

The Principle of *Satr al-'Aurah* in Proving *Jarimah Zinā*: A Critical Analysis of the Legality of Digital Evidence in Islamic Law

Islamul Haq^{1*}, Abdul Syatar²

¹ Institut Agama Islam Negeri Parepare, Sulawesi Selatan

² Universitas Islam Negeri Alauddin Makassar, Sulawesi Selatan

Correspondence:

islamulhaq@iainpare.ac.id

Received: 30-04-2026

Revised: 04-08-2026

Accepted: 16-08-2026

Abstract: *The advancement of digital technology has introduced new forms of evidence in judicial systems, including in the adjudication of private criminal offenses such as jarimah zinā. Within the framework of positive law, digital evidence such as video recordings, photographs, and electronic communications is often regarded as carrying significant probative weight. However, from the perspective of Islamic criminal law, the proof of zinā is governed by exceedingly strict standards, requiring either the testimony of four upright male witnesses or a voluntary confession by the perpetrator, both of which fundamentally reflect Sharia's commitment to protecting individual honor and dignity. The principle of satr al-'awrah, as a foundational value in Islam, underscores the obligation to conceal moral failings and safeguard privacy, thereby opening space for critical scrutiny of digital evidence that may instead expose and disseminate a person's private shame. This study aims to analyze the legality and relevance of digital evidence in proving jarimah zinā by positioning the principle of satr al-'awrah as the primary normative framework. The method employed is normative legal research utilizing a conceptual approach and a maqāṣid al-shari'ah approach. The findings indicate that digital evidence cannot be equated with the evidentiary instruments established in classical Islamic jurisprudence, as it neither meets the rigorous standards of proof nor complies with the principle of protecting human dignity. Consequently, the use of digital evidence in zinā cases must be strictly curtailed and should generally be excluded in the determination of hudūd punishments and may only be considered with extreme caution in the context of ta'zīr, while consistently upholding the principles of precaution (ihtiyāt) and the protection of human dignity. This study affirms that in confronting the challenges posed by technological advancement, Islamic criminal law is not solely oriented toward formal adjudication, but is equally committed to preserving ethical values and the objectives of Sharia, particularly the protection of honor (ḥifẓ al-'ird). Accordingly, the principle of satr al-'awrah must remain the foundational basis in responding to the challenges of digitalizing legal evidentiary processes.*

Abstrak: Perkembangan teknologi digital telah melahirkan bentuk-bentuk baru alat bukti dalam sistem peradilan, termasuk dalam penanganan tindak pidana privat seperti jarimah zinā. Dalam hukum positif, alat bukti digital, seperti rekaman video, fotografi, dan komunikasi elektronik, dipandang memiliki kekuatan pembuktian yang signifikan. Namun, dalam perspektif hukum pidana Islam, pembuktian zinā tunduk pada standar yang sangat ketat, yaitu kesaksian empat orang laki-laki yang adil atau pengakuan sukarela pelaku, yang mencerminkan komitmen syariat terhadap perlindungan kehormatan dan martabat manusia. Prinsip satr al-'awrah sebagai nilai fundamental menegaskan kewajiban menutup aib dan menjaga privasi, sehingga memunculkan kritik terhadap penggunaan alat bukti digital

yang berpotensi mengungkap aib individu. Penelitian ini bertujuan menganalisis legalitas dan relevansi alat bukti digital dalam pembuktian jarimah zinā dengan menjadikan prinsip *satr al-'awrah* sebagai kerangka normatif utama, menggunakan metode penelitian hukum normatif melalui pendekatan konseptual dan *maqāṣid al-sharī'ah*. Hasil penelitian menunjukkan bahwa alat bukti digital tidak dapat disetarakan dengan instrumen pembuktian dalam fikih klasik karena tidak memenuhi standar pembuktian yang ketat serta tidak selaras dengan prinsip perlindungan martabat manusia. Oleh karena itu, penggunaannya harus dibatasi secara ketat, dikecualikan dalam penetapan sanksi *ḥudūd*, dan hanya dapat dipertimbangkan secara sangat hati-hati dalam konteks *ta'zīr* dengan tetap menjunjung prinsip kehati-hatian (*iḥtiyāt*) dan perlindungan kehormatan (*ḥifẓ al-'ird*), sehingga menegaskan bahwa hukum pidana Islam tidak hanya berorientasi pada pembuktian formal, tetapi juga pada penjagaan nilai etis dan tujuan syariat dalam menghadapi tantangan digitalisasi pembuktian hukum.

Keywords: *Digital evidence; jarimah zinā; satr al-'awrah; maqāṣid al-sharī'ah; Islamic criminal law*



Introduction

The rapid proliferation of digital technology has fundamentally transformed patterns of human interaction, including the manner in which criminal offenses of a moral and sexual nature are committed and documented (Wall, 2024). The widespread adoption of smartphones has rendered virtually every private activity susceptible to digital documentation through instant messaging platforms, photographic records, and video recordings stored in device memory (Hand, 2016). According to the Indonesian Ministry of Communication and Information Technology, internet penetration in Indonesia reached 77.02% of the total population in 2023, equivalent to approximately 215.63 million users, representing one of the highest rates of digital adoption in Southeast Asia (Triwahyuni et al., 2025). This unprecedented level of digital connectivity has made electronic traces an almost inevitable byproduct of human conduct, including conduct of a private and intimate nature (Goodman, 2015).

As a consequence, digital evidence encompassing video recordings, photographs, and electronic communications has increasingly emerged as the primary form of evidence in reports of sexual offenses filed with law enforcement authorities (Dodge, 2018). Data from the Indonesian National Police (Polri) recorded a significant increase in cybercrime cases involving immoral content, with 1,855 cases reported in 2022 alone, many of which involved digital evidence as the principal evidentiary basis (admin, 2025). The admission of such evidence in judicial proceedings has triggered serious scholarly and jurisprudential debate regarding the standards of material truth and the integrity of the evidentiary process (Majeed et al., 2023). Digital evidence, by its very nature, is particularly susceptible to manipulation through conventional video and photo editing techniques, as well as to alterations in metadata characteristics that fundamentally distinguish it from traditional testimonial evidence (Suryal, 2024).

Within the framework of classical Islamic criminal law (*fiqh jinayah*), the evidentiary standard for establishing the offense of *zinā* (unlawful sexual intercourse) is among the most rigorous in the entire corpus of Islamic jurisprudence (Fawwas, 2025). The proof of *zinā* requires either the

simultaneous testimony of four upright male witnesses who directly witnessed the act, or a voluntary and uncoerced confession by the perpetrator. This extraordinarily high standard reflects the Sharia's profound commitment to the protection of individual honor and dignity, operationalized through the doctrinal principle that prescribed punishments (*ḥudūd*) must be averted in the presence of any doubt, as encapsulated in the maxim: *idra'ū al-ḥudūd bi al-shubuhāt* (repel *ḥudūd* penalties whenever doubt exists). The emergence of digital evidence in the form of video recordings poses a fundamental challenge to the continued relevance and applicability of this four-witness requirement in the contemporary judicial context.

Perhaps the most profound challenge posed by digital evidence in this context is its apparent incompatibility with the principle of *satr al-'awrah* as a foundational value in Islamic ethics that imposes an obligation upon Muslims to conceal the moral failings and private transgressions of their fellow believers (Ibrahim et al., 2026). This principle, grounded in several Qur'anic injunctions and Prophetic traditions (*ahadith*), establishes that sins of a private nature, which do not directly harm the public interest, ought not to be exposed or publicized in order to preserve the honor and dignity of individuals. The historical record of Islamic legal practice demonstrates that classical jurists consistently prioritized sincere repentance (*tawbah naṣūḥah*) over the public disclosure of moral failings, provided the strict evidentiary requirements were not satisfied. Accordingly, the deployment of digital recordings that expose and disseminate the details of a person's most private conduct carries a significant risk of violating the fundamental principle of the protection of honor (*ḥifẓ al-'ird*), one of the five essential objectives (*maqāṣid*) of the Sharia.

The evidentiary use of digitally obtained materials in cases of sexual offenses is further complicated by the prohibition of *tajassus*; the active surveillance or spying upon the private affairs of others which is explicitly proscribed in the Qur'an (49:12) and elaborated upon extensively in Islamic jurisprudential literature. The justification for this prohibition rests upon the recognition that intrusive surveillance of private conduct has the potential to destabilize the social fabric and to generate forms of social harm (*fitnah*) that may prove more corrosive than the original offense itself. Digital evidence obtained through privacy-violating means — such as the unauthorized access to personal devices, interception of private communications, or the non-consensual dissemination of intimate material — is therefore regarded as ethically defective from the perspective of Islamic criminal law, irrespective of its forensic authenticity.

A significant normative tension exists between the Indonesian positive law framework and the principles of Islamic criminal law with respect to the treatment of digital evidence. The Electronic Information and Transactions Law (UU ITE No. 11 of 2008, as amended by Law No. 19 of 2016) and the newly enacted National Criminal Code (KUHP), which came into force in late 2022, both provide an expansive evidentiary role for electronic information and documents (Darmawansyah et al., 2025). Notably, the new KUHP now classifies *zinā* as a complaint-based offense (*delik aduan*), thereby substantially modifying the prosecutorial framework relative to the previous colonial-era code. Nevertheless, classical Islamic jurisprudence remains deeply contested on the question of whether a video recording can be treated as equivalent to the direct ocular testimony of a witness — a contestation that reflects deeper epistemological differences regarding the nature of knowledge, certainty, and legal proof. Scholarly opinion within the *fiqh* tradition is inclined to categorize video recordings as a form of circumstantial evidence (*qarīnah*) rather than as primary proof, suggesting that digital evidence in *zinā* cases is more appropriately considered as supporting evidence within the framework of discretionary punishment (*ta'zīr*) rather than as the basis for the imposition of *ḥudūd* sanctions.

The sociological dimensions of this issue are of considerable urgency. Data from the Indonesian National Commission on Violence Against Women (Komnas Perempuan) indicate that cases of non-consensual intimate image sharing (commonly referred to as revenge pornography) reached 241 reported cases in 2022, with the actual incidence believed to be substantially higher due to underreporting (Prayudati et al., 2025). The dissemination of such content has been shown to

produce severe and long-lasting psychological trauma for victims and their families, while simultaneously generating a phenomenon of 'digital mob justice' in which accused individuals are subjected to severe social punishment through the viral spread of intimate recordings prior to any formal judicial determination. These sociological realities underscore the critical importance of developing a principled framework for the governance of digital evidence in cases of sexual offenses one that is sensitive to the rights and dignity of all parties involved.

Existing scholarship on this subject has tended to focus predominantly on the technical dimensions of the UU ITE framework or on the general question of digital evidence admissibility in Indonesian positive law, without sufficiently engaging with the normative resources of Islamic jurisprudence. This study seeks to address that lacuna by examining the legality and relevance of digital evidence in the proof of *jarimah zinā* through the normative lens of the principle of *satr al-'awrah*. In doing so, it employs a normative legal research methodology, integrating a conceptual approach with a *maqāṣid al-shari'ah* framework, in order to assess the compatibility of digital evidentiary practices with the foundational objectives and values of Islamic law. The novelty of this study lies in its proposal of a 'digital privacy protection' model a framework that restricts access to digital evidence of a sexual nature to judges and investigators exclusively, thereby preventing the public dissemination of such material and upholding the dignity of all persons implicated in the proceedings.

The ultimate aim of this study is to formulate an integrative model that reconciles the advances of digital forensics with the ethical imperatives of Islamic criminal law — ensuring that the administration of justice in the modern era remains anchored in the principles of fairness, truthfulness, and respect for human dignity. It is the contention of this study that Islamic criminal law, far from being ill-equipped to address the challenges of the digital age, possesses within its jurisprudential heritage the normative resources necessary to construct a principled, humane, and contextually sensitive response to the evidentiary challenges posed by digital technology. In particular, the principle of *satr al-'awrah*, understood as an expression of the Sharia's commitment to the protection of honor (*ḥifẓ al-'ird*) as one of its five fundamental objectives, must serve as the primary normative foundation in any jurisprudential response to the challenge of digitalizing the legal evidentiary process.

Method

This study employs a normative juridical (*yuridis normatif*) research design, grounded in a systematic and comprehensive review of legal literature. This methodological orientation is adopted on the basis that the primary objective of the research is to examine the degree of alignment and points of tension between the positive law framework governing digital evidence in Indonesia, specifically the Electronic Information and Transactions Law (UU ITE No. 11 of 2008 as amended by Law No. 19 of 2016) and the newly enacted National Criminal Code (KUHP 2022), and the doctrinal principles of Islamic criminal law (*fiqh jinayah*) pertaining to the proof of *zinā* offenses. The normative juridical approach is particularly well-suited to this inquiry, as it enables a rigorous analytical engagement with both statutory texts and classical jurisprudential sources, thereby facilitating the identification of normative gaps, doctrinal inconsistencies, and potential frameworks for legal integration. As Marzuki (2017) observes, normative legal research is the most appropriate methodological choice when the central concern is the internal coherence and substantive content of legal norms, rather than their empirical application in social practice.

The study integrates three complementary legal research approaches: a statute approach, a conceptual approach, and a comparative approach. The statute approach is employed to conduct a systematic examination of the relevant legislative instruments including the UU ITE, the KUHP 2022, and the evidentiary provisions applicable to sexual offense cases in order to map the current positive law framework governing the admissibility and weight of digital evidence. The conceptual approach, by

contrast, draws upon the foundational principles and doctrines of Islamic jurisprudence in particular the principle of *satr al-'awrah*, the *maqāṣid al-sharī'ah* framework, and the classical doctrine of *ḥifẓ al-'ird* (the protection of honor) in order to construct a normative Islamic standard against which digital evidentiary practices may be evaluated. The comparative approach, finally, enables a critical juxtaposition of the evidentiary standards operative in the two legal systems under examination: the openness of Indonesian positive law to technologically generated evidence, on the one hand, and the highly selective and stringent evidentiary requirements of classical Islamic criminal law on the other. The synthesis of these three approaches provides the analytical foundation for the development of an integrative evidentiary model that is both technically informed and ethically grounded.

The research draws exclusively upon secondary data sources, organized into three hierarchical categories of legal materials. Primary legal materials consist of binding normative instruments, including the UU ITE and its amendments, the KUHP 2022, relevant Supreme Court Regulations, as well as classical works of Islamic jurisprudence (*kutub al-fiqh*) addressing the doctrines of *shahādah* (testimony), *iqrār* (confession), and *qarīnah* (circumstantial evidence) including authoritative texts such as al-Māwardī's *al-Aḥkām al-Sultāniyyah*, Ibn Qudāmāh's *al-Mughnī*, and al-Shāfi'ī's *al-Umm*. Secondary legal materials comprise scholarly monographs, peer-reviewed journal articles, doctoral dissertations, and comparative studies addressing the intersection of digital technology, criminal evidence, and Islamic legal doctrine. Tertiary legal materials, including legal dictionaries, encyclopaedias of Islamic jurisprudence, and bibliographic indices, are consulted to clarify terminology and to identify relevant primary and secondary sources. The exclusive reliance upon secondary data is justified by the doctrinal character of the research, which is concerned with the analysis and interpretation of legal texts and juristic opinions rather than with empirical observation of legal practice in its social context.

Data collection is conducted through systematic documentary research and thematic classification of sources. Relevant materials are identified through searches of academic databases including Google Scholar, Scopus, and the Indonesian Scientific Journal Database (SINTA) as well as through targeted searches of Islamic jurisprudential repositories and digital libraries of classical *fiqh* texts. Sources are selected on the basis of their direct relevance to the research questions concerning digital evidence admissibility, the principle of *satr al-'awrah*, and the evidentiary standards applicable to *zinā* offenses under Islamic law. Collected materials are subsequently organized into thematic clusters corresponding to the principal analytical dimensions of the study: (1) the positive law framework for digital evidence; (2) the classical Islamic evidentiary doctrine; (3) the normative content and legal implications of *satr al-'awrah*; and (4) the *maqāṣid al-sharī'ah* framework as an interpretive tool for legal integration.

Data analysis is conducted through a qualitative descriptive method utilizing deductive content analysis (*analisis isi deduktif*). This analytical technique proceeds from the general principles established in Islamic criminal law doctrine — in particular the principle of *satr al-'awrah* and the overarching *maqāṣid al-sharī'ah* framework — to particular conclusions regarding the legality, admissibility, and appropriate evidentiary weight of digital evidence in cases of *zinā*. Content analysis is applied to both the statutory texts of Indonesian positive law and to the primary sources of classical Islamic jurisprudence, with a view to identifying the normative categories within which digital recordings and electronic communications may appropriately be classified under Islamic evidentiary doctrine whether as a form of *qarīnah* (circumstantial evidence), as a basis for *ta'zīr* (discretionary punishment), or as inadmissible evidence in the context of *ḥudūd* determination. The analytical process is guided by the interpretive framework of *maqāṣid al-sharī'ah*, which enables the researcher to assess not merely the formal validity of digital evidence, but also its compatibility with the substantive values and protective objectives of the Sharia most critically, the protection of human dignity and honor (*ḥifẓ al-'ird*). The ultimate outcome of this analytical process is the formulation of a normatively grounded and practically viable model for the governance of digital evidence in Islamic criminal adjudication.

Results and Discussion

Reconstruction of Digital Evidence in Islamic Criminal Law: Balancing Forensic Certainty and Privacy Protection (*Satr al-'Awrah*)

The findings of this study demonstrate that digital evidence in cases of *jarīmah zinā* cannot be accorded the status of primary proof (*bayyinah*) under Islamic law; rather, it is more appropriately classified as corroborating or circumstantial evidence (*qarīnah*). This determination is grounded in the fact that Islamic law prescribes an exceptionally rigorous evidentiary standard for the proof of *zinā* requiring either the concurrent testimony of four upright male witnesses or a voluntary confession by the accused in order to preclude the possibility of wrongful conviction. (Ahmad, 2021) The scholarly literature establishes that digital recordings and photographs are inherently susceptible to evidentiary doubt (*shubhah*) by reason of their vulnerability to manipulation through editing techniques and metadata alteration. Accordingly, digital evidence does not possess the same probative force as direct eyewitness testimony for the purpose of imposing *ḥudūd* sanctions, though it may legitimately serve as an evidentiary basis in the context of *ta'zīr* (discretionary punishment) (Elmahjub, 2021).

The legal standing of digital evidence in Indonesian positive law has been substantially reinforced through the UU ITE and the National Criminal Code of 2022 (KUHP 2022), both of which recognize electronic information as a legitimate extension of admissible evidence. This legislative recognition responds to the social reality that a significant proportion of sexual offenses are now documented exclusively in digital form, rendering electronic material indispensable to investigative authorities as an initial evidentiary basis (Dodge, 2018). Law No. 1 of 2023 further affirms that electronic evidence may assist the court in forming a judicial conviction regarding the occurrence of a criminal act. A fundamental divergence therefore exists between the two legal systems: Indonesian positive law adopts a technologically open posture toward digital evidence, while Islamic law maintains a principle of heightened caution rooted in its commitment to the protection of human dignity and honor.

The research data are classified through an evidentiary category coding scheme designed to facilitate systematic comparison between the Indonesian information technology regulatory framework and the normative principles of Islamic law. The classification is presented in Table 1 below.

Table 1. Classification of Digital Evidence Categories: Indonesian Positive Law and Islamic Law

Code	Evidence Category	Status in Positive Law	Position in Islamic Law	Sharia Limitations
B-EL	Electronic Recording	Admissible evidence (UU ITE)	<i>Qarīnah Qawīyyah</i> (Strong Circumstantial Evidence)	Must be free from manipulation or editing. Must not be obtained through <i>tajassus</i> (surveillance).
B-DS	Document / Chat Log	Extension of documentary evidence	<i>Surah al-Khaṭṭ</i> (Written Communication)	Applicable only for <i>ta'zīr</i> sanctions.
B-MT	Metadata / Location Data	Supporting forensic evidence	<i>Shubhah</i> (Evidentiary Doubt)	

B-EL	Electronic Recording	Admissible evidence (UU ITE)	Qarīnah Qawīyyah (Strong Circumstantial Evidence)	Must be free from manipulation or editing.
------	-------------------------	------------------------------------	--	---

Source: Author's analysis (2024)

The coding scheme presented in Table 1 reveals that each category of digital evidence occupies a distinct and differentiated position within the two legal systems under examination. Critically, Islamic law imposes strict normative limitations on each evidentiary category in order to safeguard the privacy rights of individuals – a reflection of the Sharia's foundational commitment to the protection of human dignity (*karāmah insāniyyah*).

A central finding of this study is that the use of digital evidence in *zinā* cases is highly susceptible to conflict with the principle of *satr al-'awrah* – the Islamic obligation to conceal the moral failings and private transgressions of one's fellow Muslims (Korbatieh, 2020). The principal basis for this concern is that judicial proceedings frequently require the replay or presentation of explicit digital content, which inevitably results in the indirect dissemination of the impugned conduct to a broader audience. Historical evidence from the Islamic legal tradition indicates that the Prophet Muḥammad (peace be upon him) consistently instructed that the private transgressions of individuals be concealed, provided they did not give rise to wider public harm (Khajeh Piri, 2026). It is therefore submitted that the use of digital evidence in *zinā* proceedings must be strictly circumscribed so as to prevent such evidence from functioning as an instrument for the dissemination of moral turpitude (*fahshā'*).

The study further finds that the methods by which digital evidence is frequently obtained involve practices of *tajassus* – covert personal surveillance which is explicitly and categorically prohibited by the Qur'an (Sūrah al-Ḥujurāt, 49:12). The justification for this prohibition lies in the recognition that the protection of individual privacy constitutes a fundamental human right guaranteed by the Sharia, provided the conduct in question does not implicate threats to public security or the collective welfare. Evidence from legal practice demonstrates that recordings obtained through unlawful means such as unauthorized access to personal devices or the non-consensual interception of private communications frequently generate secondary social harms that may be more destructive than the original offense. Digital evidence obtained through unilateral violations of privacy is therefore regarded as morally and legally defective from the perspective of *fiqh jinayah*, irrespective of its forensic validity.

The research data indicate that digital evidence in *zinā* cases is more appropriately deployed as an instrument for the imposition of *ta'zīr* sanctions rather than as the evidentiary basis for *ḥudūd* punishments. The specific rationale for this position is that *ḥudūd* penalties require absolute certainty, free from even the slightest evidentiary doubt, as encapsulated in the canonical maxim *idra'ū al-ḥudūd bi al-shubuhāt*. The forensic characteristics of digital files – susceptible as they are to editing, compression, and metadata alteration – cannot be equated with the certainty afforded by the direct visual testimony of four upright witnesses. Digital evidence therefore functions, within the Islamic criminal justice framework, as an instrument enabling the judge to impose educative and disciplinary sanctions aimed at the preservation of social order.

The study further identifies significant technical challenges in verifying the authenticity of digital recordings of a sexual nature, challenges that constitute a major obstacle to their unqualified legal admissibility (Boleng & Rohman, 2025). Data compression processes and metadata can be altered in ways that allow the time, date, and location of an event to be falsified by malicious actors. Classical Islamic jurisprudence is unequivocal that any form of evidence containing an element of doubt cannot serve as the basis for a ruling that would imperil a person's life, physical integrity, or

honor. Accordingly, rigorous forensic authentication constitutes an absolute prerequisite before digital evidence may be considered by a court whether in the general or religious court system as a basis for criminal liability.

The study identifies a meaningful convergence between the UU ITE provisions protecting victims of non-consensual intimate image sharing (commonly referred to as revenge pornography) and the Islamic legal principle of the protection of honor (*ḥifẓ al-'ird*) (Dinantira, 2024). Both legal systems prohibit the dissemination of content that damages a person's reputation when motivated by vindictive intent. Sociological evidence demonstrates that intimate digital material is frequently weaponized by former partners as a means of intimidation and coercion, with devastating consequences for the professional and personal future of victims. Islamic law accordingly lends normative support to positive law measures that impose criminal liability upon the distributors of such content as an expression of the Sharia's commitment to the protection of dignity and honor.

A further finding of this study is that digital chat logs occupy a position analogous to documentary evidence in classical Islamic jurisprudence, where written communications (*kitābah*) are recognized as carrying legal force when their authenticity can be established. The evidentiary weight of such written communications is conditioned upon either the acknowledgment of authorship by the sender or technical verification of their integrity. Contemporary jurisprudential literature supports the conclusion that chat logs may legitimately function as a form of written acknowledgment (*iqrār*) one of the recognized modes of proof in Islamic criminal law provided their authenticity is technically verified and free from any form of falsification (Alias et al., 2025).

Finally, the research identifies a significant preventive dimension to the evidentiary use of digital material that is consistent with the Islamic legal principle of *sadd al-dhari'ah* the preemptive blocking of pathways to prohibited conduct. Public awareness that all private conduct is potentially subject to digital documentation creates a powerful psychological deterrent effect upon potential offenders. This deterrent function is consonant with the Sharia's objective of creating a social environment free from moral deviance through rigorous social supervision. Legal policies governing the use of digital evidence therefore serve not merely a punitive function but also an effective preventive role in the modern era.

Legal Harmonization: Juridical Legitimacy and the Strengthening of Digital Forensics

The findings of this study indicate that the recognition of digital evidence in the context of *jarīmah zinā* represents a form of adaptive legal evolution within Islamic law in response to the advances of the information age. The principal justification for this adaptive interpretation is that digital technology is capable of providing a high degree of accuracy in the documentation of legally significant events that would previously have been impossible to establish in the absence of physical witnesses (Zarmsky, 2021). This is affirmed by the Indonesian positive law framework through the UU ITE and the KUHP 2022, both of which accord electronic information formal evidentiary status. The findings of this study therefore confirm the proposition that Islamic law is inherently dynamic and possesses the jurisprudential capacity to incorporate modern instruments as means of advancing justice — provided this incorporation remains subject to rigorous normative constraints.

A critical interpretive finding of this study concerns the evidentiary repositioning of digital material — away from the status of primary proof (*bayyinah*) and toward that of strong circumstantial evidence (*qarīnah qawīyyah*). This repositioning is grounded in the principle of evidentiary caution that is foundational to Islamic criminal law, which demands absolute certainty as a precondition for the imposition of *ḥudūd* sanctions. The fact that video recordings cannot be textually equated with the testimony of four upright witnesses does not, however, render such evidence legally irrelevant; rather, it is appropriately positioned as the evidentiary basis for the imposition of *ta'zīr* sanctions. The use of digital evidence in the courtroom thus represents a coherent

middle path between the imperatives of legal modernity and faithful adherence to classical Sharia procedure.

A deeper interpretive engagement with the dimension of privacy reveals that the implementation of digital evidence must remain subject to the principle of *satr al-'awrah* the Islamic obligation to conceal moral failings. The logical basis for this constraint is that sexual offenses are, by their very nature, private in character, and the public disclosure of their details through digital evidence risks causing damage to the dignity of individuals that may exceed the harm of the punishment itself. This position is reinforced within Islamic legal practice by the categorical prohibition of *tajassus* the active surveillance of others' private conduct for non-urgent purposes (Gustati, 2025). The use of digital evidence in *zinā* proceedings is therefore best understood as a form of legal *ijtihad* that must be bounded by moral considerations so as to prevent the generation of broader social harm (*fitnah*).

The implications of these findings provide a foundation of legitimacy for judges within the court system to deploy electronic evidence without transgressing Sharia ethics. Their practical significance lies in the potential to dispel the perception that the use of digital recordings is inherently incompatible with the Islamic value of concealing moral failings – clarifying that the purpose of such evidence is the ascertainment of material truth rather than the public exposure of shame (Siregar et al., 2025). Empirical evidence suggests that public confidence in the enforcement of law in cases of sexual offenses increases when citizens understand that technology is being deployed responsibly and within a framework that protects the privacy of all parties. The practical implication is therefore the creation of a harmonious relationship between digital forensic procedure and the preservation of human dignity within the judicial system.

The findings of this study also carry significant implications for the strengthening of digital forensics as a strategic partner in contemporary Islamic criminal adjudication. The study provides theoretical justification for the proposition that the validation of electronic data constitutes a modern expression of the quality of 'reliability' and 'integrity' that must characterize admissible evidence in Islamic law. Judicial decisions from 2022 reveal an emerging trend in which the integrity of metadata has become a decisive criterion in determining whether digital evidence is admitted or excluded by the court. As a consequence, law enforcement authorities now possess an intellectual and jurisprudential basis for advancing justice grounded not merely in oral testimony but also in scientifically rigorous and accurate data.

The longer-term implication of this study is to encourage a transformation in Islamic law curricula so as to render future Islamic legal scholars more responsive to scientific and technological evidence. The principal justification for this curricular reform is to equip future Islamic law academics with the competencies necessary to interpret classical *jinayah* texts contextually in the face of an increasingly digital evidentiary landscape. The recognition that digital evidence can be meaningfully associated with the jurisprudential concept of *qarīnah* opens a productive new space for scholarly discussion regarding the contours of a 'Contemporary Islamic Law of Evidence' (*Fiqh al-Ithbāt al-Mu'āṣir*) that is both comprehensive and responsive to modern realities. This study thus contributes to the evolution of Islamic legal thought in Indonesia, ensuring its continuing relevance as a framework for addressing legal challenges in the information era.

The finding concerning chat logs as documentary evidence carries implications for the expansion of the classical jurisprudential concept of *kitābah* (written communication). In the digital era, written communication through instant messaging has largely supplanted the role of physical correspondence in everyday human interaction (Venter, 2019). Scholarly literature affirms that written communication whose authenticity can be technically verified carries legally binding force upon its author. This interpretive synchronization accordingly provides legal certainty to the effect that the digital trail of illicit communication may serve as a legitimate basis for criminal liability – subject always to the condition of technically verified authenticity.

The discussion further emphasizes that the in camera use of digital evidence is consistent with the objective of protecting victims of non-consensual intimate image sharing. This protective rationale is urgent given that the non-consensual dissemination of intimate content is frequently employed as a tool of intimidation that destroys the future of victims (Yadav, 2023). Islamic law provides normative support for firm legal action against the distributors of such content in accordance with the principle of the protection of honor (*ḥifẓ al-'ird*). The legality of digital evidence in this study therefore serves not merely the punitive objective of sanctioning perpetrators of *zinā*, but also the protective objective of shielding individuals from inhumane digital exploitation.

The study further emphasizes that the effectiveness of digital evidence is critically dependent upon the willingness of judges to exercise a principled judicial discretion oriented toward the public good (*maṣlaḥah*). The foundational justification for this emphasis is that judges possess the authority to exclude evidence whose manner of acquisition violates Sharia ethics for example, recordings obtained through the unlawful interception of private communications in a manner that constitutes *tajassus*. Comparative data indicate that a judicially wise court will prioritize social stability and the protection of privacy over the mere formal satisfaction of evidentiary requirements. The role of the judge as the executor of *ta'zīr* discretion therefore emerges as the pivotal institutional mechanism for moderating the use of digital technology in the courtroom.

This discussion may be summarized in the proposition that the synchronization of technological advances with the principles of Islamic criminal law represents a manifestation of progressive yet deeply religious jurisprudence. The essence of Islamic law is the realization of a civilized and humane justice one that refuses to normalize the dissemination of moral turpitude through the public exposure of intimate evidence (Elmahjub, 2021). The research data confirm that the integration of digital forensics with the principle of *satr al-'awrah* provides a coherent and principled response to the challenges of the modern era without sacrificing the foundational values of the Sharia. The comparative findings of this study accordingly yield a strong recommendation to law enforcement authorities to optimize digital technology as an instrument for the protection of public morality, within a framework that is simultaneously legally rigorous, ethically sensitive, and constitutionally sound.

Limitations and Directions for Future Research

The principal limitation of this study lies in its predominantly normative and doctrinal orientation, which has necessarily restricted the scope of the analysis to the examination of legal texts and jurisprudential literature. As such, the study does not engage with the more complex technical dimensions of digital forensics as they have continued to evolve beyond 2022, nor does it incorporate empirical observations of judicial behavior in practice. This limitation reflects the deliberate design of the study, which prioritizes the analysis of legal legitimacy and Sharia ethics over the technical dimensions of digital data manipulation. Notwithstanding this limitation, the theoretical findings produced by the study constitute an important contribution to the development of contemporary Islamic criminal law discourse.

Future research is recommended to adopt a juridical-empirical methodology that evaluates the practical effectiveness of in camera proceedings in protecting the confidentiality of digital evidence in the courtroom, with a view to assessing the degree to which the principle of *satr al-'awrah* is actually implemented in judicial practice. The urgency of such research lies in the need to prevent the public disclosure of intimate material that so frequently triggers the phenomenon of 'digital mob justice' the extra-judicial punishment of accused individuals through the viral online dissemination of intimate recordings, with devastating consequences for their dignity and future prospects. Fieldwork comprising interviews with legal practitioners and observational studies of court proceedings would provide the concrete empirical data necessary to measure the degree of synchronization between digital forensic procedure and Sharia ethics. Future research should

therefore aspire to formulate operational standard procedures for digital investigation that pursue not only legal certainty but also the robust protection of individual privacy in the spirit of the Sharia.

Conclusion

This study concludes that digital evidence in the adjudication of *jarimah zinā* possesses formal legal validity within the Indonesian positive law framework; however, its position within Islamic law is supplementary in nature functioning as *qarīnah* (circumstantial evidence or legal indicator) rather than as *bayyinah* (primary proof). The fundamental basis for this determination is the inherent susceptibility of digital data to technical manipulation, which renders it incapable of satisfying the standard of absolute certainty required for the imposition of *ḥudūd* punishments a standard operationalized through the requirement of four upright male witnesses. The legislative framework established by the UU ITE and the KUHP 2022 confirms that electronic information is recognized as a legitimate extension of admissible evidence for the purpose of establishing material truth in judicial proceedings. Accordingly, digital evidence may constitute a robust legal foundation for the imposition of *ta'zīr* sanctions of an educative and preventive character, provided the requisite conditions of authenticity and lawful acquisition are satisfied.

The use of digital evidence in cases of sexual offenses is subject to strict ethical constraints arising from the principle of *satr al-'awrah*, which demands a careful balance between the imperatives of law enforcement and the protection of individual honor and dignity. The primary justification for these constraints is the imperative to prevent the occurrence of social *fitnah* (harm) and the practice of *tajassus* (covert surveillance), both of which are categorically prohibited in Islamic law particularly in respect of offenses that are private in nature. The research findings demonstrate that the deployment of digital recordings without rigorous procedural safeguards and the protection afforded by in camera proceedings carries a significant risk of violating the right to privacy and damaging human dignity (*ḥifẓ al-'ird*). It is therefore concluded that the legality of digital evidence must be accompanied by a principled ethics of concealment (*satr*), whereby access to intimate content is restricted exclusively to judicial purposes and is categorically excluded from public consumption.

Taken in its entirety, the integration of advances in digital forensics with the normative values of Islamic criminal law (*fiqh jinayah*) represents a manifestation of progressive yet authentically religious legal transformation. The significance of this integration lies in the capacity of Islamic law to remain relevant and responsive to contemporary challenges including the phenomenon of non-consensual intimate image sharing (revenge pornography) while consistently upholding the supreme value of human dignity. The evidence of this synchronization is visible in the judicial role of the *hakim*, who exercises principled discretion to exclude digital evidence obtained through unlawful or ethically impermissible means. As the definitive conclusion of this study, it is affirmed that the use of digital evidence is an inescapable feature of contemporary legal practice, one that must be governed by the principles of civilized justice (*al-'adālah al-mutaḥaddirah*) in order to realize the public good (*maṣlahah al-'āmmah*) without sacrificing the dignity of the individual. In this sense, the principle of *satr al-'awrah* is not a relic of classical jurisprudence, but a living normative value one that must continue to serve as the ethical compass of Islamic criminal adjudication in the digital age.

Acknowledgement

Thanks are due to all those who have helped in the process of researching and writing this article.

Conflict of Interest

This article has no conflicts of interest.

References

admin. (2025). POLRI's Response to Cybercrime: Strategies and Tools. *Berita Terpercaya*.

- Ahmad, H. M. (2021). Re-Assessing the Evidentiary Threshold for *Zinā'* in Islamic Criminal Law: A De Facto Exemption Proposal. *Muslim World Journal of Human Rights*, 18(1), 103–132.
- Alias, M. A. A., Wan Ismail, W. A. F., Baharuddin, A. S., Hashim, H., & Tuan Ibrahim, T. M. (2025). *Strengthening the Integrity of Digital Evidence in Syariah Criminal Proceedings: A Forensic–Legal Analysis of the Chain of Custody (CoC)*.
- Boleng, T. K., & Rohman, A. N. (2025). Regulatory Gaps and Legal Enforcement Challenges on Deepfake Pornography as a Form of Digital Sexual Violence in Indonesia. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, 3(6), 10068–10080.
- Brechin, J. (2013). A Study of the Use of Sharia Law in Religious Arbitration in the United Kingdom and the Concerns That This Raises for Human Rights. *Ecclesiastical Law Journal*, 15(3), 293–315. <https://doi.org/10.1017/S0956618X13000434>
- Darmawansyah, A., Dwiarnanto, A., & Satriyawan, I. P. (2025). A Juridical Review of Cybercrime and Defamation under Indonesia's Law No. 1 of 2024 on Electronic Information and Transactions. *Journal of Law and Humanity Studies*, 2(2), 55–61.
- Dinantira, Y. P. (2024). Perlindungan Hukum Korban Revenge Porn Dalam Undang-Undang Tindak Pidana Kekerasan Seksual (UU No. 12 Tahun 2022). *JUSTICES: Journal of Law*, 3(2), 121–133.
- Dodge, A. (2018). The digital witness: The role of digital evidence in criminal justice responses to sexual violence. *Feminist Theory*, 19(3), 303–321.
- Elmahjub, E. (2021). Islamic Jurisprudence as an Ethical Discourse: An Enquiry into the Nature of Moral Reasoning in Islamic Legal Theory. *Oxford Journal of Law and Religion*, 10(1), 16–42. <https://doi.org/10.1093/ojlr/rwaa023>
- Fadhli, A., & Warman, A. B. (2021). 'Alasan Khawatir' Pada Penetapan Hukum Dispensasi Kawin Di Pengadilan Agama Batusangkar 'Reasons for Concern' on Marriage Dispensation Decisions in Batusangkar Religious Court. *Al-Ahwal*, 14(2), 146–158. <https://doi.org/10.14421/ahwal.2021.14203>
- Fawwas, I. (2025). An Analysis of Criminal Sanctions for Adultery Under Islamic Law and the National Legal System: A Study of Legal Pluralism in Indonesia. *SYARIAT: Akhwal Syaksyah, Jinayah, Siyasa and Muamalah*, 2(1), 1–7.
- Goodman, M. (2015). *Future crimes: Inside the digital underground and the battle for our connected world*. Random House.
- Gustati, G. D. (2025). *Tajassus and the Spread of Disgrace in Islamic Perspective*.
- Hand, M. (2016). Persistent traces, potential memories: Smartphones and the negotiation of visual, locative, and textual data in personal life. *Convergence*, 22(3), 269–286.
- Ibrahim, T. M. F. H. T., Muhamad, N. H. N., Alias, M. A. A., & Baharuddin, A. S. (2026). The Role of Digital Forensics as *Qarinah Muasirah* in Proving Cyber Offences Under Malaysian Islamic Evidence Law. *Al-Istinbath: Jurnal Hukum Islam*, 11(1), 19–39.
- Kamali, M. H. (2020). *Actualization (Taf'il) of the Higher Purposes (Maqasid) of Shariah*. International Institute of Advanced Islamic Studies (IAIS).
- Khajeh Piri, A. (2026). *Islam and the Rights of Privacy Territory*. Ahlul Bayt Digital Islamic Library

Project.

- Korbatieh, S. (2020). Evidence rules in Sharia and the impact of modern technology and DNA testing. *Australian Journal of Islamic Studies*, 5(3), 4–29.
- Majeed, N., Hilal, A., & Ilyas, R. (2023). From evidential data to evidence: production, admission and evaluation of evidential data in the judicial process of proof. *Pakistan Journal of Social Research*, 5(02), 955–965.
- Nasution, K. (2005). Women’s Right in the Islamic Family Law of Indonesia. *Unisia*, 28(56), 192–204. <https://doi.org/10.20885/unisia.vol28.iss56.art10>
- Prayudati, Y. M., Trisna, W., & Desiandri, Y. S. (2025). ANALYSIS OF THE THREAT OF THE SPREAD OF INTIMATE CONTENT NON CONSENSUAL IN VIOLENCE GENDER BASED ONLINE. *SIBATIK JOURNAL: Jurnal Ilmiah Bidang Sosial, Ekonomi, Budaya, Teknologi, Dan Pendidikan*, 4(8), 1911–1924.
- Siregar, F. A., Yulis, S., & Masyitah, M. (2025). Legal Certainty on the Dissemination of Defamatory Content on Social Media: A Case Analysis of a Flogging Procession Recording in Aceh. *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan Dan Ekonomi Islam*, 17(1), 239–253.
- Smith, S. C. (2011). *Crowdsourcing sharia: Digital fiqh and changing discourses of textual authority, individual reason, and social coercion*. Georgetown University.
- Suryal, A. (2024). *RETRACTED: Leveraging metadata in social media forensic investigations: Unravelling digital clues-A survey study*. Elsevier.
- Triwahyuni, D., Anggraeni, S., Iqbal, M., Fadilla, N. T., & Mokoginta, F. (2025). Strengthening Indonesia’s Cybersecurity Through Cooperation in The ASEAN Regional Forum. *Proceedings of the 8th International Conference on Business, Economics, Social Sciences, and Humanities-Humanities and Social Sciences Track (ICOBEST-HSS 2025)*, 131.
- Venter, E. (2019). Challenges for meaningful interpersonal communication in a digital era. *HTS: Theological Studies*, 75(1), 1–6.
- Wall, D. S. (2024). *Cybercrime: The transformation of crime in the information age*. John Wiley & Sons.
- Yadav, V. (2023). Tackling non-consensual dissemination of intimate images in India’s contemporary legal framework. *International Annals of Criminology*, 61(3–4), 355–383.
- Zarmsky, S. (2021). Why seeing should not always be believing: Considerations regarding the use of Digital reconstruction Technology in International Law. *Journal of International Criminal Justice*, 19(1), 213–225.