West Science Interdisciplinary Studies
Vol. 4, No. 11, November 2026: pp. 1680-1688

Deepfake Evidence Disruption: Reconstructing Proof in Indonesian Criminal Law and *Fiqh Jinayah*

Ahmad Husairi[1], Mawaddah Warohmah[2], Sapuan Ansori[3], Maryani[4], Samin Batubara[5]
[1] Faculty of Sharia, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia and ahmadhusairi1803@gmail.com
[2] Faculty of Sharia, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia and mawaddahwarohmah882@gmail.com
[3] Faculty of Sharia, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia and sapuanansori@gmail.com
[4] Faculty of Sharia, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia and maryani@uinjambi.ac.id
[5] Faculty of Sharia, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesi and saminbatubara@uinjambi.ac.id

ABSTRACT

Deepfakes challenge criminal adjudication because audiovisual recordings, long treated as persuasive proof, can now be fabricated cheaply and convincingly. Indonesia's new Code of Criminal Procedure (Law No. 20 of 2025), in force since 2 January 2026, recognises electronic evidence as a means of proof, yet recent scholarship indicates that a coherent governance model for digital proof is still missing. *Fiqh jinayah* studies usually treat digital evidence as qarinah without separating the authentication of content from the attribution of conduct. This normative legal study applies statutory, conceptual, and functional comparative approaches to legislation. It finds that Indonesian procedural law supplies admission and authenticity hooks but no method for assessing synthetic media, while *fiqh jinayah* offers a graded and cautious toolkit: *qarinah*, bayyinah, iqrar, and shahadah. The article proposes a five-layer analytical framework as a prescriptive recommendation, not as existing law. It concludes that authenticity of content must not be conflated with proof of who made or spread it, and that technical uncertainty should operate in the accused's favour.

Keywords: *Deepfake, Electronic Evidence, Fiqh Jinayah, 2025 Criminal Procedure Code, Qarinah*

1. INTRODUCTION

Audio and video recordings were long regarded as evidence that "speaks for itself." That assumption collapsed when machine learning allowed anyone to graft a person's face and voice onto events that never happened. Technical surveys show that the techniques for creating and detecting deepfakes continue to develop [1], [2], and that the contest between creators and detectors has not reached an end point [3], [4]. A systematic review of studies from 2021–2022 found that deepfakes threaten criminal justice mainly through the erosion of trust in institutions and the falsification of evidence [5]. Fallis describes this threat as epistemic: once video can be forged, the value of a recording as a source of knowledge is eroded [6]. The danger is twofold. Fabricated content may be offered as valid evidence, and genuine evidence may be attacked with the plea that "it is a deepfake."

Judicial experience elsewhere shows that existing evidentiary tools have not yet answered this threat. Braga da Silva observes that the chambers of the International Criminal Court assess digital evidence with methods designed for physical documents, so the authenticity problems peculiar to digital evidence go untouched [7]. Perez shows that the European Union has not set minimum reliability standards for electronic evidence, while deepfakes add new concern for the right to a fair trial [8].

Indonesia entered a new era on 2 January 2026, when the National Criminal Code (Law No. 1 of 2023), the new Code of Criminal Procedure or KUHAP (Law No. 20 of 2025), and the criminal-

law adjustment statute (Law No. 1 of 2026) took effect [9]. Article 235(1) of the new KUHAP lists electronic evidence as a means of proof, and Article 242 explains its scope. Yet recognition as a means of proof is only a gateway. Samudra, Basu, and Saenz Perez argue that the new KUHAP has not created a coherent legal framework for electronic evidence: its collection, authentication, handling, preservation, and evaluation are inadequately regulated, leaving no principled governance model for digital proof [10]. Saputra et al. had earlier concluded that the KUHAP lags behind technological developments in electronic trials [11]. In deepfake cases this vacuum is acute, because a judge must establish the authenticity of the video, the reliability of the detection tool, and the connection between the accused and the content all at once.

The substantive provisions that can reach deepfakes are scattered. Article 35 of the Electronic Information and Transactions Law (EIT Law) prohibits manipulating, creating, altering, deleting, or damaging electronic information so that it appears to be authentic data, with the penalty set in Article 51(1) [12, Arts. 35, 51(1)]. Recent Indonesian scholarship has concentrated on the offence side. Oktaviani et al. find that the Criminal Code, the EIT Law, and the Personal Data Protection Law cover deepfakes only in part because they were not designed for synthetic media [13], while Suseno et al. map the regulation of cybercrime in the new Criminal Code and note that the use of artificial intelligence aggravates cybercrime [14]. Other work addresses artificial intelligence in judicial proceedings generally [15]. This article asks a different question from the drafting of offences, namely how those offences are *proved*.

In the *fiqh jinayah* tradition, digital evidence is usually discussed through the concept of qarinah. Dayanti and Zulkarnain conclude that audio recordings can be accepted as qarinah or bayyinah, especially in ta'zir cases, provided they meet authenticity requirements [16]. Wan Ismail et al. position digital documents as evidence that reinforces other proof [17]. Abikan rejects CCTV and DNA tests as a basis for the *hadd* punishment for zina because they displace the requirement of four witnesses or a confession, but accepts them in non-hudud cases [18]. Studies of Malaysian Shariah courts examine the application of chain-of-custody principles to electronic documents in Shariah criminal cases [19] and the legal framework for admitting electronic documents [20]. Jibril, Bello, and Abubakar treat AI-generated evidence as secondary evidence that cannot replace traditional proof [21]. Only Maulana and Abbas address deepfakes directly, and they do so on the classification of the offence (qadzaf), not on how it is proved [22].

On the basis of the author's search conducted in October 2026, this literature does not appear to do three things at once. First, it does not separate the question of content authenticity from the question of attribution of conduct and fault. Second, it does not read the comparison against the new KUHAP, including the fact that the list of evidence in Article 235(1) no longer names "indications" (*petunjuk*) as a separate type [9]. Third, it does not derive from the comparison a testable benchmark for assessment. The contribution of this article is conceptual and limited: a five-layer analytical framework synthesised from legal materials and literature, not a claim of absolute novelty.

This study answers three questions: (1) how Indonesian positive criminal law regulates the authentication, reliability, and assessment of digital evidence in cases involving deepfakes; (2) how the *fiqh jinayah* concepts of proof, especially *qarinah, bayyinah, iqrar*, and *shahadah*, can be used to evaluate digital evidence manipulated by AI; and (3) how a standard for evaluating digital evidence can be reconstructed by comparing the two while still safeguarding reliability, the rights of the accused, and procedural justice. Its purpose is to map doctrinal gaps and to formulate proportionate recommendations.

2. METHODS

This is normative (doctrinal) legal research with a prescriptive character. The method was chosen because the problem concerns the adequacy of evidentiary norms and concepts, not the behaviour of actors in the field. The study conducted no interviews, experiments, testing of detection tools, or statistical analysis. The approaches used are statutory, conceptual, and comparative law. The primary legal materials comprise Law No. 20 of 2025 on the Criminal Procedure Code [23], Law No. 1 of 2023 on the Criminal Code [24], and Law No. 1 of 2024 on the second amendment to the EIT Law [12].

The analysis applies grammatical and systematic interpretation of the norms, followed by functional comparison. Functional comparison does not set articles of law directly beside fiqh concepts; it first identifies the functions being compared: admission of evidence, authentication, assessment of reliability, identification of the perpetrator, and determination of guilt. The two systems differ in their sources of legitimacy and institutional contexts, so functional equivalence is limited and does not mean identity of concepts. *Fiqh jinayah* concepts are read through contemporary literature rather than directly from classical texts, so conclusions about *fiqh* are conceptual. The final stage is prescriptive analysis, which separates sharply between existing law and recommendations for reform.

3. RESULTS AND DISCUSSION

3.1 Deepfakes and the Transformation of Audiovisual Evidence in Criminal Cases

Not every use of deepfakes is criminal, and that distinction determines what must be proved. Criminal elements arise when content is used for, among other things, pornography, fraud, and information manipulation [5]. Flynn et al. show that sexually explicit deepfake images are used as a form of image-based sexual abuse, including to threaten victims, and identify challenges for law enforcement [25]. Kirchengast discusses the criminalisation and control of deepfakes and image manipulation [26]. Deepfake cases should therefore be broken down into four distinct acts: creating content, altering content, storing or possessing content, and distributing it. Each act carries different offence elements and burdens of proof. A person depicted in the content is also not automatically its maker or distributor, and is often the victim.

In evidentiary terms, deepfakes change the position of an audiovisual recording from seemingly persuasive proof to proof that must always be tested. Two risks run together: fabricated content enters as evidence, and the opposing party exploits the existence of deepfakes to sow doubt about genuine evidence [6], [5]. Relying on human perception is not enough, so forensic analysis becomes central [27]. Forensics, however, is not a definitive solution. Yu et al. judge that current detectors are not yet ready for real-world use and treat generalisation and robustness as open problems [28]. Heidari et al. note that most deep-learning detection studies focus on accuracy [29], and Rana et al. map detection methods in a systematic review [30]. The legal consequence is clear: a detection result, whether "authentic" or "fake," is expert testimony whose reliability must be assessed, not a ruling that binds the judge. Casey stresses the need to standardise how experts form and express evaluative opinions on digital evidence, so that the degree of confidence and the limits of the method are legible to the judge [31].

3.2 Indonesian Criminal Procedure on Digital Evidence

After 2 January 2026, Indonesian criminal procedure is governed by Law No. 20 of 2025, and the old KUHAP no longer applies. This change matters because Article 184(1) of the old KUHAP did not list digital evidence, which was regulated in statutes outside the KUHAP, so judges had to assess its validity from the manner of its acquisition and presentation [32], [33, Art. 184(1)]. Article 235(1) of the new KUHAP contains a list of means of proof which, according to the discussion examined, covers witness testimony, expert testimony, documents, the statement of the accused, physical evidence, electronic evidence, judicial observation, and anything else usable for proof so long as it

was not obtained unlawfully [9], [23, Art. 235(1)]. Two points are important: electronic evidence is now a type in its own right, and "indications" (petunjuk) is no longer listed as a type of evidence. Article 242 defines electronic evidence broadly, covering electronic information, electronic documents, and/or electronic systems related to a criminal offence [23, Art. 242].

According to Pudjoharsoyo, Article 235(5) codifies the exclusionary principle: a judge may declare that a means of proof has no probative force if it is not authentic or was obtained unlawfully [9]. This provision matters because it gives a basis for testing authenticity, but it does not set out how authenticity is to be tested, in line with the assessment of Samudra et al. that the regulation of authentication and assessment of electronic evidence remains inadequate [10]. The EIT Law remains relevant: electronic information and documents are recognised as valid evidence under Article 5, and manipulation to make them appear authentic is prohibited by Article 35 [12, Arts. 5, 35].

The gap lies in method. Pudjoharsoyo offers four gateways for assessing scientific evidence, namely admissibility, reliability, relevance, and sufficiency, and cites the Daubert criteria (testability, publication, error rate, standards of control, and general acceptance) as evaluative guidance, not a legal obligation [9]. The separation is useful: lawful under the statute (admissibility), genuine (authenticity), methodologically reliable (reliability), and sufficiently convincing (weight) are four different questions. A video admitted as electronic evidence is not necessarily genuine, and a genuine video does not necessarily show that the accused is guilty.

Because the system of proof rests on the judge's assessment, the greatest risk lies precisely in assessment. Amarini et al. show that the testimony of digital forensic experts helps judges establish material truth in information-technology crime cases [34], and Bakhtiar et al. found that the 2023–2024 decisions of the four district courts they examined relied heavily on forensic evidence, especially in narcotics and EIT cases [35]. That reliance is dangerous where judges lack technical literacy, since there is a tendency to hand conclusions over to experts or tools. Butt and Nathaniel note that criminal-law experts in Indonesian trials sometimes reach the question of guilt or innocence, and that such testimony can benefit the state in proving its case [36]. Jamil and Saifuddin warn that the use of artificial intelligence in courts raises problems of reliability of digital evidence, algorithmic accountability, and the erosion of independent judicial reasoning [15], while Anggraeny, Fernando, and Rinaldi emphasise that artificial intelligence must not replace human judgement in complex cases and that the rights of the accused must remain protected [37]. Institutionally, Anggraeny, Rizqullah, and Nur show that scientific crime investigation at regional police offices already includes digital forensics, so judges will increasingly face evidence produced through technical procedures [38]. The Supreme Court itself, through its official channel, has called for technical guidelines and training for judges [9].

As to the rights of the accused, the normative basis is the guarantee of fair legal certainty in Article 28D(1) of the 1945 Constitution and the presumption of innocence. In deepfake cases these principles have concrete meaning: the accused must be able to access raw data and metadata, to know the methods and error rates of the tools used by the expert, and to call a counter-expert. These are recommendations derived from principle, not explicit provisions of the KUHAP, as reaffirmed in subsection E. The answer to the first research question is therefore this: Indonesian criminal procedure provides a gateway for admission, a basis for excluding inauthentic evidence, and freedom of judicial assessment, but it does not yet provide a structured method for assessing synthetic media. This statement rests on secondary discussion of the text of the new KUHAP and should be tested against the official text as practice develops.

3.3 Digital Evidence in the Perspective of Fiqh Jinayah

Fiqh jinayah does not know "electronic evidence" as a classical category, but it does have a framework of proof that can serve as a comparator. Four main concepts are relevant: shahadah (testimony), iqrar (confession), bayyinah (proof in the broad sense), and qarinah (indication or circumstantial evidence). The scope of each concept differs by type of case. In hudud and qisas cases, evidentiary requirements are very strict and the precautionary maxim, often summarised as the duty

to refuse punishment where there is doubt (shubhah), applies strongly. Abikan gives an example: for zina, only four witnesses and a confession are accepted as proof, so circumstantial evidence such as CCTV and DNA cannot support the hadd punishment because it is open to doubt [18]. In ta'zir cases the judge has wider latitude, and Abikan recommends that such evidence be admitted in all non-hudud cases, especially where there is no human interference with the evidence [18].

Differences of opinion about qarinah must be recorded, not erased. The acceptance of qarinah as a basis for punishment is not uniform, especially for hudud and qisas, so there is no basis to say that qarinah is always accepted or always rejected. Contemporary literature shows that its acceptance is widest in ta'zir cases: Dayanti and Zulkarnain conclude that audio can be qarinah or bayyinah in ta'zir on condition of authenticity [16]. In Malaysian Shariah court practice, the admission of electronic documents is tied to the principles of chain of evidence and custody [20], [19]. It should be noted that these studies start from procedural traditions that already know written evidence enactments, so transposing them to the Indonesian context calls for caution.

Contemporary literature tends to place digital evidence as qarinah, and as supporting evidence. Wan Ismail et al. conclude that digital documents help reinforce other evidence in court [17], and Jibril, Bello, and Abubakar reach a similar conclusion for AI-generated evidence: it is secondary, cannot replace traditional proof, and should be set aside where uncertainty remains [21]. The one study touching on deepfakes concludes that creating pornographic deepfakes meets the elements of qadzaf, so hudud punishment may apply [22]. The remaining question is how those elements are proved, and this is where the strict evidentiary requirements of hudud, as described by Abikan, become relevant [18].

What these writings leave unaddressed is that deepfakes change the core condition of qarinah. Qarinah has value only if its indication is independent and reliable; deepfakes undermine precisely the reliability of audiovisual indications. Digital evidence can therefore be read as qarinah only after it passes tests of authenticity and reliability, and even then it does not automatically prove guilt. In serious cases, a recording that passes the authenticity test functions at most as an indication that must be corroborated by other evidence. The principles of caution and protection of the accused reinforce this direction: technical uncertainty is a procedural shubhah that should benefit the accused. The answer to the second research question is thus as follows: fiqh jinayah provides a conservative, graded toolkit for assessing digital evidence, with qarinah as the critical entry point rather than automatic proof.

3.4 Comparative Analysis of Evidentiary Standards

The following functional comparison does not equate articles of law with concepts; it maps evidentiary functions. Table 1 summarises the equivalences and tensions.

Table 1. Functional comparison of the proof of digital evidence

Function	KUHAP 2025 (Indonesia)	Fiqh jinayah	Comparative note
Admission of evidence	Electronic evidence is a type in its own right; requirement of non-unlawful acquisition (Art. 235)	Digital evidence positioned as qarinah or bayyinah in contemporary literature	Formal categories differ; similar "gatekeeping" function
Authentication	Inauthentic evidence may be denied probative force (Art. 235(5), according to Pudjoharsoyo)	Authenticity and freedom from fabrication required before qarinah is used	Functionally aligned; technical methods not regulated in either
Assessment of reliability	Judicial assessment; Daubert criteria only evaluative guidance	Qadi's assessment of the strength of qarinah; differences among schools on its degree	No standard technical benchmark in either system

Function	KUHAP 2025 (Indonesia)	Fiqh jinayah	Comparative note
Attribution of the perpetrator	Proved through means of proof and the judge's conviction	Qarinah must point conclusively to the perpetrator; serious cases require iqrar or shahadah	Fiqh is stricter in serious cases
Determination of guilt	Judge's conviction based on means of proof	Punishment is refused where doubt (shubhah) exists	Sources of legitimacy differ; protection of the accused may converge

Table 1 shows three findings. First, both systems reject proof that cannot be tested, but with different logics: modern criminal procedure stresses process (lawful acquisition, authentication, the right to test evidence), whereas *fiqh jinayah* stresses substantive caution to avoid wrongful punishment. Second, the disappearance of "indications" from the list in Article 235(1) does not mean that the inferential function has vanished; that function is now absorbed into the system for assessing electronic evidence and other means of proof. This brings modern judicial reasoning closer to, but does not equate it with, reasoning about *qarinah*. Third, *fiqh jinayah* retains non-digital anchors (iqrar and shahadah) for serious cases, whereas Indonesian procedure relies on the judge's conviction formed from various means of proof. The difference in sources of legitimacy (revealed text and juristic reasoning as against statute) cannot be removed.

The practical implication is that the most stable meeting point lies in the protective function, namely the testing of authenticity, reliability, and doubt, not in shared terminology. This point becomes the foundation of the framework in the next subsection.

3.5 Reconstructing a Layered Framework for Assessing Deepfake Evidence

Based on the preceding subsections, this article proposes the Layered Digital Evidence Assessment Framework for Deepfake Prosecutions (LDEAF), a five-layer analytical framework summarised in Figure 1. The framework is a working label arising from synthesis, not positive law; each layer distinguishes between existing obligations and recommendations. The layers are ordered and divided into two tracks: a content-authenticity track (layers 1–3) and an attribution-of-conduct track (layer 4), converging on the final assessment (layer 5). Failure at an early layer cannot be cured by the strength of a later one.

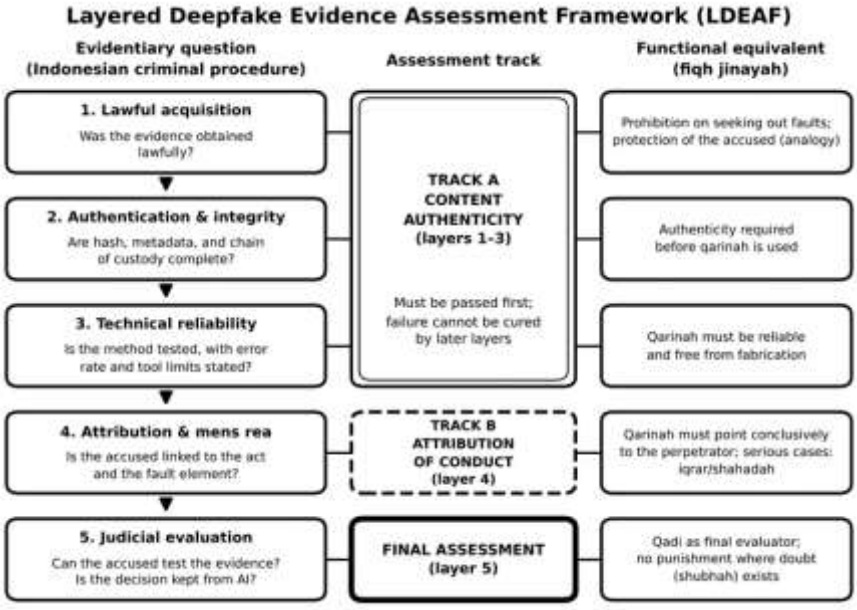


Figure 1. The Layered Deepfake Evidence Assessment Framework (LDEAF) and its functional equivalents in *fiqh jinayah*

Layer 1: Lawful acquisition. Was the evidence obtained lawfully? This is a positive obligation because Article 235 ties the probative force of evidence to acquisition that is not unlawful [9]. The fiqh equivalent is the protection of the accused from the search for faults, used here only as a principled analogy that needs support from specialised literature.

Layer 2: Authentication and integrity. Have the origin, hash value, metadata, and chain of custody been documented so that the possibility of alteration can be assessed? This question accords with Braga da Silva's critique of authenticity assessment that still follows the logic of physical documents [7], and with the study of chain of custody in Shariah criminal cases [19]. The positive-law basis is the demand for authentication in Article 235(5); the technical details are recommendations, which may draw on the idea of Samudra et al. of standards for the governance of electronic evidence [10]. Metadata must not be assumed always trustworthy because it can itself be manipulated. The fiqh equivalent is the authenticity requirement that scholars set for accepting recorded evidence [16].

Layer 3: Technical reliability. Can the examination method be tested, does it have a known error rate, and are the limits of the tool explained? The *Daubert* criteria may serve as evaluative guidance, not an obligation [9]. Deepfake detection tools must not be assumed always accurate [29], [28], and expert reports need to state the limits of the method and the degree of confidence in a standardised way [31].

Layer 4: Attribution and mental state. Does the evidence genuinely connect the accused to the charged conduct and prove the element of fault? This layer separates the person depicted, the maker, the alterer, the uploader, and the distributor, given that the victim is often the person depicted in the content. Ownership of an account, IP address, or device is not enough to infer guilt. The need arises because Article 35 of the EIT Law requires intent and purpose to make information appear authentic [12, Art. 35]. The fiqh equivalent is the requirement that qarinah point conclusively to the perpetrator and, for serious cases, be reinforced by iqrar, shahadah, or other bayyinah [18], [21].

Layer 5: Judicial evaluation and procedural safeguards. Can the accused test the evidence and present counter-evidence, and does the judge assess all the evidence without handing the conclusion to AI or experts? This accords with the requirement that the judge act as gatekeeper [9] and with concerns about the erosion of judicial reasoning [37], [36], [15]. The fiqh equivalent is the role of the qadi as final evaluator and the principle of refusing punishment where doubt exists.

An internal consistency test shows that the framework does not erase fundamental differences. Layers 1 and 5 have more general principled equivalents, layers 2 and 3 can be translated functionally through the authenticity and reliability requirements for qarinah, and layer 4 is closest to the cautious logic of fiqh. The limits of application are these: the framework is intended only for criminal cases that depend on audiovisual content that may be synthetic, does not cover all AI-based offences, and must not be read as a stand-alone validity requirement under the KUHAP. As a benchmark for other researchers, each layer can be tested by asking whether the decision or case file documents the answer.

This yields the answer to the third research question: the evaluation standard that can be reconstructed is layered and sequential, treats authentication of content and attribution of conduct as two separate questions, and makes technical uncertainty a factor favouring the accused within the cautious framework shared by both traditions.

3.6 Implications for Criminal Justice and Legal Reform

For legislators and the Supreme Court, the most urgent recommendation is technical guidelines for assessing digital and forensic evidence, as also voiced in the discussion on the Supreme Court's official channel [9], specifically regulating authentication tests for synthetic content, documentation of tool error rates, and defence access to raw data. This idea accords with the criticism of Samudra et al. that what is needed is a principled governance model for digital proof, not merely additional articles [10], and with the finding of Oktaviani et al. that the regulatory vacuum on

deepfakes hampers enforcement [13]. Bakhtiar et al. even recommend that forensic evidence be classified as an independent category [35]. Such guidelines are a policy choice, not an existing obligation.

For investigators and public prosecutors, the implication is to draft indictments that separate the acts of creating, altering, storing, and distributing, and not to stop at proving that content was generated by AI. For forensic experts, reports need to state the method, the limits of the tool, and the possibility of erroneous results [31]. For judges, the LDEAF can serve as a checklist for the reasoning in a decision. These recommendations hold only insofar as they are supported by the analysis above and need to be tested on real decisions when they become available.

CONCLUSION

Indonesian criminal procedure after Law No. 20 of 2025 recognises electronic evidence as a means of proof and provides a basis for excluding evidence that is inauthentic or unlawfully obtained, but it does not yet provide a structured method for assessing synthetic content; the assessment of reliability is left mainly to judges, who need guidance. Second, fiqh jinayah provides a cautious, graded toolkit; digital evidence may be considered as qarinah only after it passes tests of authenticity and reliability, and in serious cases it must be corroborated by other evidence. Third, the reconstruction of an evaluation standard can be formulated in five layers (lawful acquisition, authentication, technical reliability, attribution and mental state, and judicial evaluation) that separate the authenticity of content from the attribution of conduct.

The contribution of this article is conceptual and limited: an analytical framework synthesised from legal materials and literature, neither an empirical finding nor a claim of absolute novelty. The recommendation for policymakers is to draw up guidelines for assessing digital evidence and to adopt the principle that technical uncertainty favours the accused. The limitations of the study are that the official text of the 2025 KUHAP was read through secondary discussion, that no verifiable deepfake decisions were found, and that fiqh concepts were read through contemporary literature rather than classical books. Further research should test this framework on real decisions and examine classical fiqh sources directly.

REFERENCES

[1] Y. Mirsky and W. Lee, "The creation and detection of deepfakes: A survey," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–41, 2021, doi: 10.1145/3425780.

[2] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, A. Morales, and J. Ortega-Garcia, "Deepfakes and beyond: A survey of face manipulation and fake detection," *Inf. Fusion*, vol. 64, pp. 131–148, 2020, doi: 10.1016/j.inffus.2020.06.014.

[3] Á. F. Gambín, A. Yazidi, A. Vasilakos, H. Haugerud, and Y. Djenouri, "Deepfakes: Current and future trends," *Artif. Intell. Rev.*, vol. 57, no. 3, 2024, Art. no. 64, doi: 10.1007/s10462-023-10679-x.

[4] M. Masood, M. Nawaz, K. M. Malik, A. Javed, A. Irtaza, and H. Malik, "Deepfakes generation and detection: State-of-the-art, open challenges, countermeasures, and way forward," *Appl. Intell.*, vol. 53, no. 4, pp. 3974–4026, 2023, doi: 10.1007/s10489-022-03766-z.

[5] M.-P. Sandoval, M. de Almeida Vau, J. Solaas, and L. Rodrigues, "Threat of deepfakes to the criminal justice system: A systematic review," *Crime Sci.*, vol. 13, no. 1, 2024, Art. no. 41, doi: 10.1186/s40163-024-00239-1.

[6] D. Fallis, "The epistemic threat of deepfakes," *Philos. Technol.*, vol. 34, no. 4, pp. 623–643, 2021, doi: 10.1007/s13347-020-00419-2.

[7] R. Braga da Silva, "Updating the authentication of digital evidence in the International Criminal Court," *Int. Crim. Law Rev.*, vol. 22, no. 5–6, pp. 941–964, 2021, doi: 10.1163/15718123-bja10083.

[8] S. O. Perez, "Proliferation of e-evidence: Reliability standards and the right to a fair trial," *Eur. J. Crime Crim. Law Crim. Justice*, vol. 33, no. 1–2, pp. 187–211, 2025, doi: 10.1163/15718174-bja10070.

[9] A. S. Pudjoharsoyo, "Hakim sebagai 'gatekeeper' bukti ilmiah di era KUHAP baru [Judges as 'gatekeepers' of scientific evidence in the new KUHAP era]," *MARINews Mahkamah Agung*, Jan. 30, 2026. [Online]. Available: https://marinews.mahkamahagung.go.id/artikel/hakim-sebagai-gatekeeper-bukti-ilmiah-di-era-kuhap-baru-0O4

[10] A. H. Samudra, S. Basu, and C. Saenz Perez, "Digital challenge, analogue mind-set: Assessing Indonesia's electronic criminal evidence framework," *J. Indones. Leg. Stud.*, vol. 11, no. 1, pp. 257–298, 2026, doi: 10.15294/jils.v11i1.35378.

[11] R. Saputra, J. P. Setiodjati, and J. Barkhuizen, "Under-legislation in electronic trials and renewing criminal law enforcement in Indonesia (comparison with United States)," *J. Indones. Leg. Stud.*, vol. 8, no. 1, pp. 243–288, 2023, doi: 10.15294/jils.v8i1.67632.

[12] *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik* [Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions], 2024.

[13] A. Oktaviani, D. R. Hayati, E. S. Sinaga, D. N. Deris, and T. I. Irawan, "Between innovation and legal vacuum: Evaluating Indonesia's criminal law readiness against deepfake artificial intelligence," *J. Media Huk.*, vol. 33, no. 1, pp. 158–177, 2026, doi: 10.18196/jmh.v33i1.29574.

[14] S. Suseno, A. M. Ramli, R. F. Mayana, T. Safiranita, and B. A. N. Tiarma, "Cybercrime in the new criminal code in Indonesia," *Cogent Soc. Sci.*, vol. 11, no. 1, 2025, Art. no. 2439543, doi: 10.1080/23311886.2024.2439543.

[15] A. Jamil and S. Saifuddin, "The use of artificial intelligence in the court process in Indonesia: A review of procedural law on the aspect of evidence and decision-making," *Lex Sci. Law Rev.*, vol. 10, no. 1, pp. 521–550, 2026, doi: 10.15294/lslr.v10i1.28681.

[16] R. Dayanti and Zulkarnain, "An analysis of Islamic criminal justice regarding the validity of audio recordings as evidence," *Al-Risalah: J. Ilmu Syariah Huk.*, vol. 25, no. 2, pp. 559–674, 2025, doi: 10.24252/al-risalah.vi.59773.

[17] W. A. F. Wan Ismail, A. S. Baharuddin, L. A. Mutalib, and M. A. A. Alias, "An appraisal of digital documents as evidence in Islamic law," *Acad. J. Interdiscip. Stud.*, vol. 10, no. 3, p. 198, 2021, doi: 10.36941/ajis-2021-0076.

[18] Y. I. Abikan, "Examining the admissibility or otherwise of evidence generated from closed-circuit television (CCTV) and deoxyribonucleic acid (DNA) test as means of proof of zina under Islamic law," *Al-Manahij: J. Kaji. Huk. Islam*, vol. 17, no. 1, pp. 83–96, 2023, doi: 10.24090/mnh.v17i1.8172.

[19] M. A. Yahya, A. A. M. Shariff, and S. Saifuddin, "Application of principles of chain of evidence and chain of custody during storage and forensic examination of electronic documentary evidence in Shariah criminal cases in Malaysia," *IIUM Law J.*, vol. 31, no. S1, pp. 143–164, 2023, doi: 10.31436/iiumlj.v31is1.874.

[20] M. A. A. Alias, W. A. F. Wan Ismail, A. S. Baharuddin, H. Hashim, and M. S. Mallow, "An appraisal of the legal framework governing the admissibility of electronic documents as evidence in Malaysian Shariah courts: Current practices and future legal directions," *IIUM Law J.*, vol. 33, no. 2, pp. 69–108, 2025, doi: 10.31436/iiumlj.v33i2.1077.

[21] A. M. Jibril, R. A. Bello, and A. Abubakar, "AI-enhanced criminal investigations and Ḥudūd offenses: A Sharīʿah compliance framework," *Alauddin Law Dev. J.*, vol. 7, no. 2, pp. 137–150, 2025, doi: 10.24252/aldev.v7i2.56748.

[22] F. Maulana and S. Abbas, "Deepfake pornography as Qadzaf: Legal status and Hudud implications," *Al-Risalah: J. Ilmu Syariah Huk.*, vol. 25, no. 2, pp. 979–991, 2025, doi: 10.24252/al-risalah.vi.62018.

[23] *Undang-Undang Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana* [Law No. 20 of 2025 on the Criminal Procedure Code], 2025.

[24] *Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana* [Law No. 1 of 2023 on the Criminal Code], 2023.

[25] A. Flynn, A. Powell, A. J. Scott, and E. Cama, "Deepfakes and digitally altered imagery abuse: A cross-country exploration of an emerging form of image-based sexual abuse," *Br. J. Criminol.*, vol. 62, no. 6, pp. 1341–1358, 2022, doi: 10.1093/bjc/azab111.

[26] T. Kirchengast, "Deepfakes and image manipulation: Criminalisation and control," *Inf. Commun. Technol. Law*, vol. 29, no. 3, pp. 308–323, 2020, doi: 10.1080/13600834.2020.1794615.

[27] L. Verdoliva, "Media forensics and DeepFakes: An overview," *IEEE J. Sel. Top. Signal Process.*, vol. 14, no. 5, pp. 910–932, 2020, doi: 10.1109/JSTSP.2020.3002101.

[28] P. Yu, Z. Xia, J. Fei, and Y. Lu, "A survey on deepfake video detection," *IET Biom.*, vol. 10, no. 6, pp. 607–624, 2021, doi: 10.1049/bme2.12031.

[29] A. Heidari, N. J. Navimipour, H. Dag, and M. Unal, "Deepfake detection using deep learning methods: A systematic and comprehensive review," *WIREs Data Min. Knowl. Discov.*, vol. 14, no. 2, 2024, Art. no. e1520, doi: 10.1002/widm.1520.

[30] M. S. Rana, M. N. Nobi, B. Murali, and A. H. Sung, "Deepfake detection: A systematic literature review," *IEEE Access*, vol. 10, pp. 25494–25513, 2022, doi: 10.1109/ACCESS.2022.3154404.

[31] E. Casey, "Standardization of forming and expressing preliminary evaluative opinions on digital evidence," *Forensic Sci. Int.: Digit. Investig.*, vol. 32, 2020, Art. no. 200888, doi: 10.1016/j.fsidi.2019.200888.

[32] D. G. G. Santosa and K. M. I. Kamali, "Acquisition and presentation of digital evidence in criminal trial in Indonesia," *J. Huk. Peradil.*, vol. 11, no. 2, pp. 195–218, 2022, doi: 10.25216/jhp.11.2.2022.195-218.

[33] *Undang-Undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana* [Law No. 8 of 1981 on Criminal Procedure], 1981.

[34] I. Amarini, R. A. Cahyadri, M. A. Fitriani, and N. Ismail, "The legal position of digital forensic experts in the settlement of information technology crime cases," *Lex Sci. Law Rev.*, vol. 8, no. 1, pp. 355–384, 2024, doi: 10.15294/lslr.v8i1.2952.

[35] H. S. Bakhtiar, A. Ilyas, A. Kholiq, H. S. Bakhtiar, and A. Yusup, "The role of forensic evidence in Indonesia's criminal justice," *Forensic Sci. Int.: Synergy*, vol. 12, 2026, Art. no. 100693, doi: 10.1016/j.fsisyn.2026.100693.

[36] S. Butt and A. Nathaniel, "Evidence from criminal law experts in Indonesian criminal trials: Usurping the judicial function?," *Int. J. Evid. Proof*, vol. 28, no. 2, pp. 129–153, 2024, doi: 10.1177/13657127231217319.

[37] K. Anggraeny, Z. Fernando, and K. Rinaldi, "Robot prosecutors and the future of criminal justice in Indonesia: Innovation, ethics, and legal implications," *Padjadjaran J. Ilmu Huk. (J. Law)*, vol. 12, no. 1, pp. 25–47, 2025, doi: 10.22304/pjih.v12n1.a2.

[38] K. D. Anggraeny, A. N. Rizqullah, and M. Nur, "The implementation of scientific crime investigation mechanisms in police regional office proof criminal cases," *Indones. J. Crim. Law Stud.*, vol. 9, no. 1, pp. 89–116, 2024, doi: 10.15294/ijcls.v9i1.36419.