International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 17-01-2026, Accepted: 16-02-2026, Published: 03-03-2026
Volume 12, Issue 1, 2026, Page No. 378-382

Deepfakes and false digital evidence in Indian Courts

Pooja Kisan Bhosale[1]*, Dr. Mannalal R Pandiya[2], Dr. Vijay Sahadeo Chavan[3]
[1] Research Scholar, Department of Law, Shri Jagdishprasad Jhabarmal Tibrewala University (SJJTU), Rajasthan, India
[2] Assistant Professor, Department of Law, Shri Jagdishprasad Jhabarmal Tibrewala University (SJJTU), Rajasthan, India
[3] External Co-Guide, Department of Law, Shri Jagdishprasad Jhabarmal Tibrewala University (SJJTU), Rajasthan, India
Corresponding Author: Pooja Kisan Bhosale

Abstract
The rapid advancement of artificial intelligence has introduced a new category of digital manipulation known as deepfakes, which has significant implications for the administration of justice. Deepfakes refer to artificially generated or altered audio, video, or image content created using sophisticated machine learning technologies that can convincingly imitate real individuals and events. While digital evidence has become increasingly central to modern litigation, the rise of synthetic media poses unprecedented challenges to legal systems worldwide, including India. Courts are now frequently confronted with electronic evidence such as screenshots, voice recordings, and social media content, particularly in matrimonial disputes and criminal proceedings. These areas are especially vulnerable due to the private and emotionally charged nature of relationships, where digital communications often serve as crucial evidence.

The misuse of deepfake technology can facilitate the fabrication of false allegations, manipulation of electronic records, and distortion of factual narratives, thereby threatening the integrity of judicial processes. Indian legal frameworks governing electronic evidence, although evolving, were not designed to address the complexities of AI-generated synthetic content. Consequently, issues of authentication, admissibility, and evidentiary reliability have become increasingly prominent. This paper examines the technological foundations of deepfakes, their potential misuse in matrimonial and criminal litigation, and the existing legal provisions regulating electronic evidence in India. It further analyses judicial responses to digital evidence and identifies critical gaps in regulatory and procedural safeguards. The study concludes by proposing reforms aimed at strengthening forensic verification mechanisms, enhancing judicial awareness, and developing robust legal standards to address the growing threat posed by synthetic evidence.

Keywords: Deepfakes, synthetic evidence, electronic evidence, matrimonial litigation, digital forensics, cyber law

Introduction

In recent years, technology has transformed nearly every aspect of human life, including how people communicate, build relationships, and resolve disputes. Courts today increasingly rely on digital evidence such as emails, text messages, social media posts, audio recordings, and electronic documents. This shift toward digital proof has made legal proceedings faster and more convenient, but it has also created new challenges. One of the most serious emerging concerns is the rise of deepfake technology and the growing possibility of false digital evidence being used in courts.

Deepfakes are digitally manipulated audio, video, or images created using artificial intelligence. With the help of advanced machine learning tools, it is now possible to generate highly realistic content that can make a person appear to say or do things that never actually happened. What once required sophisticated technical expertise is now available through easily accessible mobile applications and online platforms? As a result, the misuse of such technology is no longer limited to experts but can be carried out by ordinary individuals with minimal technical knowledge.

The legal implications of deepfakes are particularly serious because modern courts increasingly treat digital communication as reliable evidence. Screenshots of conversations, voice recordings, and social media content are frequently used to establish facts in both civil and criminal proceedings. However, the ability to fabricate such evidence through artificial intelligence creates a significant risk to the fairness of judicial processes. False digital content can mislead courts, damage reputations, and result in wrongful legal action against innocent individuals.

This problem is especially concerning in emotionally sensitive disputes such as matrimonial conflicts and criminal allegations involving personal relationships. In such cases, private digital communications often play a central role in proving claims related to cruelty, harassment, infidelity, or threats. Because these disputes already involve strong emotions and personal tensions, the temptation to manipulate digital evidence can be high. The presence of deepfake technology makes it easier than ever to create convincing but false proof, which may be difficult for courts to detect without proper forensic examination.

Although Indian law recognizes electronic records as admissible evidence, the legal framework was developed at a time when artificial intelligence-based manipulation was not a widespread concern. Existing rules primarily focus on the authenticity of electronic records but do not specifically address the unique challenges posed by synthetic media. As a result, courts face increasing difficulty in determining whether digital evidence is genuine or artificially created.

Against this backdrop, it becomes necessary to examine the impact of deepfakes on the justice system. This paper explores the concept of deepfake technology, its potential misuse in litigation, the legal provisions governing electronic evidence in India, and the challenges faced by courts in dealing with synthetic digital content. It also highlights the urgent need for stronger safeguards, better

forensic tools, and greater judicial awareness to ensure that technological advancements do not undermine the integrity of the legal system.

Understanding Deepfakes and Synthetic Digital Evidence

To understand the risks that deepfakes pose to the legal system, it is first important to understand what they are and how they work. The term "deepfake" is derived from two words — "deep learning," a branch of artificial intelligence, and "fake," meaning something that is not real. Deepfakes are digitally created or altered audio, video, images, or even text that appear authentic but are actually manufactured using advanced software. These tools use artificial intelligence to study large amounts of real data, such as a person's face, voice, or writing style, and then generate new content that closely imitates that individual.

In the past, creating fake digital content required considerable technical expertise and expensive software. Today, however, technology has become much more accessible. Numerous mobile applications and online tools allow users to edit images, alter voices, and even create realistic face-swap videos within minutes. This ease of access has significantly increased the potential for misuse. Deepfake technology is no longer limited to research laboratories or film studios; it has become available to ordinary individuals with little technical knowledge.

Deepfakes can take several forms that are particularly relevant to legal disputes. One common type is manipulated video content, where a person's face is digitally placed onto another body, making it appear that the person performed certain actions. Another form involves voice cloning, where software can replicate a person's speech patterns to create fake audio recordings. There are also digitally altered images, including morphed photographs, which can falsely depict individuals in compromising situations. In addition, fabricated text messages and edited screenshots of online conversations have become increasingly common, especially in disputes involving personal relationships.

The danger of such synthetic digital evidence lies in its high level of realism. Unlike traditional forms of forgery, deepfakes are often difficult to detect with the naked eye. Even trained observers may struggle to distinguish between genuine and manipulated content without the assistance of digital forensic analysis. This makes deepfakes particularly harmful in legal settings, where courts depend heavily on the credibility of evidence presented before them.

Another major concern is the speed at which deepfakes can spread. Once false digital content is created, it can be shared instantly through social media, messaging platforms, and online networks. This rapid circulation can cause immediate reputational damage and may influence public perception even before legal verification takes place. In legal disputes, such widespread sharing can also create pressure on parties and complicate the process of establishing the truth.

It is also important to note that deepfakes are not always created with malicious intent. In some cases, they are used for entertainment, satire, or artistic purposes. However, when such technology is used to deceive courts, fabricate allegations, or manipulate evidence, it becomes a serious legal and ethical problem. The misuse of synthetic digital content can undermine trust in electronic evidence, which has become an essential part of modern judicial proceedings.

As courts increasingly rely on digital records to determine facts, the possibility of fabricated electronic evidence presents a significant challenge. Traditional legal safeguards were designed to deal with physical documents and simple digital records, not highly sophisticated AI-generated content. Therefore, understanding the nature and risks of deepfakes is essential before examining how existing legal systems address this emerging threat.

Legal Framework Governing Electronic Evidence in India

As digital communication has become an integral part of everyday life, courts in India have increasingly recognized electronic records as valid forms of evidence. Emails, text messages, social media posts, audio recordings, and digital documents are now frequently presented in legal proceedings. However, the law governing electronic evidence was developed before the emergence of advanced artificial intelligence technologies such as deepfakes. As a result, while the legal framework provides general rules for handling digital records, it does not fully address the unique challenges posed by synthetic digital content.

Indian law treats electronic records as a form of documentary evidence. This means that digital materials, such as computer files, mobile data, and online communications, can be used in court to prove facts. However, unlike physical documents, electronic records are more vulnerable to alteration and manipulation. Therefore, the law places special emphasis on ensuring that such evidence is authentic and reliable before it is accepted by courts.

One of the key requirements for the admissibility of electronic evidence is proof of its authenticity. Courts must be satisfied that the digital record has not been tampered with and accurately represents the original data. To ensure this, legal rules require that electronic evidence be accompanied by proper certification regarding its source, method of storage, and the manner in which it was produced. This certification process is intended to maintain the integrity of digital records and prevent the use of fabricated or altered material.

Another important aspect of electronic evidence law is the concept of chain of custody. This refers to the process of documenting how digital evidence was collected, stored, and handled from the time it was created until it is presented in court. Proper documentation helps establish that the evidence has not been modified or interfered with. However, in many real-life disputes, especially those involving personal relationships, digital content such as screenshots and recordings is often collected informally without proper safeguards. This weakens its reliability and makes it difficult for courts to determine its authenticity.

The legal framework also recognizes the role of digital forensic examination. Courts may rely on expert analysis to verify whether electronic records have been altered or manipulated. Forensic experts use specialized tools to detect inconsistencies in metadata, identify signs of editing, and confirm whether digital files are genuine. While this mechanism provides an important safeguard, it is not always used consistently due to limited resources, lack of awareness, and procedural delays.

The emergence of deepfake technology has further complicated the legal treatment of electronic evidence. Traditional rules were designed to address simple forms of

digital tampering, such as edited documents or altered photographs. Deepfakes, however, involve sophisticated artificial intelligence that can generate entirely new content rather than merely modifying existing material. This makes detection much more difficult and raises questions about whether current legal safeguards are adequate to deal with such advanced manipulation.

Another challenge lies in the burden placed on parties to prove the authenticity of digital evidence. In many cases, individuals may not have the technical knowledge or resources required to verify whether content is genuine or artificially created. This imbalance can lead to unfair outcomes, particularly when courts rely heavily on digital proof without adequate forensic scrutiny.

Thus, while Indian law has made significant progress in recognizing electronic evidence, it still faces serious limitations in addressing the complexities introduced by deepfake technology. The rapid development of artificial intelligence has outpaced legal reforms, creating a gap between technological reality and legal preparedness. This gap becomes especially evident in sensitive disputes where digital evidence plays a decisive role.

Deepfakes in Matrimonial and Criminal Litigation: Risks and Misuse

The growing use of digital communication in personal relationships has made electronic evidence a central feature of many legal disputes, particularly in matrimonial and criminal cases. Conversations that once took place privately are now recorded through text messages, emails, social media interactions, and voice notes. As a result, courts increasingly rely on such digital material to determine facts relating to cruelty, harassment, threats, infidelity, and financial disputes. However, the emergence of deepfake technology has introduced serious risks in this context, as it allows individuals to create highly convincing but false digital evidence.

Matrimonial disputes are especially vulnerable to the misuse of synthetic digital content because they often involve emotional conflicts and personal grievances. In divorce proceedings, parties frequently present screenshots of conversations to demonstrate allegations of misconduct, such as extramarital relationships or abusive behaviour. With the availability of advanced editing tools, it has become possible to fabricate or alter such conversations with relative ease. Deepfake technology can further enhance this manipulation by generating realistic chat records or voice recordings that appear genuine but have no factual basis.

Another area of concern is the use of morphed or fabricated images in disputes related to personal relationships. Artificially generated photographs can be used to falsely portray individuals in compromising situations, potentially damaging reputations and influencing legal outcomes. Such content can be particularly harmful in matrimonial litigation, where courts must evaluate sensitive allegations that often rely heavily on digital proof. Without proper forensic verification, it may be difficult to distinguish between authentic and manipulated material.

Criminal cases involving personal disputes also face similar risks. Digital evidence is frequently used to support allegations of harassment, threats, or coercion. For example, audio recordings are often presented to demonstrate verbal abuse or intimidation. However, voice cloning technology now makes it possible to create synthetic recordings that closely imitate a person's speech patterns. These fabricated recordings can mislead investigators and courts if they are accepted without careful examination.

The misuse of deepfake technology is not limited to creating false evidence; it can also be used as a tool of intimidation. Individuals may threaten to release fabricated digital content to exert pressure during disputes, particularly in situations involving financial negotiations or settlement discussions. The fear of reputational damage can compel victims to agree to unfair terms, thereby undermining the fairness of legal proceedings.

One of the key reasons matrimonial and personal disputes are particularly vulnerable to synthetic evidence is the informal manner in which digital material is collected and presented. Unlike evidence gathered through official investigative procedures, personal digital records are often obtained without proper documentation of their origin or authenticity. Courts may therefore face difficulties in verifying whether such evidence has been altered or artificially created.

Another challenge arises from the emotional nature of these disputes. Parties may strongly believe in the authenticity of the digital evidence they present, even when it has been manipulated. This can complicate the fact-finding process and place additional burdens on courts to carefully scrutinize electronic records. The high volume of cases and limited access to forensic resources further increases the risk that synthetic evidence may go undetected.

The potential misuse of deepfakes in matrimonial and criminal litigation highlights the urgent need for stronger safeguards in handling digital evidence. Without appropriate verification mechanisms, the increasing reliance on electronic records may inadvertently create opportunities for injustice. As technology continues to evolve, the legal system must adapt to ensure that digital advancements do not compromise the integrity of judicial decision-making.

Judicial Approach to Electronic Evidence and Emerging Challenges

Indian courts have gradually adapted to the increasing use of electronic evidence in legal proceedings. Over the past two decades, judges have recognized that digital records such as emails, mobile messages, call recordings, and online communications often play a crucial role in establishing facts. As a result, courts have developed certain principles to ensure that electronic evidence is handled carefully and does not compromise the fairness of trials. However, the emergence of deepfake technology has created new challenges that existing judicial practices were not designed to address.

One of the key concerns for courts when dealing with electronic evidence is authenticity. Judges must determine whether a digital record is genuine and has not been altered. Unlike traditional documents, electronic records can be easily modified without leaving visible signs. Therefore, courts often insist on proper certification and verification before accepting such evidence. This cautious approach reflects an awareness that digital material is inherently more vulnerable to manipulation than physical records.

Courts have also emphasized the importance of technical examination in cases involving disputed electronic evidence. When doubts arise regarding the authenticity of digital material, judges may rely on forensic experts to analyze the

data. Such experts examine metadata, identify signs of editing, and assess whether a file has been tampered with. This process helps courts avoid relying on misleading or fabricated evidence. However, forensic examination is not always sought in every case, particularly in disputes where parties present digital records informally.

Another important aspect of the judicial approach is the recognition that screenshots and printed copies of digital content are not always reliable. Courts have repeatedly noted that such materials can be easily altered or taken out of context. As a result, judges often require supporting evidence to establish the credibility of digital records. This may include verification from service providers, original device data, or expert analysis.

Despite these safeguards, courts face several practical challenges when dealing with electronic evidence. One major difficulty is the lack of technical expertise among legal professionals. Judges and lawyers may not always be familiar with the complexities of modern digital manipulation techniques, including deepfakes. This knowledge gap can make it difficult to fully understand how synthetic media is created and how it can be detected.

Resource constraints also pose significant challenges. Digital forensic analysis requires specialized tools, trained personnel, and considerable time. Many courts, particularly those handling high volumes of cases, may not have immediate access to such resources. As a result, electronic evidence may sometimes be accepted without thorough verification, increasing the risk of relying on inaccurate or manipulated material.

The rapid pace of technological development further complicates the situation. Deepfake technology continues to evolve, becoming more realistic and harder to detect. Traditional methods of verifying electronic records may not be sufficient to identify advanced AI-generated content. This creates a situation where legal safeguards struggle to keep pace with technological innovation.

Another emerging challenge is the growing reliance on digital communication in everyday life. As more interactions take place online, the volume of electronic evidence presented in courts is steadily increasing. This makes it more difficult for judges to thoroughly examine each piece of digital material. The risk of overlooking subtle manipulation therefore becomes higher.

Overall, while Indian courts have shown awareness of the risks associated with electronic evidence, the rise of deepfake technology presents unprecedented challenges. The existing judicial approach, though cautious, may not be fully equipped to handle highly sophisticated forms of synthetic digital content. This highlights the need for enhanced training, better forensic infrastructure, and updated legal standards to ensure that the integrity of the judicial process is preserved.

Legal Gaps and Challenges in Addressing Deepfakes

Despite the growing use of digital evidence in courts, the legal system still faces significant gaps in effectively addressing the challenges posed by deepfake technology. One of the primary issues is that existing laws were designed to regulate traditional forms of electronic records, not highly advanced artificial intelligence–generated content. As a result, while current legal provisions provide general safeguards against tampering and forgery, they do not specifically address the unique risks associated with synthetic media.

A major legal gap lies in the absence of clear definitions and regulations relating to deepfakes. At present, Indian law does not provide a specific legal framework that directly deals with AI-generated manipulated content. Instead, such cases are addressed under broader provisions related to forgery, impersonation, or cyber offences. While these provisions can be applied in certain situations, they do not fully capture the complexity of deepfake technology, which can involve highly sophisticated forms of digital fabrication that are difficult to categorize under existing legal concepts.

Another significant challenge is the difficulty of detection. Deepfakes are designed to appear realistic, making it extremely difficult for ordinary individuals and even trained professionals to identify manipulation without specialized forensic tools. This creates a serious problem in legal proceedings, where parties may rely on digital evidence that appears authentic on the surface. The burden of proving that such evidence is fabricated often falls on the opposing party, who may lack the technical knowledge, financial resources, or access to forensic expertise required to challenge it effectively.

The rapid pace of technological development further widens the gap between law and reality. Artificial intelligence tools are evolving faster than legal systems can adapt. As detection technologies improve, deepfake creation techniques also become more advanced, resulting in a continuous cycle that makes regulation challenging. Legal frameworks, which typically require lengthy legislative processes, often struggle to keep up with these rapid technological changes.

Another important concern is the lack of awareness among legal stakeholders. Judges, lawyers, and law enforcement officials may not always be fully informed about the capabilities and risks associated with deepfake technology. Without proper training, there is a risk that synthetic evidence may be accepted at face value, particularly in cases where the manipulation is subtle and not immediately apparent.

Procedural limitations also contribute to the problem. Digital forensic examinations can be time-consuming and expensive, which may discourage parties from seeking verification in routine disputes. Courts handling large numbers of cases may not have the resources to conduct detailed forensic analysis in every instance where digital evidence is presented. This practical limitation increases the likelihood that manipulated content may go undetected.

Furthermore, there is currently no standardized protocol for verifying suspected deepfake evidence in legal proceedings. The absence of clear procedural guidelines can lead to inconsistent practices across different courts. Some judges may insist on forensic verification, while others may rely on the credibility of the parties presenting the evidence. Such inconsistencies can create uncertainty and affect the uniform administration of justice.

The lack of legal clarity also raises broader concerns about trust in digital evidence. As awareness of deepfake technology grows, courts may become increasingly cautious in accepting electronic records, even when they are genuine. This could undermine the efficiency and convenience that digital evidence was intended to provide.

Overall, the challenges posed by deepfakes highlight a clear need for legal reforms that specifically address synthetic digital content. Without updated regulations, improved forensic capabilities, and greater awareness among legal

professionals, the gap between technological advancement and legal preparedness will continue to widen, potentially affecting the fairness and reliability of judicial outcomes.

Way Forward and Conclusion

The rapid development of deepfake technology presents a serious challenge to the justice system, particularly at a time when courts are increasingly dependent on digital evidence. While technological advancements have made communication easier and evidence more accessible, they have also created new risks that cannot be ignored. To ensure that the integrity of judicial proceedings is preserved, it is essential to adopt a proactive and well-balanced approach that addresses both technological realities and legal safeguards.

One of the most important steps forward is the need for clear legal recognition of deepfakes as a distinct form of digital manipulation. Existing laws relating to forgery and cyber offences provide a basic framework, but they do not specifically address the complexities of artificial intelligence–generated content. Introducing clear legal definitions and guidelines relating to synthetic media would help courts identify, categorize, and handle such evidence more effectively. Specific provisions dealing with the creation, distribution, and use of deepfakes for malicious purposes could act as a strong deterrent against misuse.

Strengthening digital forensic infrastructure is equally essential. Courts should have easier access to trained forensic experts and advanced technological tools capable of detecting manipulated digital content. Establishing specialized forensic units and promoting collaboration between legal institutions and technological experts would significantly improve the ability to verify electronic evidence. Faster and more reliable forensic processes would also help reduce delays in legal proceedings.

Another crucial area of reform is capacity building among legal professionals. Judges, lawyers, and law enforcement officers must be provided with regular training to understand how deepfake technology works, how it can be misused, and what indicators may suggest manipulation. Awareness programs and technical workshops can help bridge the knowledge gap between rapidly evolving technology and traditional legal practices. Such training would enable courts to evaluate digital evidence more critically and confidently.

Standardized procedural guidelines for handling suspected synthetic evidence would also improve consistency in judicial decision-making. Clear protocols regarding when forensic verification is required, how digital evidence should be collected, and how authenticity should be established would help prevent uncertainty and reduce the risk of inconsistent practices across different courts.

At the same time, it is important to maintain a balanced perspective. Not all digital evidence is unreliable, and excessive skepticism could undermine the efficiency of legal proceedings. The objective should be to strengthen safeguards without discouraging the legitimate use of electronic records. By combining technological awareness with legal caution, courts can continue to benefit from digital advancements while minimizing the risk of manipulation.

In conclusion, deepfake technology represents a significant new challenge for the legal system, particularly in areas where digital evidence plays a decisive role, such as matrimonial and criminal disputes. The increasing realism and accessibility of synthetic media make it essential for legal frameworks to evolve in response to technological change. Strengthening laws, improving forensic capabilities, enhancing professional awareness, and establishing clear procedural safeguards are critical steps toward ensuring that justice is not compromised by artificial manipulation. As technology continues to advance, the legal system must remain adaptable and vigilant to protect the fundamental principle that judicial decisions must always be based on truth and authenticity.

References

1. Information Technology Act, 2000 (India).
2. Indian Evidence Act, 1872 (as amended for electronic records).
3. Ministry of Electronics and Information Technology, Guidelines on Cyber Security and Digital Evidence, Government of India.
4. Ratanlal & Dhirajlal, the Law of Evidence, 27th ed. (LexisNexis, 2022).
5. Avtar Singh, Introduction to the Law of Evidence, 6th ed. (Eastern Book Company, 2021).
6. Susan Brenner, Cybercrime and the Law: Challenges, Issues and Outcomes (Northeastern University Press, 2019).
7. Danielle Citron, “Deepfakes and the New Threat to Truth,” (2019) 107 California Law Review.
8. Chesney & Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” (2019) 107 California Law Review.
9. National Crime Records Bureau, Cyber Crime in India Report (latest edition).
10. European Commission, Tackling Deepfakes and Disinformation: Policy Report, 2020.