© SEP 2026 | IRE Journals | Volume 10 Issue 3 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I3-1722738

A Comparative Legal Analysis of Deepfake Evidence in Bangladesh

MD SHAMSAD HOSSAIN
Daffodil International University, Dhaka, Bangladesh

Abstract- ***Deepfake technology, which involves the creation of synthetic audio, video, and image content through artificial intelligence to portray real individuals engaging in actions or speech that never occurred, poses a significant evidentiary challenge that the traditional digital-evidence doctrine is not equipped to handle. Bangladeshi courts are increasingly dependent on electronic records; however, the Evidence Act of 1872, even after its amendment in 2022, lacks provisions addressing AI-generated content, authentication standards specific to synthetic media, and qualification frameworks for experts required to identify such content. This study explores whether Bangladesh's evidentiary framework is sufficient to meet this challenge and, if not, what reforms are necessary to bridge this gap. Utilizing doctrinal and comparative methods, this paper analyzes the statutory and case law treatment of digital evidence in Bangladesh in comparison with the approaches adopted in the United Kingdom and Malaysia. These jurisdictions were chosen for their shared evidentiary heritage and differing regulatory styles: judicial reliability review in the UK and codified statutory presumption in Malaysia. The analysis reveals that none of the jurisdictions reviewed have established a deepfake-specific evidentiary regime, but each provides transferable doctrinal elements: Malaysia's structured certification mechanism, the UK's substantive reliability inquiry, and an emerging legislative trend, as seen in the Cyber Security Act of 2026 in Bangladesh, which considers the direct regulation of AI-generated content. This study proposes a sequential authentication framework and a series of legislative, institutional, and procedural reforms designed to be integrated within Bangladesh's current judicial infrastructure rather than relying on it alone.***

Keywords: Deepfake evidence, artificial intelligence, digital evidence authentication, Evidence Act 1872, admissibility, comparative evidence law, digital forensics.

I. INTRODUCTION

1.1 Background and Context

The reliability of evidence serves as a standard by which courts evaluate factual claims. In the past, this assessment was limited to what could be physically examined: witness demeanor, document provenance, or object condition. Over the past three decades, the proliferation of electronic records has broadened the categories of evidence available to courts; however, it has not altered the fundamental assumption that a digital file, despite its imperfections, corresponds to an actual event. However, deepfake technology challenges this assumption. A deepfake is an audio, video, or image content generated or manipulated by artificial intelligence to portray a real person engaging in actions or speech that did not occur, with sufficient realism to evade casual detection (Chesney & Citron, 2019). Initially emerging in 2014 as a research artifact of the Generative Adversarial Network (GAN) architecture (Goodfellow et al., 2014), this technology is now accessible through consumer-grade tools, enabling ordinary litigants, not just well-resourced institutional actors, to fabricate convincing evidence. Bangladesh provides a pertinent context for examining these issues. Its courts are increasingly dealing with digital evidence in cybercrime, commercial fraud, family disputes involving social media communications, and online defamation claims. The Evidence Act, 1872 (Amendment 2022) introduced Sections 65A and 65B to regulate the admissibility of electronic records in court. This amendment represents a necessary modernization of a nineteenth-century statute; however, it was drafted on the assumption that a digital file is either authentic or altered from an authentic original. It does not account for recordings without authentic originals. Bangladesh is not alone in this regard; the United Kingdom and Malaysia, which share an evidentiary lineage with Bangladesh through common law and, in Malaysia's case, a nearly identical statutory drafting tradition, have also failed to enact deepfake-specific evidentiary rules. However, each has developed a partial response: the United Kingdom through a judicially administered

reliability review and Malaysia through codified certification, offering points of comparison for jurisdictions at earlier stages of addressing this challenge.

1.2 Statement of the Problem

When a party tenders a digital recording as evidence, the court must determine whether it depicts what it purports to depict. Historically, courts rarely considered wholesale fabrication; disputes centered on relevance, hearsay, or privilege, with a recording's underlying authenticity largely assumed. Deepfake technology displaces that assumption by making convincing, wholly fabricated content cheap to produce and difficult to detect without specialized analyses. The Evidence Act of 1872 does not define deepfakes or AI-generated content, set any rules for how to check the authenticity of synthetic media, or give any way to order a forensic examination when manipulation is suspected. Sections 65A and 65B presuppose that a digital file is either genuine or edited from a genuine original; they do not address content fabricated without an authentic predicate. Sections 45 and 45A permit expert opinion evidence but prescribe no qualification standards for the experts offering it. The result is a structural gap: courts have the statutory authority to hear expert testimony on deepfake authenticity but no statutory guidance on how to evaluate it.

1.3 Research Gap, Significance, and Thesis

Existing scholarship on deepfake evidence concentrates on jurisdictions—principally the United States and the European Union—with developed forensic infrastructure and an established body of digital-evidence case law. Comparatively little attention has been paid to developing common law systems, where forensic capacity is more constrained, and statutory reform proceeds more slowly. This study addresses this gap by grounding its analysis in what Bangladesh's existing judicial and forensic infrastructure can realistically absorb, rather than treating foreign frameworks as templates for direct transplantation. The stakes are not abstract: a wrongful conviction secured on a fabricated confession recording or a civil judgment obtained through a manipulated settlement recording becomes increasingly probable as deepfake tools become more accessible and harder to detect. The converse risk—courts treating all contested digital evidence with reflexive suspicion—would be equally damaging to a system of justice that now depends substantially on electronic records. Therefore, the objective of the reform is calibration, not exclusion.

The central thesis advanced in this paper is that notwithstanding the 2022 amendments, Bangladesh's evidentiary framework remains structurally unequipped to address deepfake evidence because it conflates the integrity of a digital file with the authenticity of its content—two inquiries that deepfake technology, for the first time, definitively separates. A comparative analysis of the United Kingdom and Malaysia shows that neither jurisdiction has fully resolved this separation; however, targeted statutory provisions, a substantive reliability standard for authentication, and accredited expert qualification regimes together offer a workable template that Bangladesh can adapt without wholesale institutional reconstruction.

1.4 Objectives and Research Questions

This study aims to examine the technical characteristics of deepfake technology relevant to legal analysis, identify the structural gaps in Bangladesh's evidentiary architecture, assess the available methods of detection, authentication, and admissibility, compare the approaches taken in the United Kingdom and Malaysia, and propose legislative, institutional, and procedural reforms suited to Bangladesh's circumstances. These objectives are pursued through five research questions: What characteristics distinguish deepfake content from conventional digital manipulation in ways that matter for evidentiary doctrine? Does the Evidence Act of 1872, as amended in 2022, provide adequate safeguards against deepfake evidence? What technical and procedural mechanisms are available to authenticate or detect deepfake content in judicial proceedings? How have the United Kingdom and Malaysia addressed the authentication of AI-generated or computer-generated evidence, and what can Bangladesh draw from each? What reforms would most effectively strengthen Bangladesh's evidentiary response within realistic institutional constraints?

1.5 Methodology, Scope, and Limitations

This study employs doctrinal and comparative legal methods to achieve its objectives. Primary sources comprise the Evidence Act, 1872, and its 2022 amendments; the Cyber Security Act, 2026 (CSA 2026); and the corresponding statutory frameworks of the United Kingdom and Malaysia, supplemented by reported judicial decisions, where available. Secondary sources included peer-reviewed legal scholarship, digital forensic literature, and institutional reports. The United Kingdom and Malaysia were selected because both share a common law evidentiary heritage with Bangladesh—Malaysia's Evidence Act 1950 is drafted in close structural parallel to Bangladesh's own, while English authentication doctrine has historically informed judicial practice throughout the wider common law world—while differing in the specificity of their statutory response to computer-generated evidence and the maturity of their forensic infrastructure. The comparative method is employed analytically to identify principles capable of adaptation to Bangladesh's institutional and resource context, not to recommend wholesale importation of foreign rules.

This study addresses deepfake evidence in civil and criminal proceedings. It does not undertake an empirical evaluation of specific detection technologies or original empirical research on judicial practice, both of which lie outside doctrinal and comparative studies. Given the pace of development in generative AI, some technical descriptions offered here may quickly become outdated; accordingly, the analysis emphasizes legal principles likely to retain relevance independent of the specific technology in use at any given time. Defamation and privacy implications are addressed only insofar as they bear on the remedies arising from litigation.

II. THE CONCEPTUAL AND TECHNICAL FRAMEWORK OF DEEPFAKES

2.1 Definition and Technical Development

The term "deepfake" combines "deep learning," a class of machine learning that processes data through multi-layered neural networks, with "fake," denoting fabricated or altered content. Chesney and Citron (2019) define deepfakes as AI-generated audio or video that is realistic enough to be mistaken for genuine recordings of real people. The operative term of this definition, "realistic-seeming," captures the doctrinally significant feature of the technology: detection requires technical analysis rather than unaided perception.

The decisive technical development was Goodfellow et al.'s (2014) introduction of Generative Adversarial Networks, in which a generator network produces synthetic content while a discriminator network attempts to distinguish it from genuine examples, with iterative competition between the two progressively improving the generator's output until it reliably defeats the discriminator. Subsequent developments — autoencoder-based face-swapping, diffusion models capable of producing photorealistic still images, and large language models capable of replicating an individual's written or spoken idiom — have extended this capability across every major category of evidentiary content: video, audio, image, and text (Russell & Norvig, 2021). The practical consequence for evidentiary doctrine is that the artifacts historically used to detect manipulation—audible splicing, visible pixelation, and inconsistent lighting—are diminishing with each successive generation of generative tools, while detection increasingly requires forensic analysis beyond the capacity of an unaided observer, including a trained observer (Farid, 2022).

2.2 Evidentiary Significance of the Authenticity–Integrity Distinction

The doctrinal significance of deepfake technology lies in the distinction that the conventional digital evidence doctrine does not need to draw with precision: the difference between the integrity of a file and the authenticity of its content. Established authentication procedures—hash verification, metadata preservation, and chain-of-custody documentation—are designed to establish integrity, that is, that a file has not been altered since it was collected. They do not, and cannot, establish that a file's content corresponds to a real event. A deepfake may have impeccable provenance and an unbroken chain of custody from the moment it was created

while depicting nothing that ever occurred. As Mason and Seng (2021) observe, the chain-of-custody doctrine answers the question of whether evidence remained intact after collection, not the antecedent question of whether it was authentic at the moment of its creation. Therefore, authentication standards calibrated to the deepfake era must reach the reality of a file's content, not merely the integrity of its handling—a shift those existing evidentiary frameworks, including Bangladesh's, have not yet made.

It is important to note that deepfake technology is not inherently harmful; legitimate applications include film restoration, assistive voice synthesis for individuals who have lost the capacity for natural speech, and historical or educational reconstructions. The evidentiary concern is not with the technology itself but with its use to deceive a tribunal of fact, a distinction that should inform the proportionality of any regulatory response to AI-generated evidence. Measures targeting deceptive use are preferable to those restricting the underlying technology.

III. LITERATURE REVIEW

Scholarly engagement with deepfake evidence has developed along two largely separate paths. First, exemplified by Chesney and Citron (2019) and the subsequent literature it generated, deepfakes are treated principally as a threat to democratic discourse, privacy, and national security, with evidentiary admissibility addressed as a subsidiary concern. The second, more technical track, exemplified by Farid (2022) and the forensic science literature on which this study draws, focuses on detection methodology—the technical means of distinguishing synthetic from genuine media—with comparatively limited engagement with how courts should weigh the resulting forensic findings as a matter of evidentiary doctrine.

Neither track has produced a developed body of scholarship addressing the specific evidentiary architecture of jurisdictions outside the United States and the European Union. Existing treatments of digital evidence authentication in common law systems—including the comparative work of Mason and Seng (2021) on electronic evidence across multiple jurisdictions and the doctrinal analysis offered by Roberts and Zuckerman (2022) on criminal evidence in England and Wales—predate the point at which deepfake-specific fact patterns became a live concern for evidentiary doctrine and accordingly treat AI-generated content, where addressed, as an extension of conventional digital manipulation rather than as a categorically distinct problem.

Scholarship specific to Bangladesh's evidentiary frameworks remains limited. Rahman and Naser (2023) examine the admissibility of electronic evidence following the 2022 amendments to the Evidence Act but do not address AI-generated content specifically, reflecting the relatively recent emergence of deepfake technology as a practical concern for Bangladeshi courts rather than any settled judgment that the issue is immaterial. The comparative literature on Malaysia's Section 90A framework, including Ahmad Shariff et al. (2021), similarly predates sustained scholarly attention to deepfakes, although the structural features of the Malaysian framework it analyses remain directly relevant to the authentication problem deepfakes present.

This paper situates itself at the intersection of these tracks: it treats deepfake evidence as a distinct evidentiary category requiring a doctrinal response, draws on the technical detection literature to inform that response, and extends the comparative analysis of digital evidence authentication to a jurisdiction—Bangladesh—that has not yet been the subject of sustained scholarly treatment of this specific question. This also incorporates legislative developments occurring in 2025 and 2026, including Bangladesh's CSA 2026.

and the United Kingdom's expansion of deepfake-specific criminal offenses, which postdate the existing literature and directly bear on the comparative claims advanced here.

IV. THE LEGAL FRAMEWORK IN BANGLADESH

4.1 The Evidence Act, 1872, and the 2022 Amendment

The Evidence Act of 1872 remains the foundational statute governing the admissibility and evaluation of evidence in Bangladesh's courts. Enacted under colonial administration and drafted in close parallel with the Indian Evidence Act of the same year, the Act's core principles — relevance, the exclusion of hearsay, and the evaluative treatment of expert opinion — remain doctrinally sound in a digital context. The deficiency is not the age of the Act but its silence on what artificial intelligence can now do to digital files.

The 2022 amendment introduced Sections 65A and 65B, establishing electronic records as admissible evidence and creating a certification mechanism by which a responsible official's signed certificate can support admission without further verification, which is structurally similar to the certification procedure formerly available under Section 69 of the UK's Police and Criminal Evidence Act 1984 (since repealed) and to the certification requirement under Malaysia's Evidence Act 1950. This mechanism serves a legitimate efficiency function: requiring full forensic proof of provenance for every electronic record would be administratively unworkable. Its limitation in the deepfake context is structural rather than incidental: a certifying official can attest that a system functioned as intended and was not tampered with after capture, but cannot attest to whether the content depicted ever corresponded to a real event or not. A video can be certified, entirely accurately, as retrieved from a properly functioning server through an unbroken chain of custody, while being wholly fabricated from inception. Section 65B authenticates handling, not reality, and a deepfake satisfying every condition specified in the section remains a deepfake.

4.2 Admissibility, Weight, and the Locus of Contestation

Section 3 broadly defines "evidence" to encompass deepfake audio-visual material without difficulty, as the definition imposes no independent authenticity requirement at the admissibility stage. Authenticity operates as a factor bearing on weight rather than admissibility, except where a specific exclusionary rule applies. The practical consequence is that a deepfake will, in most cases, clear the admissibility threshold without difficulty, with substantive contest deferred to the evaluative stage. This allocation is not objectionable in itself — admissibility thresholds calibrated to exclude all contested digital evidence would be unworkable — but it places considerable weight on the evaluative stage being equipped to conduct a rigorous inquiry, which sections 45 and 45A do not currently ensure.

4.3 Expert Evidence under Sections 45 and 45A

Sections 45 and 45A permit courts to receive opinion evidence on questions of science, art, or foreign law, providing the doctrinal vehicle through which digital forensic expertise would ordinarily enter deepfake-related proceedings. However, the Act prescribes no qualification standard for digital forensics experts and no methodological benchmark against which competing expert opinions can be assessed. Bangladesh has no equivalent to the reliability-screening function performed in United States federal practice by the Daubert standard, under which courts assess the testability, peer review, and known error rate of an expert's methodology before admitting the resulting opinion. In its absence, Bangladeshi courts are required to evaluate the reliability of a deepfake-detection methodology without a structured framework for doing so, which is a significant gap given that forensic deepfake detection methodologies vary considerably in maturity and validation, and that an erroneous assessment of reliability at this stage will rarely be correctable on the available record.

4.4 The Cyber Security Act, 2026 and Subsequent Legislative Activity

The statutory landscape surrounding digital offences in Bangladesh has changed significantly since the 2022 amendments. The Cyber Security Act, 2023, was repealed on May 21, 2025, and replaced by the Cyber Security Act, 2026, promulgated amid sustained domestic and international criticism that the 2023 Act's speech-related provisions had been used to suppress legitimate expression (Prothom Alo, 2025). The Cyber Security Act is significant because it introduces, for the first time in South Asia, offences

specifically addressing the misuse of artificial intelligence, including the use of AI systems to gain unauthorized access to critical information infrastructure and the generation of AI-produced content for blackmail, sextortion, or harassment (Lexplosion Solutions, 2025).

This requires a qualification of the claim, advanced in earlier treatments of Bangladesh's cyber legislation, that domestic law contains no provision addressing AI-generated content. The Cyber Security Act does address certain AI-facilitated offences. However, it does not address the evidentiary status of AI-generated content in litigation, which remains governed exclusively by the Evidence Act framework discussed above. The Ordinance criminalizes particular harmful uses of AI-generated material without establishing any authentication standard, certification requirement, or expert qualification regime applicable when such material is offered as evidence. A prosecution under the Ordinance for the malicious creation of AI-generated content is a different proceeding, governed by different doctrinal questions, from a trial in which AI-generated content is tendered as the evidentiary basis for another claim.

The legislative trajectory is, in any event, continuing. In June 2026, the Home Minister informed Parliament that the government had initiated further amendments to the ordinance, specifically targeting the removal of harmful AI-generated content from social media platforms, including updated definitions of misinformation and defamation and an expedited content-removal mechanism (TBS News, 2026). This indicates active legislative recognition that the existing framework requires extension to address AI-generated content more directly — an extension that this paper argues should extend to the evidentiary, not only the platform regulation, dimension of the problem.

4.5 Judicial Treatment of Digital Evidence

Bangladeshi courts have not yet produced reported case law addressing deepfake evidence specifically, a fact better explained by the recency of the technology's emergence as a practical litigation concern than by any settled judicial view that the issue is unimportant. Courts have engaged with digital evidence authenticity in adjacent contexts — disputed CCTV footage, contested electronic communications, and social media content — relying on the section 65B certification mechanism and, where authenticity is disputed, on expert opinion under sections 45 and 45A. Whether this approach, developed for conventional digital manipulation disputes, will prove adequate for deepfake-specific fact patterns is the central doubt this paper seeks to substantiate.

4.6 Structural Gaps and the Case for Reform

Several structural deficiencies follow from the above analysis. There is no statutory definition of deepfakes or AI-generated content in the evidentiary framework. There is no mandatory disclosure or certification requirement specific to digital audio-visual evidence that would trigger an authentication inquiry automatically, rather than only when a party affirmatively raises the issue of authentication. The Evidence Act confers no express power to order a pre-admission forensic examination of contested digital evidence; any such order would presumably rest on inherent jurisdiction, the scope of which in this context is untested. No judicial protocol specifically addresses deepfake-related disputes, and the digital forensic capacity within Bangladesh's law enforcement and judicial support infrastructure remains limited relative to the technical demands of deepfake detection.

These gaps have consequences beyond the immediate cases in which they arise. As digital evidence becomes more prevalent in Bangladeshi litigation and deepfake generation tools become more accessible, the probability of fabricated evidence reaching the court rises in tandem. A single high-profile case in which a wrongful conviction or fraudulent civil judgment is later attributed to deepfake evidence would damage confidence in the administration of justice substantially more than the legislative effort required to prevent it. The Ordinance's recent extension to AI-facilitated offences and the further amendments under active consideration as of mid-2026 demonstrate that anticipatory legislative action in this space is institutionally and politically feasible; the evidentiary dimension addressed in this paper is a

logical extension of a reform process already underway.

V. COMPARATIVE ANALYSIS: THE UNITED KINGDOM AND MALAYSIA

5.1 The Function of Comparison

In this context, comparative analysis serves an analytical rather than a prescriptive purpose. Legal transplantation fails when it disregards the institutional, cultural, and resource constraints of the receiving system. The value of examining the United Kingdom and Malaysia lies not in treating either as a model for direct replication but in the range of structural problems each has encountered and the divergent solutions each has attempted. Bangladesh shares an evidentiary heritage with both: the Evidence Act itself is a colonial-era inheritance common to all three systems, while differing substantially from each in terms of institutional resourcing and the pace of technological adoption.

5.2 The United Kingdom

5.2.1 Statutory and Doctrinal Framework

English evidence law applicable to digital material is distributed across several statutes: the Police and Criminal Evidence Act 1984, the Computer Misuse Act 1990, the Criminal Justice Act 2003, and the Civil Evidence Act 1995, supplemented by the Criminal Procedure Rules 2020 and an extensive body of case law. The absence of a single consolidating statute is sometimes characterized as a weakness, but the flexibility inherent in common law adjudication has allowed courts to extend established authentication principles to new categories of digital evidence without legislative intervention for each technological development.

The doctrinally significant feature of the English approach is its orientation toward substantive reliability, rather than procedural certification. While Malaysian and Bangladeshi law rely on statutory presumptions triggered by certification, English courts assess digital evidence by reference to what can actually be established about its provenance, handling, and internal consistency. This orientation is reinforced by the Law Commission's 1997 report on evidence in criminal proceedings and by guidance issued by the Forensic Science Regulator, which, while not binding in the strict sense, is treated by courts as authoritative in practice, producing a de facto requirement of forensic validation whenever digital evidence is genuinely contested, conditional on a party actually raising the authenticity challenge in the first place.

English courts also apply a rigorous gatekeeping function to expert evidence: under the Criminal Procedure Rules and supporting case law, an expert witness must demonstrate relevant expertise, ground their opinion in a reliable methodology, and assist the court rather than advocate for a party's position. This framework provides a structured mechanism for testing expert evidence on deepfake authenticity, although English courts have not yet produced a landmark decision directly addressing deepfake-specific authentication (Mason and Seng, 2021).

5.2.2 Deepfake-Specific Legislative Developments

The United Kingdom has moved further than either Bangladesh or Malaysia toward direct legislative engagement with deepfakes, although its provisions address the harmful use of the technology rather than its evidentiary status in litigation. Section 188 of the Online Safety Act 2023 inserted sections 66B to 66D into the Sexual Offences Act 2003, criminalizing the sharing or threatened sharing of intimate images without consent in terms broad enough to capture images that merely "appear to show" a person in an intimate state — a formulation deliberately drafted to encompass deepfake content (5KBW, 2025). This addressed the distribution of non-consensual intimate deepfakes but, on its original terms, left the creation of such material unaddressed where it was never shared. The Data (Use and Access) Act 2025 closed this gap by creating a distinct offence of creating or requesting the creation of a non-consensual intimate image, which was brought into force in early 2026 (Hansard, 2026). At the time of writing, the Crime and Policing Bill, which completed its third reading in the House of Lords in March 2026, proposes further deepfake-specific offences and remains before Parliament (QMUL Legal Advice Center, 2026).

These measures are narrower than a general evidentiary framework — they address deepfakes as

instruments of image-based abuse rather than as a category of contested litigation evidence — but they demonstrate a legislature willing to revisit and progressively extend deepfake-specific criminal provisions at a pace markedly faster than Bangladesh's. The Law Commission's ongoing review of evidence law, which includes AI-generated evidence within its scope, suggests that deepfake-specific evidentiary standards, distinct from the criminal offences already enacted, may be introduced in due course.

5.3 Malaysia

5.3.1 The Section 90A–90C Framework

Malaysia's Evidence Act 1950 is, of the two comparators, structurally closer to Bangladesh's Evidence Act. Sections 90A, 90B, and 90C, inserted to address computer-generated evidence, provide a considerably more detailed statutory framework than that currently possessed by Bangladesh. Section 90A establishes the conditions for admitting a document produced by a computer in the ordinary course of its operation, ordinarily supported by a certificate from a person responsible for the computer's operation, with section 90A(6) operating as a deeming provision permitting admission without a certificate in certain circumstances. Section 90B governs the weight to be attached to a document admitted under section 90A, directing courts to consider the circumstances of its production. Section 90C states that sections 90A and 90B prevail over any inconsistent provisions elsewhere in Malaysian law.

5.3.2 Operation and Limits of the Presumption

The certification mechanism under Section 90A was designed to facilitate the routine admission of business records without requiring full forensic proof on each occasion, a sound rationale within its original context. In the deepfake context, its principal vulnerability is that a party tendering fabricated content can invoke the presumption of reliability unless the opposing party affirmatively challenges it, and mounting that challenge requires forensic evidence that is often expensive and technically demanding to obtain. Malaysian courts have shown some awareness of this tension, applying heightened scrutiny to digital evidence in certain criminal proceedings, notwithstanding the statutory presumption, particularly where the stakes are high (Mohamad, 2019). Malaysian case law has also developed guidance on the qualifications and methodology expected of digital forensic experts that exceeds what Bangladeshi courts currently have available, representing institutional experience from which Bangladesh's own expert-evidence framework could draw.

5.3.3 Residual Gaps

Similar to Bangladesh and the United Kingdom, Malaysia has not enacted deepfake-specific evidentiary legislation. Sections 90A–90C address the reliability of computer-generated records as a general category; they do not squarely address a recording that is forensically indistinguishable from a genuine original because it was synthesized by AI from inception rather than derived from any authentic source. As deepfake technology becomes more prevalent in Malaysian litigation, the existing framework will require targeted amendments to remain adequate.

5.4 Comparative Evaluation and Lessons for Bangladesh

The comparison across the three jurisdictions reveals a consistent pattern: each has formally recognized electronic evidence, each relies substantially on expert testimony to resolve contested authenticity questions, and none has enacted deepfake-specific evidentiary standards. The jurisdictions differ in the robustness of their authentication infrastructure — the United Kingdom's is the most developed, Malaysia's intermediate, and Bangladesh's the least developed — in the specificity of their statutory frameworks for computer-generated evidence, where Malaysia's targeted provisions exceed Bangladesh's general ones, and in the depth of accumulated judicial experience with contested digital evidence, where English courts are the most advanced.

For Bangladesh, the most directly transferable lesson from Malaysia concerns the value of a detailed statutory provision for electronic records: the existing Section 65B framework is markedly less developed than Malaysia's Section 90A regime and could be strengthened along similar lines without requiring

wholesale statutory redesign. From the United Kingdom, the relevant lesson is methodological: authentication should be approached as a substantive inquiry into the reliability of the evidence itself rather than a procedural formality satisfied by certification alone. Neither comparator offers a complete solution, but each contributes a component — Malaysia's procedural specificity, the United Kingdom's substantive reliability orientation, and the demonstrated institutional capacity in both jurisdictions to legislate iteratively as the technology develops — that Bangladesh can adapt into a more robust domestic framework.

VI. CHALLENGES IN VERIFYING DEEPFAKE EVIDENCE

6.1 The Nature of the Authentication Problem

Authentication is the process of establishing that evidence is what it purports to be, conventionally requiring proof of provenance, integrity, and relevance to real-world events. Deepfakes complicate all three inquiries, but most fundamentally the third: a deepfake file may have impeccable provenance and unimpeachable integrity — properly retrieved from a legitimate source, untampered with since collection — while being entirely false in its depiction of reality. This is the integrity–authenticity distinction introduced in Section 2.2, which explains why authentication procedures developed for conventional digital evidence are necessary but not sufficient in the deepfake context.

6.2 Technical Detection Methods

Metadata examination provides an initial screening tool; anomalies such as a creation timestamp predating the depicted event can raise suspicion, but metadata is readily stripped or falsified, so it functions as a preliminary filter rather than a conclusive test (Farid, 2022). Digital forensic analysis examines a file for artifacts characteristic of AI generation, such as inconsistencies in facial geometry, irregular blink patterns, imperfect lip synchronization, mismatched lighting, and statistical irregularities in pixel distribution. Trained examiners using specialized tools can identify many deepfakes that would pass casual inspection, but generative techniques are under continuous refinement, specifically to eliminate these markers, producing an evolving contest in which detection methodology must be revalidated against newly emerging generation techniques rather than treated as fixed.

Automated AI-based detection tools — neural network classifiers, frequency-domain analysis targeting the spectral signatures characteristic of GAN-generated images, and biometric comparison against known authentic recordings — extend forensic capacity beyond what human review can achieve at scale (Chesney & Citron, 2019). These tools report high accuracy on the datasets against which they are validated, but may perform less reliably against deepfakes produced by techniques outside their training distribution. They are properly understood as forensic aids that inform rather than substitute expert judgment. Cryptographic and blockchain-based content registration creates an immutable timestamp and content hash at the moment of creation, such that subsequent alterations produce detectable mismatches (NIST, 2023). However, this approach is prospective only: it offers no assistance with deepfakes never registered as authentic, which describes the overwhelming majority of deepfake content currently in circulation.

6.3 Legal and Procedural Methods

Expert testimony will remain the primary evidentiary vehicle for deepfake authentication in most contested cases, which makes the absence of a qualification or methodological standard in the Evidence Act (discussed in Section 4.3 above) a central rather than a peripheral deficiency. Chain-of-custody documentation, while unable to resolve the authenticity question directly, retains evidentiary relevance by narrowing the temporal window within which fabrication could plausibly have occurred and by providing corroborative weight in cases where the chain is broken or irregular. No authentication conclusion should rest on a single category of evidence: forensic findings should be assessed alongside circumstantial corroboration — whether the persons depicted were demonstrably present at the claimed location, whether independent contemporaneous records support or contradict the recording, and whether the content is consistent with the established conduct of the individuals concerned.

6.4 A Proposed Authentication Sequence

Drawing on the foregoing analysis, a sequential authentication protocol is proposed for cases in which the authenticity of digital audio-visual evidence is genuinely contested: first, verification of the file's source and provenance; second, metadata analysis for anomalies inconsistent with the claimed origin; third, digital forensic examination for artifacts associated with AI generation using recognized methodology; fourth, supplementary screening using validated AI detection tools; fifth, independent expert evaluation of the forensic findings; sixth, assessment of the forensic conclusions against available corroborating evidence; and finally, judicial evaluation of the authentication evidence as a whole before any ruling on admissibility or evidentiary weight. This sequence is compatible with the existing procedural framework and could be adopted by judicial practice direction without requiring prior legislative amendment, although statutory codification (discussed in Section 8 below) would give it a more secure footing.

VII. PREVENTING THE MISUSE OF DEEPFAKE EVIDENCE

7.1 The Case for Prevention

Detection and authentication are reactive; they engage with deepfake evidence only after it has been created and tendered. Reliance on reactive mechanisms alone carries significant costs: forensic examination is expensive, technically demanding, and not always available before a decision must be made, and where deepfake evidence has already shaped pre-trial decisions to arrest, charge, or settle, the resulting harm may be only partially reversible even once the evidence is later discredited. Preventive measures aim to interrupt misuse earlier in the causal chain, a goal justified not only by efficiency but also by the procedural-justice interest in courts retaining their character as reliable fact finders rather than becoming routinely vulnerable to fabricated submissions.

7.2 Technological and Legal Safeguards

Digital watermarking embeds the device, timestamp, and integrity information into a file at creation in a manner resistant to undetected removal. Standardized adoption across devices used by law enforcement and regulated institutions would render the absence of an expected watermark probative evidence. Provenance-tracking standards, such as the Coalition for Content Provenance and Authenticity (C2PA) initiative, pursue a comparable objective by recording a tamper-evident history of a file's origin and editing history (NIST, 2023). AI-assisted pre-submission screening within court filing systems, analogous to risk-based monitoring in anti-money laundering compliance, could flag audio-visual evidence presenting risk indicators for forensic review prior to admission, while no automated screen will be exhaustive.

On the legal side, mandatory disclosure requirements compelling early notice — together with provenance and authenticity documentation — for any party intending to rely on digital audio-visual evidence would give the opposing party a genuine opportunity to investigate authenticity before the trial. Courts should also be given express statutory power to order the forensic examination of contested digital evidence prior to admission, analogous to existing powers to order medical examinations in personal injury claims. Placing this power directly in the Evidence Act, rather than leaving it to uncertain inherent jurisdiction, would provide greater clarity. Institutional investment — dedicated forensic capacity within the Bangladesh Computer Council or an equivalent body, and structured judicial and professional training — underlies the practical availability of all the foregoing measures and should be treated as a precondition for their effectiveness rather than a separate, lower-priority recommendation.

VIII. REMEDIES AGAINST DEEPFAKE EVIDENCE

8.1 Procedural, Criminal, and Civil Dimensions

The remedial landscape spans procedural, criminal, and civil domains that are not mutually exclusive but are interrelated. A single act of submitting fabricated evidence may simultaneously warrant procedural sanctions within litigation, criminal liability for the fabricator, and civil claims by the affected third parties.

Within the litigation itself, the primary procedural remedy is the exclusion of evidence found, following an authentication inquiry, to be fabricated, appropriately coupled, where warranted, with an adverse inference against the party who tendered it. In civil proceedings, this may draw support from the existing spoliation doctrine, which treats the destruction or concealment of evidence as indicative of a weak underlying case. Cost sanctions, the striking out of claims or defenses founded on fabricated evidence, and referral to professional disciplinary bodies where lawyer tendered evidence without reasonable grounds for believing in its authenticity reinforce the incentive for the profession to undertake authentication diligence before introducing digital audio-visual material.

Deliberate fabrication of evidence may, in principle, engage liability under the Evidence Act's provisions on false evidence, the Penal Code's forgery and fraud provisions, and the cyber-offence provisions discussed in Section 4.4 above, although none of these was drafted with deepfake fabrication specifically in mind, requiring prosecutors to fit the conduct within categories defined for other purposes. A deepfake-specific offence — addressing the knowing creation, possession, or submission of AI-generated or AI-manipulated content with intent to deceive a court or law enforcement body, modelled on the United Kingdom's progressive extension of deepfake-specific criminal liability discussed in Section 5.2.2 — would remove this definitional uncertainty and signal the seriousness with which fabricated evidence is treated.

Civil remedies — defamation, misuse of private information, or its Bangladeshi analog, malicious falsehood, and general tort liability — are available to individuals harmed by deepfake content, whether through non-consensual depiction or through the loss of a legitimate claim attributable to manipulated evidence used against them. Where deepfake content continues to circulate, injunctive relief restraining further dissemination is often of greater practical value to a victim than retrospective compensation, and courts should be prepared to grant urgent interim relief while substantive proceedings remain pending.

8.2 Practical Limits

The effectiveness of any remedy depends on the institutional capacity to administer it. Identifying the creator of a deepfake may be technically difficult when sophisticated anonymization has been used or the fabrication originated abroad, and criminal prosecution requires forensic proof to a standard that places considerable demands on investigative resources. The speed of digital circulation compounds this difficulty: a deepfake may reach a wide audience before it is identified as fabricated and before any legal process can be initiated, leaving remedies that operate after the fact necessarily incomplete and ineffective. This reinforces the priority that should be attached to the preventive measures discussed in Section 7: the most valuable legal response to deepfake evidence is one that prevents it from being treated as genuine in the first place, rather than one that compensates for the harm once it has already occurred.

IX. FINDINGS AND DISCUSSION

The analysis supports four principal findings. First, deepfake technology presents an evidentiary challenge that is qualitatively distinct from conventional digital manipulation because it fabricates content with no authentic original against which a comparison can be drawn — a separation between the integrity of a file and the authenticity of its content that existing authentication doctrine was not designed to address. Second, Bangladesh's evidentiary framework, including the 2022 amendments, remains structurally inadequate to this challenge: it authenticates the handling of digital files without authenticating the reality of their content and provides no qualification or methodological standard for the expert testimony on which deepfake authentication depends.

Third, comparative analysis shows that this is not a uniquely Bangladeshi deficiency — neither the United Kingdom nor Malaysia has enacted a deepfake-specific evidentiary regime — but both offer components transferable to Bangladesh's context: Malaysia's more granular statutory treatment of computer-generated evidence and the United Kingdom's orientation toward substantive reliability

review over procedural certification. Fourth, the comparative picture is not static: Bangladesh's own CSA 2026, and the further amendments under consideration as of mid-2026, together with the United Kingdom's rapid extension of deepfake-specific criminal offences through the Online Safety Act 2023, the Data (Use and Access) Act 2025, and the pending Crime and Policing Bill, demonstrate that legislatures in this comparator group are capable of swift, iterative statutory responses to an evolving technology — undercutting any assumption that the reforms proposed here would be institutionally unrealistic for Bangladesh.

This also clarifies what reforms should not be attempted. A framework treating all contested digital evidence with reflexive suspicion would be as damaging as one that ignores the deepfake problem entirely, given how far Bangladeshi litigation now depends on electronic records. The object of the reforms below is calibration: directing heightened scrutiny to evidence whose authenticity is genuinely in dispute without imposing forensic burdens on the routine electronic records that constitute the bulk of digital evidence before Bangladeshi courts.

X. RECOMMENDATIONS

10.1 Legislative Recommendations

Five legislative reforms are recommended in this regard. The Evidence Act, 1872, should be amended to introduce a statutory definition of "deepfake evidence" and "AI-generated content" as a distinct category of electronic records attracting heightened authentication requirements. A provision should be inserted requiring any party intending to rely on digital audio-visual evidence to serve an authentication certificate, prepared by a qualified digital forensics expert, on the opposing party a defined period before the trial, coupled with an express power for the court to order a pre-admission forensic examination on application. The Act should specify the qualifications and methodological standards required of experts offering opinions on the authenticity of AI-generated evidence, drawing on the approach of the UK Forensic Science Regulator discussed in Section 5.2.1. A specific criminal offence of fabricating AI-generated evidence for submission to a court or law enforcement body should be introduced, with penalties proportionate to the resulting harm to the victim. Finally, the CSA 2026 should be reviewed, in the course of the amendment process already under way as of mid-2026, to ensure that its AI-related provisions extend clearly to deepfake fabrication intended to mislead courts, a dimension distinct from the platform-content concerns the current amendment process appears principally directed at.

10.2 Institutional Recommendations

A dedicated National Digital Evidence and Deepfake Forensics capacity should be established within the Bangladesh Computer Council or a comparable body with statutory authority to provide expert evidence to courts, law enforcement, and prosecutors. A national accreditation scheme for digital forensics experts should be developed, specifying the qualifications and continuing professional development requirements for practitioners offering opinion evidence on deepfake authenticity. Digital evidence and deepfake technology modules should be incorporated into judicial training at all levels, both initial and continuing, and into bar professional training, including practical instruction on identifying potential deepfakes, instructing forensic experts, and testing opposing expert’s evidence.

10.3 Procedural Recommendations

Practice directions should require parties in civil and criminal proceedings to disclose the provenance and chain of custody of digital audio-visual evidence at the earliest, practicable opportunity. Courts should adopt the sequential authentication framework proposed in Section 6.4 as a standard practice for cases in which the authenticity of digital evidence is genuinely disputed. Pending statutory reform, judges should be empowered by practice direction to appoint independent court forensic experts in deepfake cases where the parties' own expert evidence is in genuine conflict.

10.4 International Cooperation

Deepfakes do not respect national borders: content may be fabricated in one jurisdiction and tendered in another, generation tools may be hosted on foreign infrastructure, and networks producing fabricated

content for criminal purposes frequently operate transnationally. Bangladesh should engage more actively with multilateral initiatives on AI governance, including UNESCO's work on platform governance (UNESCO, 2023) and the Council of Europe's engagement with AI in criminal justice (Council of Europe, 2022). It should also update bilateral mutual legal assistance arrangements to specifically address AI-generated evidence, including the sharing of forensic expertise and the admissibility of foreign expert evidence.

XI. CONCLUSION

The law of evidence exists to serve the pursuit of truth in adjudicative proceedings. Where the reliability of evidence cannot be assumed, the truth-seeking function of those proceedings — and with it, the legitimacy of their outcomes — is compromised. Deepfake technology is not a speculative future risk for Bangladesh's courts; it is a present risk, operating within an evidentiary framework designed for different conditions. This study sought to answer not whether Bangladesh's legal system must respond, but how. The comparative analysis offered here suggests that the answer lies less in importing any single foreign model than in combining transferable components from each comparator with reforms calibrated to Bangladesh's own institutional capacity.

Neither the United Kingdom nor Malaysia has produced a complete solution. The United Kingdom's doctrinal flexibility and developed forensic infrastructure provide meaningful protection, but lack dedicated statutory grounding for deepfake authentication specifically; Malaysia's statutory provisions are more specific but were not designed with AI-generated content in view. Bangladesh's position, while currently the least developed of the three on this question, carries a corresponding advantage: the opportunity to draw on accumulated experience from both comparators and the institutional willingness already visible in the CSA 2026 and its pending amendment to legislate in this space before deepfake evidence becomes routine in contested litigation rather than the comparatively rare occurrence it remains today.

The reforms proposed in this paper are achievable within Bangladesh's existing institutional framework and do not depend on resources beyond what a genuine commitment to integrity would justify. They require recognition that the digital evidentiary environment has changed in ways that the existing law has not yet absorbed and the institutional will to close that gap before, rather than after, it produces a result that the justice system cannot defend.

REFERENCES

[1] 5KBW. (2025, June 30). Sexual offences in the Online Safety Act of 2023. https://www.5kbw.co.uk/2024/11/28/sexual-offences-in-the-online-safety-act-2023/

[2] Ahmad Shariff, N., Ismail, R., & Hamzah, N. (2021). Challenges of the admissibility of digital evidence in Malaysia. Current Law Journal, 9(2), 1–18.

[3] Chesney, R., & Citron, D. K. (2019). Deepfakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753–1820.

[4] Council of Europe. (2022). Artificial intelligence and the criminal justice system. Council of Europe Publishing,

[5] The Evidence Act of 1872 (Act No of. I of 1872) (Bangladesh).

[6] Farid, H. (2022). Creating and detecting deepfakes. Springer.

[7] Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative adversarial networks. Advances in Neural Information Processing Systems, 27, 2672–2680.

[8] Government of Bangladesh. (2022). Evidence Act, 1872 (Amendment of 2022). Ministry of Law, Justice and Parliamentary Affairs.

[9] Government of Bangladesh. (2025). Cybersecurity Act of 2026. Ministry of Law, Justice and Parliamentary Affairs.

[10] Hansard (UK Parliament, House of Lords). (2026, January 14). Social media: Non-consensual sexual deepfakes [Debate

transcript]. https://hansard.parliament.uk/lords/2026-01-14/debates/2AF08B6C-1AFC-4395-B356-E383ABF28161/SocialMediaNon-ConsensualSexualDeepfakes

[11] Lexplosion Solutions. (2025, December 22). Cyber Security Ordinance 2025: Implications for Bangladeshi Businesses https://lexplosion.in/cyber-security-ordinance-2025-implications-for-businesses-in-bangladesh/

[12] Malaysia. (1950). Evidence Act of 1950 (Act No.56).

[13] Mason, S., & Seng, D. (Eds.). (2021). Electronic evidence and electronic signatures (6th ed.). Institute of Advanced Legal Studies, London, UK.

[14] Mohamad, D. (2019). Digital forensics and the admissibility of electronic evidence in Malaysian Syariah courts: Towards a standardized approach. Lex Forensica Journal, 1(1), 1–22.

[15] National Institute of Standards and Technology (NIST). (2023). Reducing the threat of deepfake manipulation: U.S. Department of Commerce,

[16] Prothom Alo. (2025, May 22). The government issues a gazette on the Cyber Security Ordinance. https://en.prothomalo.com/bangladesh/government/5gj5obvmuw

[17] QMUL Legal Advice Centre. (2026, March 31). Deepfakes and consent: The law finally catches up. Queen Mary University of London, London, UK https://www.qmul.ac.uk/lac/our-legal-blog/2026-blogs/items/deepfakes-and-consent-the-law-finally-catches-up-.html

[18] Rahman, M. T., & Naser, A. (2023). Admissibility of electronic evidence in Bangladesh: Contemporary challenges and prospects. Bangladesh Journal of Law, 34(1), 45–63.

[19] Roberts, P., & Zuckerman, A. (2022). Criminal evidence (3rd ed.). Oxford University Press.

[20] Russell, S., & Norvig, P. (2021). Artificial intelligence: A modern approach (4th ed.). Pearson.

[21] TBS News. (2026, June 8). Cyber Security Act to be amended to remove harmful AI-generated content: Home Minister. https://www.tbsnews.net/bangladesh/cyber-security-act-be-amended-remove-harmful-ai-generated-content-home-minister-1457531

[22] UNESCO. (2023). Guidance for the governance of digital platforms. UNESCO Publishing.

[23] United Kingdom Government (UKG). (1984). Police and Criminal Evidence Act, 1984.

[24] United Kingdom Government (UKG). (2020). Criminal Procedure Rules 2020.

[25] United Kingdom Government (UKG). (2023). Online Safety Act 2023.

[26] United Kingdom Government (UKG). (2025). Data (Use and Access) Act of 2025.