readiness on Authenticity and Admissibility Confidence

Predictor	B	SE	β	t	p	95% CI for B
Constant	1.923	0.142	—	13.54	<.001	[1.644, 2.202]
Institutional and forensic readiness	0.514	0.047	.536	10.94	<.001	[0.422, 0.606]
R	R²	Adjusted R²	F(1, 298)	p	Decision	
.536	.287	.285	119.68	<.001	H2 supported	

According to Table 7, the Institutional and Forensic readiness significantly and positively influenced the Authenticity and Admissibility confidence ($\beta = .536$, $t = 10.94$, $p < .001$). For each unit increase in institutional readiness, there was a 0.514 unit increase in evidentiary confidence. The variance in confidence could be accounted for by institutional and forensic readiness accounting for 28.7%. Hence, the access to professionals, validated tools, labs, training and timely examination greatly enhanced professionals' confidence, and H2 was supported.

Hypothesis Three

Table 8: Regression Effect of Legal-Procedural Safeguards on Perceived Fair-Trial Protection

Predictor	B	SE	β	t	p	95% CI for B
Constant	1.126	0.198	—	5.69	<.001	[0.736, 1.516]
Legal-procedural safeguards	0.681	0.044	.668	15.48	<.001	[0.594, 0.768]
R	R²	Adjusted R²	F(1, 298)	p	Decision	
.668	.446	.444	239.63	<.001	H3 supported	

Table 8 shows that legal-procedural safeguards were positively correlated with perceived fair-trial protection and statistically significant ($\beta = .668$, $t = 15.48$, $p < .001$). Each increase of one unit in safeguards yielded an increase of 0.681 units in perceived fair-trial protection. The model accounted for 44.6% of the variance in the dependent variable, a substantial amount of variance. For this reason, H3 was supported.

Hypothesis Four

Table 9 Regression Effect of Authenticity and Admissibility Confidence on Perceived Fair-Trial Protection

Predictor	B	SE	β	t	p	95% CI for B
Constant	1.307	0.168	—	7.78	<.001	[0.976, 1.638]
Authenticity and admissibility confidence	0.647	0.043	.655	14.96	<.001	[0.562, 0.732]
R	R²	Adjusted R²	F(1, 298)	p	Decision	
.655	.429	.427	223.80	<.001	H4 supported	

As revealed in table 9, statistically significant positive effects were found for authenticity and admissibility confidence on perceived fair-trial protection ($\beta = .655$, $t = 14.96$, $p < .001$). Evidentiary confidence was significantly associated with a 0.647-unit increase in perceived protection of fair-trial rights, per one-unit increase in evidentiary confidence. The predictor explained 42.9% of the variation in fair-trial protection. Therefore, there was a significant increase in the level of trust in the ability to assess evidence reliably and transparently, strengthening the perception of procedural fairness, and thus supporting H4.

Discussion

The results showed that AI-generated deep fakes pose a significant threat to the validity and acceptance of digital evidence in Pakistan's judicial system. The perceived threat of a deep fake was very high, with most respondents indicating that faked evidence in court, incorrect rulings by judges, and falsely denying the authenticity of real recordings were most prevalent (Khan & Ullah, 2024). The significant negative effect of perceived deep fake threat on evidentiary confidence supported H1. This discovery suggested that awareness of the synthetic-media capabilities had eroded professionals' confidence in traditional forms of digital-evidence authentication (Mathlouthi et al., 2025). The outcome was in line with the concerns of Chesney and Citron (2019) who suggested that deep fakes may be used to "challenge the reliability of audiovisual evidence and open the door for fabrication and denials". It also backed the stance of Muhammad (2025) who claimed that the courts could not anymore draw their primary focus on the "realistic" nature of digital recordings (Khan & Ximei, 2022).

The results showed that AI-generated deep fakes pose a significant threat to the validity and acceptance of digital evidence in Pakistan's judicial system (Khan & Wu, 2020). The perceived threat of a deep fake was very high, with most respondents indicating that faked evidence in court, incorrect rulings by judges, and falsely denying the authenticity of real recordings were most prevalent. The significant negative effect of perceived deep fake threat on evidentiary confidence supported H1 (Lederer, 2019). This discovery suggested that awareness of the synthetic-media capabilities had eroded professionals' confidence in traditional forms of digital-evidence authentication. The outcome was in line with the concerns of Chesney and Citron (2019) who suggested that deep fakes may be used to "challenge the reliability of audiovisual evidence and open the door for fabrication and denials". It also backed the stance of Muhammad (2025) who claimed that the courts could not anymore draw their primary focus on the "realistic" nature of digital recordings.

The respondents were quite strong with regards to legal-procedural safeguards. Original files and metadata retention, chain of custody documentation, independent examination, authentication hearings and judicial decisions based on reasoning were deemed essential. The strongest effect was found for legal-procedural safeguards in support of H3 (Naveed Asghar v. State, 2021) which is related to perceived fair-trial protection. This revealed that the fairness of related evidence by AI was not solely based on technical detection (Pakistan Penal Code, 1860, § 292). Even if a forensic conclusion is technically valid, it can prejudice the justice if the other party is not given access to the original file, back tracking, validation or an independent expert. This was thus in line with the theory of procedural justice that focuses on transparency, neutrality, participation and meaningful opportunities to challenge adverse evidence (Khan & Wu, 2021b).

Perceived fair-trial protection was also positively influenced by authenticity and admissibility confidence, which was in line with H4. Those who responded thought that an impartial and honest assessment of digital evidence would shield litigants from the submission of fake, misleading, or unfair evidence (Cyberspace Administration of China, 2022). This connection was evident in this relationship where evidentiary reliability and procedural fairness were both closely linked (Shi, 2025). Without reliable ways to differentiate between a true recording and manipulated content, courts would not be able to ensure fair-trial rights. Meanwhile, confidence had to be kept in check because there was no magic bullet or definitive decision that was completely unbiased (Constitution of Pakistan, 1973, art. 10A). The results generally supported all four hypotheses and the proposed conceptual framework. The threat of technology decreased the level of confidence in the evidence, while the readiness of institutions increased. Legal-procedural measures were directly strengthened to foster fair trial protection, while the evidentiary confidence had a positive effect on perceptions of judicial fairness. The findings indicated that Pakistan needed a multi-faceted approach that included legal reform, forensic infrastructure, professional training, evidence-preserving protocols, independent examination, and clear judicial reasoning among other things (Khan & Wu, 2021a).

Conclusion

The study aimed to explore the impact of deep fakes created by AI on the authenticity and admission of digital evidence and the fair trial rights safeguarding in Pakistan. Its emphasis was on the perceptions of judges, judicial officers, practicing advocates, public prosecutors, investigators, cybercrime officers, and digital-forensic experts. This investigation incorporated four research questions and hypotheses on perceived deep fake threat, institutional and forensic preparedness, legal-procedural safeguards, authenticity and admissibility confidence and fair-trial protection. The results of the quantitative analysis confirmed all four of the proposed relationships in the conceptual framework.

The results confirmed that the legal and forensic community viewed deep fakes as a serious problem in the process of determining the facts in court. AI technologies might produce highly convincing images, videos, and audio recordings that could produce faux admissions or communications, or even impersonate individuals or fabricate events. Deep fakes also could generate such a liar's dividend, whereby people who are challenged to authentic recordings would only have to claim that they have been manipulated. The marked negative impact of perceived deep fake threat indicated that the more aware of these threats, the less trust was placed in the reliability of audiovisual evidence. The concept of visual realism could no longer be deemed adequate as evidence of fact.

The study also recommended that Pakistan urgently needed to strengthen its institutional and forensic capacity. The respondents indicated that existing professional training was lacking, there was a lack of access to qualified AI-forensic experts, the laboratory capacity was inadequate, and there was a lack of validated detection tools. There was a positive effect on evidentiary confidence, however, due to institutional readiness. This illustrated how courts can benefit from the use of forensic infrastructure, professional expertise, timely examination, quality assurance and reporting to better assess AI susceptible evidence.

Legal-procedural safeguards proved to be the most significant factor in predicting participants' perceived fair-trial protection. Reliable authentication required proper preservation of original file, metadata, cryptographic hashes, source-device information, and chain-of-custody records. Equally important was disclosure, the independent forensic examination, an expert challenge, an authentication hearing and a reasoned decision by the judge. There might be a situation that justice could not be served if one side did not have the opportunity and resources to understand and contest the evidence.

As the admissibility confidence and fair-trial protection were positively correlated with authenticity, it was concluded that evidentiary accuracy was at the heart of procedural justice. Without reliable procedures for determining the authenticity, relevance, and admissibility of digital evidence, courts would be unable to protect accused persons, complainants, victims, and litigants. Courts, however, should not accept evidence based on an audiovisual representation merely because it seemed realistic, nor should they discredit it because they know it could be manipulated in that way. Finally, a well-balanced system of calibrated verification was

needed for deep fakes. Pakistan's requirements were an integrated approach to legal and institutional aspects which included AI-specific evidentiary guidance, qualified experts, accredited laboratories, transparent forensic methods, professional training, equality of arms, and judicial oversight. This would provide a framework for the preservation of the legitimate value of real digital evidence without the danger of false evidence, public mistrust of the administration of justice, wrongful conviction, burden on a defendant, and exclusion of evidence.

Recommendations

Development of AI-Specific Evidentiary Guidelines

The high courts should establish consistent rules for authentication and admissibility of AI-generated and/or AI-manipulated evidence. These guidelines need to include the evidence-based groundings for pictures, videos, audio recordings, and other synthetic media. They should cover original file preservation, metadata, provenance, cryptographic hashing, and chain of custody, disclosure and expert examination. In a serious criminal or civil case, where disputed electronic evidence is a key issue, courts should exercise greater standards of proof to determine whether that evidence is authentic. A uniform set of guidelines would alleviate inconsistent rulings and promote the confidence of professionals in how the judicial system deals with evidence that can be influenced by AI.

Strengthening Institutional and Forensic Capacity

The government needs to set up or designate digital-forensic labs that can analyze sophisticated AI-generated content. Such laboratories are required to have qualified experts, and should be equipped with validated tools with documented testing, quality-control procedures and regular technological updates. Courts, prosecutors, investigators, defense counsel and litigants should have access to examination facilities which are made reasonably accessible throughout Pakistan. The methodology used, results found, limitations, and degree of certainty should be clearly explained in a forensic report. Increased institutional capacity would help to reduce examination delay and increase accuracy of authenticity and admissibility decisions.

Professional Training and AI Literacy

There should be ongoing training at judicial academies, bar councils, prosecution agencies, police academies and cybercrime agencies concerning evidence created by artificial intelligence. Training should include an overview of deep fakes, metadata, and provenance, chain of custody, cryptographic verification, and limitations of detection, expert evidence and the liar's dividend. Judges and lawyers were not expected to be computer scientists, but they did have to be literate enough to ask relevant questions and assess technical arguments. Forensic professionals must also be trained on how to present complicated information in a way that is clear and comprehensible to the legal system. Increased collaboration between legal practitioners, investigators, technologists and forensic institutions can be improved through regular interdisciplinary workshops.

Protection of Equality of Arms

Both sides to have meaningful chance to examine comprehend and question evidence that is subject to AI. The prosecution or evidence proponent shall produce the original file, forensic copies, metadata, acquisition records, software outputs and relevant expert method. If digital evidence is pivotal in the proceedings then financially disadvantaged litigants and accused persons should be afforded independent forensic support. These measures would help ensure that the outcome of evidence isn't determined by resource inequity and build the sense of, and actual, protection of fair-trial rights.

Legislative Reform and Future Research

It is essential to review the Qanun-e-Shahadat Order, PECA and related procedural laws to take into account malicious synthetic impersonation, fabrication of evidence, voice cloning, and AI-generated audiovisual material. Legislative improvements ought to clarify essential concepts and be sufficiently flexible and neutral on technological points to accommodate future growth. The law must differentiate harmful deception from legitimate satire, parody, artistic creation or research and clearly disclosed synthetic content. Future studies could focus on real cases, performance in court, regional variations, perceptions of victim and accused persons, and professionals' perceptions. Future research using qualitative, longitudinal, experimental and mixed methods would substantiate and expand on the current quantitative results.

References

1. Abdelrehim Hammad, A. A., Khan, A., & Soomro, N. E. (2021). Digital economy barriers to trade regulation: Status, challenges, and China's response. *International Journal of Social Sciences Perspectives*, 8(2), 41–49.
2. Ahmed, S., & Chishti, M. A. (2022). Electronic evidence under Pakistani jurisprudence: A critical analysis of Article 164 of the Qanun-e-Shahadat Order 1984. *Pakistan Law Review*, 13(2), 45–68.
3. *Amar Yasir Ali v. State*, 2013 PCrLJ 783 (Pak.).
4. Apolo, Y., & Michael, K. (2024). Beyond a reasonable doubt? Audiovisual evidence, AI manipulation, deep fakes, and the law. *IEEE Transactions on Technology and Society*, 5(2), 156–168.
5. *Asfandiyar v. Kamran*, 2016 SCMR 2084 (Pak.).
6. Bernacka, A. (2025). Deep fake technology: Legal problems in the light of the EU AI Act. In L. Cornacchia and L. Scollo (Eds.), *Artificial intelligence and criminal law: International perspectives*. Springer.
7. *Bridges v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058.
8. *Bykov v. Russia*, App. No. 4378/02, European Court of Human Rights (Mar. 10, 2009).
9. Casey, E. (2020). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (4th ed.). Academic Press.
10. Chesney, R., & Citron, D. K. (2019). 21st century-style truth decay: Deep fakes and the challenge for privacy, free expression, and national security. *Maryland Law Review*, 78(4), 882–891.
11. Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820.
12. China Briefing. (2022, December 20). *China to regulate deep synthesis (deep fake) technology starting in 2023*.
13. *Code of Criminal Procedure*, 1898 (Act No. V of 1898) (Pak.).
14. *Constitution of the Islamic Republic of Pakistan*, art. 10A (1973).
15. Cornacchia, L., & Scollo, L. (Eds.). (2025). *Artificial intelligence and criminal law: International perspectives*. Springer.
16. Council of Europe. (1950). *Convention for the Protection of Human Rights and Fundamental Freedoms*, art. 6.
17. Council of Europe. (2001). *Convention on Cybercrime*, European Treaty Series No. 185.
18. Council of Europe. (n.d.). *Cybercrime Judicial Monitor* (Issue 10).
19. Cyberspace Administration of China. (2022). *Provisions on the administration of deep synthesis of Internet information services*.
20. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
21. Dawn. (2024). *National Forensic Agency Bill passed*.
22. Deloitte. (2024). *Digital fraud report 2024*.
23. Economist & Jurist. (2025). *Deep fakes en los juzgados: Cuando la prueba miente mejor que tú*.
24. *Electronic Transactions Ordinance*, 2002 (Ordinance No. LI of 2002) (Pak.).
25. Eurojust. (n.d.). *Use of AI systems for criminal purposes and in the administration of justice*.
26. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union*.
27. Eurostat. (2024). *Digital fraud in the European Union: Statistics and trends*.
28. Ferguson, A. G. (2018). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.
29. Furizal, Ma'arif, A., Maghfiroh, H., Suwarno, I., Prayogi, D., Kariyamin, Lonang, S., & Sharkawy, A.-N. (2025). Social, legal, and ethical implications of AI-generated deep fake pornography on digital platforms: A systematic literature review. *Social Sciences & Humanities Open*, 12, Article 101882. <https://doi.org/10.1016/j.ssaho.2025.101882>
30. *Gäffgen v. Germany*, App. No. 22978/05, European Court of Human Rights (June 1, 2010).
31. Ghani, H. U., Gong, X., Haider, A., & Khan, A. (2025). The Indian concern regarding the China–Pakistan Economic Corridor and its justification from the perspective of international law. *China and WTO Review*, 11(2), 25–39.
32. Ghiurău, D., & Popescu, D. E. (2025). Distinguishing reality from AI: Approaches for detecting synthetic content. *Computers*, 14(1), Article 1.
33. Giangiacomo, A. (2025). *Mandatory discovery, algorithmic expert and free evaluation of evidence*. Publisher information is missing.
34. Government of India. (2000). *Information Technology Act, 2000* (Act No. 21 of 2000).

35. Gregory, S. (2024). *From social media to deep fakes : Participatory human rights witnessing and advocacy using audiovisual media, incorporating the emerging impacts of deceptive AI and technologies for authenticity and trust (2007–2022)* [Doctoral dissertation, University of Westminster].
36. Gupta, D., & Fatunmbi, T. O. (2024). Generative AI and deep fakes : Ethical implications and detection techniques. *Journal of Science, Technology and Engineering Research*, 2(1), 45–56.
37. Hameed, U., et al. (2026). CCTV evidence and the law: The emergence of the silent-witness doctrine in *State v. Zahir Jaffer*. Volume, issue, pages, and complete authorship are missing.
38. Hausknecht, A. (2025). The impact of deep fakes on trust in user-generated evidence. In *Deep fakes and the law: Challenges, responses, and critique*. Routledge.
39. Horsman, G. (2021). Explainable artificial intelligence in digital forensics. *Forensic Science International: Digital Investigation*, 38, Article 301245.
40. Hui, Z., Haider, A., & Khan, A. (2025). International trade and plastic waste in oceans: Legal and policy challenges. *Frontiers in Marine Science*, 12, Article 1627829.
41. Huston, R. P., & Bahm, M. E. *Deep fakes 2.0: The new era of “truth decay.”* Publication year and source are missing.
42. INCIBE. (2025). *Cybersecurity incident report 2024*.
43. International Bar Association. (2025). *Deep fakes : Can the AI Act protect Europe?*
44. *Ishtiaq Ahmed Mirza v. Federation of Pakistan*, PLD 2019 SC 675 (Pak.).
45. Javaid, B., & Saleem, S. (2025). Admissibility of artificial intelligence-based evidence in Pakistan: Legal standards and judicial responses. *UCP Journal of Law and Legal Education*, 3(3).
46. Juefei-Xu, F., Wang, R., Huang, Y., Guo, Q., Ma, L., & Liu, Y. (2022). Countering malicious Deep fakes : Survey, battleground, and horizon. *International Journal of Computer Vision*, 130(7), 1678–1734. <https://doi.org/10.1007/s11263-022-01606-8>
47. *Kashif Anwar v. Aga Khan University*, 2013 YLR 2294 (Pak.).
48. Khan, A. (2018). *Autonomous weapons and their compliance with international humanitarian law* [Master’s thesis].
49. Khan, A. (2022). E-commerce regulations in the emerging era: The role of the WTO in resolving the complexities of electronic trade. *ASR: Chiang Mai University Journal of Social Sciences and Humanities*.
50. Khan, A. (2023). *Rules on digital trade in the light of WTO agreements* [Doctoral dissertation, Zhengzhou University].
51. Khan, A. (2024). The emergence of the Fourth Industrial Revolution and its impact on international trade. *ASR: Chiang Mai University Journal of Social Sciences and Humanities*, 11.
52. Khan, A. (2024). The intersection of artificial intelligence and international trade laws: Challenges and opportunities. *IIUM Law Journal*, 32, 103–[page range unavailable].
53. Khan, A., & Hussain Shah Jilani, M. A. (2019). Killer robots and their compliance with the principles of the law of war. *Journal of Law & Society*, 50, 55–[page range unavailable].
54. Khan, A., & Jiliani, M. A. H. S. (2023). Expanding the boundaries of jurisprudence in the era of technological advancements. *IIUM Law Journal*, 31, 393–[page range unavailable].
55. Khan, A., & Ullah, M. (2024). The Pakistan–China FTA: Legal challenges and solutions for marine environmental protection. *Frontiers in Marine Science*, 11, Article 1478669. <https://doi.org/10.3389/fmars.2024.1478669>
56. Khan, A., & Usman, M. (2023). The effectiveness of international law: A comparative analysis. *International Journal of Contemporary Issues in Social Sciences*, 2(3), 780–786.
57. Khan, A., & Wu, X. (2020). The impact of the digital economy on intellectual property law. *Journal of Politics and Law*, 13, 117–[page range unavailable].
58. Khan, A., & Wu, X. (2021a). Bridging the digital divide in the digital economy with reference to intellectual property. *Journal of Law and Political Sciences*, 28(3), 256–263.
59. Khan, A., & Wu, X. (2021b). Reforms for the culmination of the deadlock in the appellate body of the WTO: An agenda for saving the multilateral trading system. *Journal of Humanities, Social and Management Sciences*, 2(1), 50–62.
60. Khan, A., & Ximei, W. (2022). Digital economy and environmental sustainability: Do information and communication technology and economic complexity matter? *International Journal of Environmental Research and Public Health*, 19(19), Article 12301. <https://doi.org/10.3390/ijerph191912301>
61. Khan, A., Abd Elrhim, A. A., & Soomro, N. E. (2021). China’s perspective on reforming the World Trade Organization. *Journal of Politics and Law*, 14, 104–[page range unavailable].
62. Khan, A., Amjad, S., & Usman, M. (2020). The role of customary international law in contemporary international relations. *International Review of Social Sciences*, 8(8), 259–265.

63. Khan, A., Jillani, M. A. H. S., Abdelrehim Hammad, A. A., & Soomro, N. E. H. (2021). Plurilateral negotiation of WTO e-commerce in the context of the digital economy: Recent issues and developments. *Journal of Law and Political Sciences*.
64. Khan, A., Jillani, M. A. H. S., Ullah, M., & Khan, M. (2025). Regulatory strategies for combatting money laundering in the era of digital trade. *Journal of Money Laundering Control*, 28(2), 408–423.
65. Khan, A., Khan, A. S., & Khan, I. (2022). Responsibility of killer robots for causing civilian harm: A critique of AI application in warfare doctrine. *Pakistan Journal of International Affairs*, 5(1), 15–33.
66. Khan, A., Usman, M., & Amjad, S. (2020). Enforcing economic, social, and cultural rights: A global imperative. *International Review of Social Sciences*, 8(9).
67. Khan, A., Usman, M., & Amjad, S. (2023). The digital-age legal revolution: TAPED's trailblazing influence. *International Journal of Contemporary Issues in Social Sciences*, 2(4), 524–535.
68. Lederer, F. I. (2019). The regulatory and evidentiary implications of artificial intelligence in the courtroom. *Syracuse Law Review*, 68(2), 317–348.
69. Lin, L. S. (2025). Organisational challenges in U.S. law enforcement's response to AI-driven cybercrime and deep fake fraud. *Laws*, 14(4), Article 46.
70. Liu, X., Khan, M., & Khan, A. (2023). Review of *The law and practice of global ICT standardization*, by O. Kanevskaia. *International & Comparative Law Quarterly*, 72(4), 1094–1097.
71. Llorente, R. V. (2024). Deep fakes in the dock: Preparing international justice for generative AI. *SciTech Lawyer*, 20(2), 28–33.
72. Makhambetsaliyev, D. (2025). *Deep fakes and the legal construction of identity: Between personhood and performance*. The work was described as unpublished.
73. *Maqsood Alam v. State*, 2024 SCMR 156 (Pak.).
74. Mathlouthi, N., Haider, A., Khan, A., & Ahmad, N. (2025). The role of Hainan Free Trade Port in shaping China's WTO commitments and international trade policies. *China and WTO Review*, 11(1), 71–82.
75. Mkpo, D. C. (2025). Is truth and integrity of justice on trial in the age of artificial intelligence? Reassessing digital evidence in the context of AI-generated evidence such as deep fakes. *International Review of Law and Jurisprudence*, 7(1).
76. *Muhammad Ammar Shafi and Others v. State*, 2025 YLR 1681 (Pak.).
77. *Munas Parveen v. Additional Sessions Judge*, PLD 2015 231 (Pak.).
78. Munjić, M. (2025). *Encrypted-platform evidence and the right to challenge it: From formal guarantee to structural contestability*. Publication source is missing.
79. Murray, M. D. (2025). Visual legal rhetoric in the age of generative AI and deep fakes : Renaissance or dark ages? *SMU Science and Technology Law Review*, 28, 199–[page range unavailable].
80. National Judicial Academy. (2025). *Research on AI evidence training*. A retrievable publication record is required.
81. *Naveed Asghar v. State*, PLD 2021 SC 600 (Pak.).
82. *Pakistan Penal Code, 1860* (Act No. XLV of 1860), § 292 (Pak.).
83. *Pakistan Telecommunication (Re-organization) Act, 1996* (Act No. XVII of 1996) (Pak.).
84. Paris, B. (2021). Configuring fakes: Digitized bodies, the politics of evidence, and agency. *Social Media + Society*, 7(4), Article 20563051211062919. <https://doi.org/10.1177/20563051211062919>
85. PASTIC. (2025). *Judicial activism in Pakistan: The impact of modern devices on evidence*. Publication details are missing.
86. *Payment Systems and Electronic Fund Transfers Act, 2007* (Act No. IV of 2007) (Pak.).
87. *Prevention of Electronic Crimes Act, 2016* (Act No. XL of 2016) (Pak.).
88. PTV News. (2026). *Azma Bukhari's fake viral video case hearing*. The exact date and URL are required.
89. *Qanun-e-Shahadat Order, 1984* (President's Order No. X of 1984), arts. 59, 73–78, 164 (Pak.).
90. Qin, H., & Chen, L. (2025). Virtual justice, or justice virtually: Navigating the challenges in China's adoption of virtual criminal justice. *Computer Law & Security Review*, 56, Article 106112. <https://doi.org/10.1016/j.clsr.2025.106112>
91. Roth, A. (2017). Machine testimony. *Yale Law Journal*, 126(7), 1972–2053.
92. *Salman Ahmad Khan v. Judge Family Court*, PLD 2017 698 (Pak.).
93. Seth, K. (n.d.). *Combating deep fakes and cybercrime* [Video]. YouTube. <http://www.youtube.com/watch?v=LQStYoHDzI>
94. *Shafqat Masih v. State*, 2021 MLD 1415 (Pak.).
95. Shaikh, S. A. (2026). AI, deep fakes and the emerging challenges to justice systems: A global and Pakistani legal perspective. *Pakistan Legal Decisions*. Volume, issue, and page numbers are required.
96. Shi, Y. (2025). The crisis of deep fakes in generation and detection: Are current responses sufficient? *iSChannel*, 19(1).

97. Shirish, A., & Komal, S. (2023). A socio-legal inquiry on deep fakes . *California Western International Law Journal*, 54, 517–[page range unavailable].
98. Singh, S., & Dhumane, A. (2025). Unmasking digital deceptions: An integrative review of deep fake detection, multimedia forensics, and cybersecurity challenges. *MethodsX*, 15, Article 103632. <https://doi.org/10.1016/j.mex.2025.103632>
99. *State v. Ahmed Omar Sheikh*, 2021 SCMR 873 (Pak.).
100. *State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).
101. *Sughra Bibi v. State*, PLD 2018 SC 595 (Pak.).
102. Superior Court of California. (2023). *Deep fake sanctions decision*. The case name, court division, docket number, and decision date are required.
103. The Friday Times. (2026, February 20). *Deep fake dilemma: Is Pakistan's justice system ready for synthetic media?* <https://www.thefridaytimes.com>
104. The proposed Indian *Digital India Act* should not be cited as enacted legislation until an official bill or enacted text is available.
105. United Kingdom. (2023). *Online Safety Act 2023*, c. 50.
106. United Nations Development Programme. (2024). *Transforming digital spaces in Pakistan: Policy, legal reforms, and advocacy to combat technology-facilitated gender violence*.
107. United Nations Office on Drugs and Crime. (2024). *Digital evidence in Pakistan: Legal framework and gaps*. A verifiable report title or URL is required.
108. United Nations. (1966). *International Covenant on Civil and Political Rights*, art. 14.
109. *United States v. Thomas*, 877 F.3d 591 (6th Cir. 2017).
110. Williams, B. (2025a). *AI and the future of digital evidence in law and journalism*. Publication source is missing.
111. Williams, B. (2025b). *Regulatory approaches to AI-generated content and privacy protection*. Publication source is missing.



2026 by the authors; Journal of Global Social Transformation (JGST). This is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (<http://creativecommons.org/licenses/by/4.0/>).