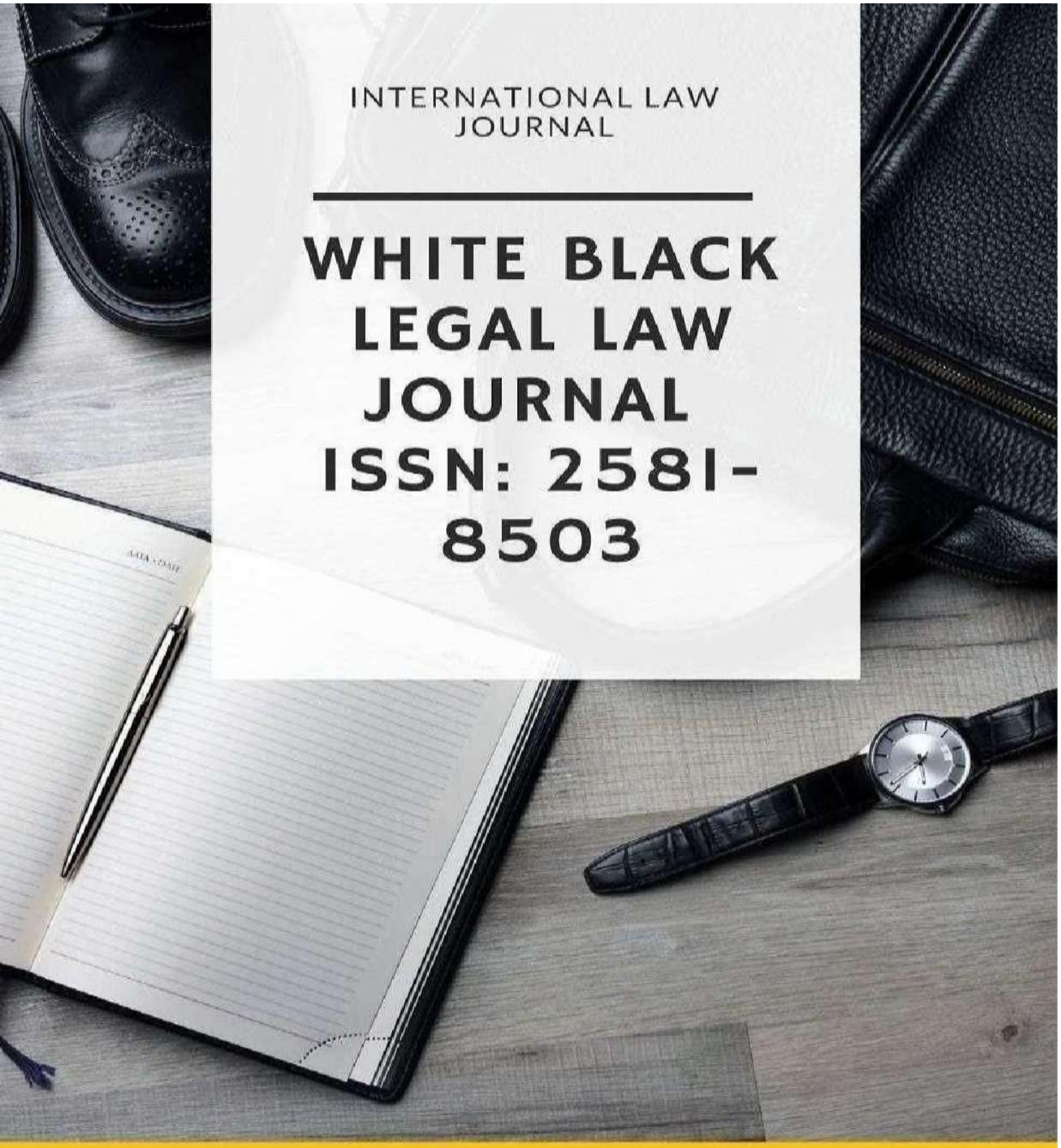

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB, LLM degrees from Banaras Hindu University & PHD from university of Kota. He has succesfully completed UGC sponsored M.R.P for the work in the Ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; PH.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St. Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,
Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing PH.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, PH.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, PH.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on CR.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); PH.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal provide dedicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 2 | Sep 2025 ISSN: 2581-8503

MANIPULATION OF ELECTRONIC EVIDENCE IN THE ERA OF AI AND RECENT CHALLENGES REGARDING DEEPFAKES AND MORPHED PICTURES

AUTHORED BY - RAAHUL TR
SEMESTER: 5TH
COURSE YEAR: 3RD YEAR
COURSE: B.COM LLB {HONS.}
PRESIDENCY UNIVERSITY, BANGALORE

TABLE OF CONTENTS

1) ABSTRACT

This research helps in studying the current issues relevant in the court of law, where the evidence is found of such a nature that it can be easily manipulated or be subject to manipulation due to the weak nature of data. This arises due to the increase in AI-driven tools, which not only make it easier but also ensure that such tools can create an accurate manipulation, leaving no inconsistencies. This study compares how indias legislative functions are holding up to this manipulation with other countries, and ensures to provides solution on how this can be easily combated by strengthening the verification methods of Evidence And how extra judicial measures can be utilised to find whether such evidence are real or falsified, this study provides a brief about one of the major rising issues regarding deepfakes and morphing of pictures, and how it affects the people and the court of law to interpret evidence. And lays down such penalties for the crimes regarding falsification of evidence, creation of morphed pictures, and deepfakes. This research helps in strengthening the judicial role of India to provide accurate decisions by admitting the proper evidence and not manipulated evidence, showcasing the strength that the court of law holds by providing accurate justice.

2) INTRODUCTION

The age of the Digital era has transformed how information is transformed, interpreted, and presented before the court of law. The electronic evidence, once one of the most crucial pieces of evidence due to the amount of electronic transactions and devices being utilised in modern times, has now become one of the most controversial pieces of evidence due to its being subject to manipulation. This happens due to the amount of technical and AI tools present. Courts highly depend on evidence like video, voice recording, or screenshots to facilitate fact-finding. But when such technologies are themselves subjected to manipulation it makes it very hard for the courts to admit such evidence. The rise of AI has not just increased risks for the court but also the risk to normal people, where we can see the increasing usage of Deepfakes and morphed images, where even if the person has not committed such an act, it can be artificially created to make such a person do Acts without proper authorisation or consent from the person. While our legal statutes do specify the laws about the verification of such evidence, this study provides how such verification is incomplete if compared with other nations, and is provided in a practical aspect. This study concludes by providing solutions for the court to ensure such misuse doesn't increase day by day and to put an end to such practices by ensuring proper authenticity measures are taken, technical measures, and legal measures are implemented to

uphold the legitimacy of decisions made by the judges in courts.

3) AIM OF THE RESEARCH

This study primarily investigates the validity of electronic evidence, which is increasingly susceptible to alteration in the digital and AI-dominated age. The central objective of this research is to explore how societal manipulation of social media or other electronic evidence occurs. Through methods such as fabricated screenshots, altered conversations, morphed images, and AI-generated deepfakes, this manipulation affects the admissibility under the Bharatiya Sakshya Adhiniyam 2023. Additionally, this research highlights the consequences of accepting manipulated evidence and examines how it hinders courts from delivering precise and consistent rulings. It also suggests a framework for legal, technical, and procedural measures to prevent issues arising from the acceptance of electronic evidence, thus maintaining the integrity of court decisions and preserving the evidential value of such electronic materials. The capacity to propose such solutions stems from the defined objective, which enables addressing fundamental issues and providing effective answers to them.

How can India firm up its legal and judicial infrastructure to avoid and detect tampering of electronic evidence by drawing lessons from global practices and implementing preventions, statutory clarifications, and remedies for guaranteeing quality justice?

4) RESEARCH METHODOLOGY

This research mainly adopts a qualitative approach with a proper review of academic literature, research papers, and reports in relation to the topic of how electronic content, which is presented as evidence in the court of law, can be easily manipulated, such as morphed images, deepfake content, and conversations between individuals. This study uses a doctrinal analysis of the existing laws and regulations governing the authentication of digital evidence and follows a comparative study to compare other nations, like the UK and the US, to find how they have adopted such legislation or steps to counter issues, and apply it in this study to find a mutual solution for India. This study also synthesises the legal and technical findings and different approaches taken, and analyses various studies to reach a conclusion and propose a practical reform that covers the practice of forensics, judiciary, and policy guidelines to improve the accuracy of evidence submitted to the court to uphold the supremacy of the decision rendered by the judges and ensure its consistency.

5) MANIPULATION OF ELECTRONIC EVIDENCE

The evidence, which is in electronic form and is admissible in court, is called electronic evidence. This may include text, emails, call logs, computer logs, surveillance footage, social media posts and content, screenshots, and instant messages. These hold a probative value that can be stored, transmitted, or transformed in digital form. This evidence has currently become one of the most crucial forms of evidence due to the number of people using electronic devices such as mobile phones, laptops, and cloud services, and transactions have also become way easier due to the electronic mode of transactions. Due to this usage, the legislative statutes have provided provisions for such evidence arising out of electronic devices like Bharatiya Sakshya Adhiniyam (BSA), 2023. This is the primary legislation governing evidence, replacing the Indian Evidence Act, 1872.[1] Under Section 57 of the BSA, electronic records are treated as primary evidence when produced directly for the court's inspection and carry the same weight as tangible evidence[2]. Under Section 63[3] of BSA, Electronic Records are Documents, it states that electronic records are to be treated as "documents" and permits the admission of them without the original being subject to compliance with some conditions.[4]

However even after the amount of rules and regulations we have for electronic evidence It's very easy for it to be created, manipulated and transformed hence making it easy to be manipulated, the physical document and evidence hold a greater value as they cannot be duplicated as easily as digital document as a duplicated tangible evidence or document would leave behind loss of quality which can be spotted easily, but in case of an electronic evidence this can be easily manipulated without leaving a trace. In the current era of technology, the court must be vigilant during the admission of electronic evidence, as it may be easily manipulated.

5.1 HOW CAN ELECTRONIC EVIDENCE BE MANIPULATED

[1] *Vanshika Kapoor*, All About Digital Evidence, *iPleaders (Feb. 23, 2024)*, *https://blog.ipleaders.in/all-aboutdigital-evidence/*.

[2] The Evolving Enigma: Electronic Evidence in India, *Vidhi Legal Policy (Apr. 2024)*, *https://vidhilegalpolicy.in/blog/the-evolvingenigma/#:~:text=Ultimately%2C%20the%20entire%20(older),weight%20as%20any%20tangible%20document*.

[3] *Bharatiya Sakshya Adhiniyam, 2023*, § 63, India Code, https://www.indiacode.nic.in/showdata?actid=AC_CEN_5_23_00049_2023-47_1719292804654&orderno=63 India Code+1

[4] *Sk. Shireen, Electronic Evidence (Dec. 2024), https://cdnbbsr.s3waas.gov.in/s3ec01a0ba2648acd23dc7a5829968ce53/uploads/2024/12/2024122766.pdf*. *CDN BBSR*

Electronic evidence can be easily manipulated as it is very easy to transform, store, and retrieve it. Making it prone to manipulation, the manipulated evidence could lead to a wrong decision if not decided with proper precaution and verification. The manipulation can be done in the following ways:

1. **Fabrication and editing**: Images which are presented to the court May be easily a subject to Fabricated Evidence as a simple editing software can change the reality of the evidence, screenshot of a text message from Instagram, WhatsApp, messenger or any other social media platforms may be edited or fabricated using word processing software or simple image editing as they can be easily manipulated by copying interface elements and adding new text messages or images. This issue is very core as manipulative evidence can very much cause harm to the proceedings, and by gaining unfair advantage, this highlights the necessity for the courts to take into account a certificate before admission of any electronic evidence, especially in the era of AI, where it's very easy to manipulate such evidence with a simple prompting.
2. **Data Tampering**: Here, the simple details of the data stored in the evidence can be easily tampered with, for instance, with hex editors[5], which can edit the details where geolocation, date of creation, and other details can be modified to misrepresent such data. This shows how the details must be cross-verified rather than accepting primary details as it is; thorough investigation and helpful tools from the internet can help in verification.
3. **Deep Fakes and Morphed pictures**: in the current era of modern technology and AI, the advances seen in machine learning are phenomenal to the extent that they can create highly realistic videos or audio in which an event that has not occurred occurs. Morphed pictures are when a user blends multiple images into one using a face-swapping technique to create defamatory or misleading remarks, but these images and videos lack accuracy, leaving certain details to identify their artificial creation, showcasing a need for proper checking of any video or image evidence provided to the court.
4. **Cyber-attacks and data alteration**: Cyber-attacks are a very common threat when the nature of data is versatile or vulnerable, leaving it prone to being altered

[5] Alex, *What Is a Hex Editor and How to Use It*, UltraEdit Blog (Dec. 20, 2022), https://www.ultraedit.com/blog/what-is-a-hex-editor-and-how-to-use-it/.

or modified. This show cases the importance of safeguarding such data to ensure no cyberattacks occurs and the data can be showcased as evidence in the court but if not protected and the data was attacked, it would be very hard to prove in court such attack had occurred, sophisticated hackers ensure to manipulate the hash[6] values of the files which if they gain access before the hashes are done then it may undermine integrity checks.

5. **Implications for court**: these forms of manipulation help in understanding the very nature of the evidentiary value electronic evidence upholds, but the issue arises when it's manipulated or misused to be used in favour of the party. That being said, the courts must at all times ensure to double-check this evidence admitted, try getting expert opinions, and also check the authenticity. As the technology evolves, the judiciary must also evolve with its viewpoint to uphold the fruits of litigation.

5.2 Relevant cases:

i. [7]***Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India).***

Here, the court provided that the electronic records always require a proper certificate to ensure their authenticity, setting the precedent that electronic records are admissible only if accompanied by proper certification. And set the baseline of authentication requirements.

ii. ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India).***[8]

The court clarified that a Section 65 B (now 6(4) of BSA 2023) certificate is always mandatory unless the device is itself presented in court.

iii. Sabu Mathew George v. Union of India, (2018) 3 SCC 229[9]

Here, the responsibility of the Internet was undermined during the discussion of an advertisement for sex determination and to prevent misuse of Digital Platforms for usage like Deep fakes, etc.

---

[6] Pass the Hash Attack, CrowdStrike (n.d.), https://www.crowdstrike.com/en-us/cybersecurity101/cyberattacks/pass-the-hash-attack/.

[7] Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 S.C.C. 473 (India), discussed in *Preservation of E-Documents*, iPleaders, https://blog.ipleaders.in/preservation-of-e-documents/#:~:text=The%20defendants%20relied%20heavily%20on,Section%2065%2DB%20are%20met.

[8] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1, PDF judgment available at https://aphc.gov.in/docs/imp_judgements/Arjun%20Panditrao%20Khotkar%20_%20Kailash%20Kushanrao%20Gorantyal%20And%20Ors._1701334263.pdf Aphc

[9] Sabu Mathew George v. Union of India, *(2018) 3 S.C.C. 229, available at https://indiankanoon.org/doc/192654466/*.

iv. **State of Maharashtra v. Dr Praful B. Desai**, (2003) 4 SCC 601[10]

Recognised the admission of the video conferencing as valid evidence, but ensured the authenticity was there, while the admission Even though the current legal statute called as Bharatiya Sakshya Adhiniyam strictly recognises the electronic records as admissible evidence under section 63[11] of BSA and requires a certificate for admission under 63(4)[12], but the major key factor here is that the evidence can still be exposed to sophisticated Manipulation, screenshots can be easily modified using basic editing tools, the images and videos can be easily created which can stimulate actions that never occurred, the data can be altered using hex editors, these technical possibilities must be examined thoroughly by the court of law before admission of evidence. The primary safeguard that is provided by the legal statute is the manner in which copies are presented for such electronic evidence, but not whether the underlying content itself is genuine.

The certificates which is required for admitting such evidence can also be subject to manipulation and difficult to obtain as it can be forged and in the recent emergence of AI it has been one of the most eye opening topics in studies relating to how data's are easily manipulated by a simple text, how easily deepfakes and morphed images are created, which could result in a greater extent of exploit if not used in moderation.

1. **KHALID VS DELHI POLICE (2025)[13]**

In this case, a former JNU student's lawyer had claimed that applicable evidence was used in 17 cases, which were related to the 2020 New Delhi riots. Here, the court found multiple months after the arrest of Khalid. Suggestive manipulation. Out of 750 cases, 93 ended in an acquittal. And in 17 cases, it was indicated that fake evidence and unreliable witnesses were used.

[10] State of Maharashtra v. Dr. Praful B. Desai, *(2003) 4 S.C.C. 601, available at https://indiankanoon.org/doc/560467/.*
[11] *Bharatiya Sakshya Adhiniyam, 2023*, § 63, India Code, https://www.indiacode.nic.in/showdata?actid=AC_CEN_5_23_00049_2023-47_1719292804654&orderno=63
[12] *Bharatiya Sakshya Adhiniyam, 2023*, § 63(4), Indian Kanoon, https://indiankanoon.org/doc/90089205/ (last accessed Sept. 28, 2025).
[13] Khalid Courts Found Fake Evidence in 17 Riots Cases, *Times of India* (Sept. 15, 2025), https://timesofindia.indiatimes.com/city/delhi/khalid-courts-found-fake-evidence-in-17-riotscases/articleshow/124097389.cms.

2. **REKHA DEVI VS STATE OF UTTAR PRADESH (2025)[14]**

   Here, Rekha Devi had falsely accused 2 men of gang rape, but later found that the electronic evidence, including mobile phone data and location, was inconsistent with her claims, leading to a conviction for false accusation.

3. **NOIDA POLICE'S DIGITAL EVIDENCE COMPLIANCE (2025)[15]**

   Despite the existing laws, the Noida police had shown poor compliance with the mandatory digital evidence requirement, as of the 7322 FIRs filed between 1st July 2024 and 1st July 2025, only 13% were uploaded with digital evidence via the E-Sakshya platform, and the low compliance rate raised concerns about the authenticity of digital evidence in legal proceedings.

   These cases showcase the authenticity of digital and electronic evidence in the current world and showcase how it has been misused, even though there are existing provisions.

6) HOW TO DETECT AND PREVENT MANIPULATION OF EVIDENCE

In the modern era of AI and technology it has become very easy to manipulate any sort of electronic or technical substance from the original matter, the rapid increase in usage of AI has resulted not just in a positive manner but is inversely increasing negatively, the increase in AI driven deepfakes and morphed images has increasingly become an issue for the modern society where its used to defame people or used in court proceedings to falsify facts and get the judgement in favour. Though this misuse is on a large scale, it hasn't confined any authorities to determine whether the work is artificial or not. Court investigators and forensic professionals must develop these tools and protocols during the procedures to ensure the evidence is not tampered with and render expert analysis whenever required.

6.1) DETECTION TECHNIQUES

1) **AI DEEPFAKE DETECTION:**

[14] Electronic Evidence Exposed Complainant's Claims, *Times of India* (Aug. 20, 2025), https://timesofindia.indiatimes.com/city/lucknow/electronic-evidence-exposed-complainantsclaims/articleshow/121893376.cms.

[15] 7.3K FIRs Filed by Noida Cops in 1 Year Since BNS Rollout, but Digital Evidence Only in 13%, *Times of India* (Sept. 14, 2025), https://timesofindia.indiatimes.com/city/noida/7-3k-firs-filed-by-noida-cops-in-1-year- sincebns-rollout-but-digital-evidence-only-in-13/articleshow/124056031.cms.

Recent technological advances have prompted both positive and negative responses. The main negative issue is the proliferation of defective videos and synthetic media that can convincingly depict a person performing actions they never did. This undermines reliable visual inspection. However, these can be detected by analysing subtle clues in the video, checking frame by frame for inconsistencies, or identifying irregular lip movements, unnatural gestures, blinking patterns, and issues with quality and realism in videos and audios. Some tools assist in analysing these problems more effectively, such as:

1. Microsoft video authenticator[16]
2. McAfee Deepfake detector [17]
3. FaceForensics++[18]

These can be must at all times be utilized by the courts before admitting such evidence to ensure it holds the probative value and is not fake or artificial in nature, but the issue arises when the court interprets the law as it unverified, leaving a massive loophole to be exploited by the parties with technological access while the ones against whom such evidences are laid suffer.[19]

2) CRYPTOGRAPHIC HASHING:

Hashing ensures the creation of a unique and fixed-size fingerprint of any data to verify its integrity, and it ensures the integrity of such digital signatures by using a combination of hashing and asymmetric (public/private key) cryptography to authenticate a sender's message and prevent it from being tampered with.[20]

The major purpose is to authenticate the sender's identity and to ensure that the integrity of the message, data, or document is maintained.

[16] Jordan Cortado, Digital Forensics Techniques to Detect Deepfakes, UNIVERSITY OF HAWAI'I-WEST O'AHU CYBERSECURITY, https://westoahu.hawaii.edu/cyber/forensics-weekly-executivesummmaries/digital- forensics-techniques-to-detect-deepfakes/ (Oct. 11, 2024).
[17] Jordan Cortado, Digital Forensics Techniques to Detect Deepfakes, UNIVERSITY OF HAWAI'I-WEST O'AHU CYBERSECURITY, https://westoahu.hawaii.edu/cyber/forensics-weekly-executivesummmaries/digital- forensics-techniques-to-detect-deepfakes/ (Oct. 11, 2024).
[18] Jordan Cortado, Digital Forensics Techniques to Detect Deepfakes, UNIVERSITY OF HAWAI'I-WEST O'AHU CYBERSECURITY, https://westoahu.hawaii.edu/cyber/forensics-weekly-executivesummmaries/digital- forensics-techniques-to-detect-deepfakes/ (Oct. 11, 2024).
[19] Lawful Legal**,** *AI-Generated Evidence in Indian Courts: The Next Legal Frontier*, https://lawfullegal.in/aigenerated-evidence-in-indian-courts-the-next-legal-frontier/ (last visited Sept. 28, 2025).
[20] "Digital Signatures in Cryptography: Everything You Need to Know," HyperVerge Blog (Mar. 20, 2025), https://hyperverge.co/blog/digital-signatures-in-cryptography/.

The process of cryptographic hashing: at first, the Hash of the document is created, and then the encryption takes place, where the recipient receives a signed document and an encrypted signature. The recipient also must verify the document, then the recipient uses the sender's key to decrypt such a signature, revealing the document. Making it a more protected process and preventing any sort of 3rd party tampering.

3) **DATA LOGGING:**

Every file always consists of a record of details that tell about its origin, modification, and the geolocation at times. This is called metadata, which can be used to ensure the veil of inconsistencies can be lifted, causing such files to be exposed to tampering, as such details will provide a timestamp of creation date and EXIF data, which shows how the tampered data is different. The system and the data logs can be utilised in a manner to track he history of files, which helps in accessing various transfers, the number of times it was accessed, and the edits that occurred in such a file. There can be a misuse even in metadata, which decreases the likelihood of detection of the data being tampered with.

6.2 PREVENTIVE MEASURES FOR COURTS:

1. ***Investigative training and***
2. **judicial interpretation:**

To ensure there is proper detection of the digital evidence, and the use of not only technical tools but also the help of expert tools to facilitate judges, prosecutors, and investigators. To train such experts to ensure no such inconsistency is found between their diligence and the investigation, this can be done by training in understanding the features of modern manipulation techniques and using forensic tools to determine if such evidence is manipulated or not. This awareness is very necessary as in the current world of technology, where the majority of affairs happen through electronic devices, it leaves a wide window open to possibilities of misuse.

3. ***Use of the current technologies***

Beyond the forensics, the court can utilise publicly available technologies to combat such manipulation. Emerging technologies, such as blockchain-based logging of digital evidence and AI tools, offer safeguards. This helps in the creation of AI monitoring tools, which help in monitoring, evaluating, and detecting suspicious alterations in evidentiary records, flagging the tampering before it is admitted in the court of law.

4. *Appointing technical forensic experts*

The court may at times order a requirement of an expert's opinion on a particular matter which the court after trying all the test are not able to identify such manipulation and if the case is involving high stakes or high usage of technical evidences then these decisions on whether if it is manipulated evidence or not can be easily determined by rendering an opinion from the forensic experts who may help the courts in identifying the meta data integrity, may use the technical tools which could be helped to assess the true reality of such evidence and ensure no such evidence are not manipulated or misused or tampered. The use of such an expert may arise out of the qualification of the person, as the expert might have given the opinions before or is highly specialised in such a field, the case revolves around. But one must ensure there exists no bias, and such an opinion of an expert is taken into account only if evaluated, verified, and properly supervised.

1. ENSURING PROPER SECURITY:

When evidence is being collected by the court, it must be properly protected; all evidence must be properly protected, stored, and transferred according to the chain of custody rules. This includes the documents filed by the forensics, evidence for rebuttals, and also the evidence provided by the parties, to ensure no such tampering is committed by the 3rd party. At all times, this evidence must be provided for surveillance and proper vigilance by setting up security to prevent unauthorised access. Evidence that holds a significant value must be taken with more care as well.

The combination of these steps can be utilised by the court of law to prevent any unlawful or unauthorised tampering or manipulation of data. This upholds the safety and security provided by the judiciary, entrusting people to submit evidence in full confidence and to ensure no artificial or manipulated evidence is admitted.

1) Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473[21]

THE SUPREME COURT ruled that for the electronic evidence to be admissible, its integrity must be ensured through certification, and proper collection of such documentation is a preventive measure.

1. **Tomaso Bruno v. State of Uttar Pradesh**, (2015) 7 SCC 178[22]

[21] *Anvar P.V. v. P.K. Basheer*, (2014) 10 S.C.C. 473, available at https://aphc.gov.in/docs/imp_judgements/Anvar%20PV%20case.pdf

[22] *Tomaso Bruno & Anr. v. State of U.P.*, (2015) 7 S.C.C. 178,

The court criticised the failure of the investigating agency to produce the required electronic evidence and stressed how important the forensic and scientific methods are for the evidence collection.

These two cases understand how the judicial interpretation towards evidence and the necessity of evidence takes place, making it significant for courts to practise preventive measures in the modern era of AI and technology to ensure it's not being misused at large and to also ensure that such misuse does not harm any parties.

7) STRENGTHENING OF THE PROBATIVE VALUE OF ELECTRONIC EVIDENCE

Evidence getting manipulated is very much a practical issue currently in the court of law due to the amount of usage done by people, and the growing nature of AI manipulation of evidence has become more complex and hard for courts to analyse and interpret their decisions based on the evidence presented. The rising issues like Deepfakes and sophisticated manipulation of evidence result in the need for a proper legislative provision preventing such actions. The growing India has always updated its laws as needed; these laws provide a pathway to admit electronic evidence in a much wider scope, outlining the institutional capacities and protecting the justice system.

1. STAUTORY FRAMWORK:

Section 63 of BSA[23] addresses electronic records as "documents", and section 63(4)[24] requires the person submitting such electronic evidence above to present a certificate of authenticity when the original work is not produced. Although these sections are relevant, they leave an inconsistent remark in context to the manipulation of the evidence, and only admit such evidence that is original with the certification, showcasing how the person must prove the authenticity of original evidence.

K. Ramajayam v. Inspector of Police, 2016 SCC OnLine Mad 3869[25]: The Madras

available at https://digiscr.sci.gov.in/view_judgment?id=NDM4OQ%3D%3D

[23] *Bharatiya Sakshya Adhiniyam, 2023*, § 63, India Code, https://www.indiacode.nic.in/showdata?abv=CEN&actid=AC_CEN_5_23_00049_2023-47_1719292804654&orderno=63 (last accessed Sept. 28, 23).

[24] *Bharatiya Sakshya Adhiniyam, 2023*, § 63(4), Indian Kanoon, https://indiankanoon.org/doc/125020475/ (last accessed Sept. 28, 2025).

[25] *K. Ramajayam @ Appu v. The Inspector of Police*, (2016) Madras High Court, SCC OnLine Mad 451, available at https://indiankanoon.org/doc/179639914/.

High Court here held that the court requires proper certification and proof of electronic evidence before relying on such evidence.

This showcases how the judicial and legal interpretation of preventing electronic evidence is seen, but the crucial part is that such certificates can be subject to forgery and manipulation, making it a huge burden for the judiciary to render quality decisions.

2. **USE OF EXPERTS**

If there is a speculation of tampering with the evidence, the court has the proper authority to fulfill the interest of the court proceedings with the use of an expert witness in digital forensics to ensure that such inconsistencies are solved and render proper opinions on such speculation of the authenticity of evidence. This shows that mere judicial and legal interpretation is not necessarily enough and can be sorted in an efficient manner by discussing with an expert.

State of Kerala v. P. B. Sourabhan, 2016 SCC OnLine Ker 27939[26]: the High Court of Kerala took an expert testimony from a government forensic laboratory to establish that the audio was not altered. This shows how external roles can play a pivotal role in a court proceeding with mere advice or opinion.

3. **TECHNICAL COUNTERPOINTS:**

The Age of AI-driven forensic tools to check the validity of evidence is another better, cheaper, and efficient option for the courts to conclude, as this resolves the need for an efficient workforce or delay in judgment, and can be decided faster. Pilot projects in India's national cyber forensics lab employ the blockchain-based evidentiary chains, which help in storing hash values to prevent undetected alterations.

But the necessary steps to ensure such a tool is reliable are to ensure such tools are publicly trusted and utilised on a large scale to build such trust. If an unreliable tool is used and the wrong decision is rendered, then such wrongful evidence could also be admitted by the court.

4. **POLICY FRAMEWORKS**

Several high courts have issued the (SOPs) Standard Operating Procedures[27]. Requiring the investigators to use accredited cyber forensic laboratories and to ensure preservation of such evidence in storage. This highlights how the judiciary and forensic are evolving

[26] *State of Kerala v. P. B. Sourabhan & Ors.*, Criminal Appeal No. 192 of 2016, Supreme Court of India, Mar. 4, 2016, available at https://www.legalauthority.in/judgement/state-of-kerala-vs-p-b-sourabhan-3695.

[27] *What Is a StandardOperating Procedure (SOP)?*, American Express, https://www.americanexpress.com/enus/business/trends-and-insights/articles/agile-business-strategy-making-room-for-standard-operatingprocedures/ (last visited Sept. 28, 2025).

as per the evolution of AI and other significant technologies, making it easier for courts to render decisions and to determine the integrity of any data.

7.2 PENALTIES UNDER THE EXISTING LEGAL FRAMEWORKS

The Information Technology Act, 2000, provides a list of penalties[28]

SECTIONS	OFFENCE	PUNISHMENT
SECTION 65	Tampering with computer source code	Fine up to 2 lakh and up to 3 years of imprisonment, or both
SECTION 66C	Identity theft, including the unauthorized use of digital signatures	Up to 3 years of imprisonment and a fine of up to 1 lakh
SECTION 66 D	Cheating by personation through computer resources	Imprisonment up to 3 years and a fine of up to 1 lakh
SECTION 72	Breach of confidentiality and privacy of electronic records	Imprisonment up to 2 years or a fine of up to 1 lakh, or both

8. COMPARATIVE ANALYSIS

Electronic evidence has become one of the most central topics not just in India but also in countries with various jurisdictions. These countries have issues revolving around the manipulation of electronic evidence. Many countries have utilized a different approach, highlighting how India could develop or provide us with certain lessons to ensure India's legal and judicial framework is strong and functioning.

UNITED STATES

The US relies on(the federal rules of evidence 901)[29], which ensures the electronic evidence is authenticated by reasonable means, like expert testimony or distinctive characteristics. This approach is broad and flexible, ensuring proper reliability. This showcases how the US does not require a proper certification but requires, moreover, the reliability of such evidence. This could be adopted by the Indian courts to ensure that evidence is reliable on the basis of reasonable means rather than mere certification.

[28] *Information Technology Act, 2000*,https://www.meity.gov.in/static/uploads/2024/03/ITbill_2000.pdf.
[29] *Federal Rules of Evidence Rule 901* (Fed. R. Evid. 901), https://www.law.cornell.edu/rules/fre/rule_901.

***United States v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014)[30]**

The court here admitted Records from Silk Road servers, which relied on Heavy Expert testimony to authenticate the particular data. This shows us how the US emphasizes forensic verification, rather than a mere certificate.

UNITED KINGDOM

The UK relies heavily on demonstrating the reliability of certain evidence, which is presented to the court by evidentiary protocols, Reports of Experts, and security in documentation, being the central topics of the admissibility under the UK's Civil Evidence Act 1995[31].

***R v. Andrews* [2013] EWCA Crim 1562[32]:** Here, the Court of Appeal Examined Electronic evidence, stressing the need to demonstrate the reliability and expert verification, but not statutory certification

The major insights for India from these countries are that to adopt a more reliable process than just a certificatory process, as such a certificatory process may be subject to Forging of the certificate or manipulation of the certificate, Whereas The reliability increases when the evidence is proved or authenticated via reasonable circumstances.

9) DEEPFAKES AND MORPHING OF IMAGES.

In recent times, in society, defects and morphing of images have been very much relevant, creating a lot of issues, both legally and morally. Our current society has created a lot of rules and regulations to battle this issue. By laying down foundational rules against such evidence, which is fabricated, being highly realistic, it introduces legal and procedural challenges.

9.1 LEGAL PROVISIONS

Section 63 (4) of BSA[33] provides that digital evidence must be given with a certification under the provision from the party who require such facts to be proven in court. This helps in ensuring

[30] *United States v. Ulbricht*, 31 F. Supp. 3d 540 (S.D.N.Y. 2014), available at https://public.fastcase.com/HAaWKTwxGB4e4tJdZb2xpLvt6T1wAsWbI1hoQpY33MZvAU3xikWlneF9uPdRxvDxi 97oCOMVAtRcpogOwGJqYg%3D%3D.

[31] *Civil Evidence Act 1995*, https://www.legislation.gov.uk/ukpga/1995/38/contents/enacted.

[32] *R v. Andrews*, [2013] EWCA Crim 2750, available at https://www.casemine.com/judgement/uk/5a8ff7ac60d03e7f57eb1156.

[33] *Bharatiya Sakshya Adhiniyam, 2023*, § 63(4) (India), https://www.indiacode.nic.in/showdata?actid=AC_CEN_5_23_00049_2023-47_1719292804654&orderno=63.

the authenticity of the data. Information Technology Act, 2000 (IT Act) Section 66E[34] criminalizes the offense of privacy by capturing or Publishing Images without any consent, showcasing how such generation of deepfakes can be prevented with proper legal measures. Section 67[35] prohibits the publication of obscene material in electronic form, which can encompass the morphed or deepfake images published with the intent to defame. The Digital Personal Data Protection Act, 2023 (DPDP)[36] Framework helps in safeguarding personal data, which can be used in cases where the usage of deepfakes or morphed pictures is involved. Though the courts won't allow electronic evidence unless and until it is backed by a certificate to preserve authenticity, here we see a gap and a clear ignorance in law, as these provisions do not explicitly address the issues posed by deepfakes and morphed images, which undermines the authenticity.

9.2 POTENTIAL MISUSE AND SOCIAL HARM:

Deepfakes can be used to defame, harass people, or to intentionally spread false narratives, and can also be used to extort others, which can undermine public trust and be subject to misuse on a large scale, causing social harm. The current frameworks must incorporate preventive measures as well as remedial actions, and impose stricter penalties to ensure the strict prevention of the creation of Deepfakes or morphed images. In this rapid era of technological advancement, sophisticated morphing, voice cloning, and facial synthesis can be easily created. The legal system must adopt dynamic protocols for forensics to ensure proper detection of AI-driven tools, as relying solely on statutes is insufficient. Courts often need broader interpretations, which can foster consistency in judicial decisions with society and raise important societal questions about liability. Judges, lawyers, and investigators may lack the necessary technical expertise. To distinguish real from manipulated content, I may not be able to detect defects in morphed pictures. This gap creates risks for civil and criminal cases. In many instances, these defaced and morphed images are used obscenely to defame or harm a person's reputation. Here, the issue is not just about the individual's identity but also about their image in society, which is severely impacted. This demonstrates how AI tools and technical means, when used irresponsibly, can cause adverse effects not only to individuals. This

[34] *Information Technology Act, 2000*, § 66E (India), https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=81.
[35] *Information Technology Act, 2000*, § 67 (India), https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=83.
[36] *Digital Personal Data Protection Act, 2023* (India), https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf.

highlights the current state of legislation and the challenges of potential misuse leading to social harm from Deepfakes and morphed images. It also shows how India is progressing in efforts to prevent and address this issue. To effectively deter and rectify such acts, India needs to develop a stricter legal framework that ensures such acts are not repeated and that proper forensics are available to evaluate electronic evidence. This is essential to prevent the presentation of false evidence, as deepfakes and morphed images can produce realistic content that did not actually occur.

9.3 CASE ANALYSIS

1) Blackmail Using Morphed Images in Rajasthan[37]

In August 2024, a man was arrested in Barmer, Rajasthan. He was caught blackmailing a woman using AI-generated morphed photos. The father had later revealed that He found 10 to 15 edited obscene videos and photos of his daughter on WhatsApp, accompanied by a threat of demanding money. The police had identified the suspect, and through technical analysis of the IP address and WhatsApp details, found him in possession of the phone, which was used to commit the crime.

This case helps us to identify how the amount of defects and morphed images is used for extortion and threats in order to gain benefits, such as financial benefits or any other benefits. This can be decreased by proper legal statutory frameworks, providing stricter penalties for any such ads committed, like deepfakes or morphing of pictures.

10) CONCLUSION

This study concludes by finding that the Manipulation of electronic evidence is one of the most commonly occurring issues for the court of law due to the emerging mass use of AI and technical tools to edit and manipulate such electronic evidence. This study provides how such courts can practise extra legislative and judicial functions to ensure the manipulation is reduced by implementing methods of proper authenticity tests. By rendering services from forensics when required in cases, as not all functions can be rendered by the judges, this method helps in reducing the burden on the judges. This study addresses the common issue, which is a central controversy in the courts of law, regarding morphed pictures and deepfakes, which can harm the reputation of an individual in society by doing certain acts the person claims to never have

[37] Times of India. Man held for blackmailing woman via morphed pics. *Times of India*, Aug. 28, 2024. https://timesofindia.indiatimes.com/city/jaipur/man-held-for-blackmailing-woman-via-morphedpics/articleshow/124199844.cms.

done. This study provides measures to adopt to identify the ground reality of such deepfakes and morphed pictures by the actions or by measures using the current existing technical tools to identify. These measures help in reducing the burden on the judiciary and ensure the accuracy of decisions by the courts, and uphold the legitimacy and supremacy of decisions.

11) BIBLIOGRAPHY

Cases

1. Anvar P.V. v. P.K. Basheer**,** (2014) 10 S.C.C. 473, available at https://indiankanoon.org/doc/187283766/.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal**,** (2020) 7 S.C.C. 1, PDF judgment available at https://aphc.gov.in/docs/imp_judgements/Arjun%20Panditrao%20Khotkar%20_%20Kailash%20Kushanrao%20Gorantyal%20And%20Ors._1701334263.pdf.
3. Sabu Mathew George v. Union of India**,** (2018) 3 S.C.C. 229, available at https://indiankanoon.org/doc/192654466/.
4. State of Maharashtra v. Dr. Praful B. Desai**,** (2003) 4 S.C.C. 601, available at https://indiankanoon.org/doc/560467/.
5. K. Ramajayam @ Appu v. The Inspector of Police, (2016) Madras High Court, SCC Online Mad 451, available at https://indiankanoon.org/doc/179639914/.
6. State of Kerala v. P. B. Sourabhan & Ors.**,** Criminal Appeal No. 192 of 2016, Supreme Court of India, Mar. 4, 2016, available at https://www.legalauthority.in/judgement/state-of-kerala-vs-p-b-sourabhan-3695.
7. Tomaso Bruno & Anr. v. State of U.P.**,** (2015) 7 S.C.C. 178, available at https://digiscr.sci.gov.in/view_judgment?id=NDM4OQ%3D%3D.
8. Times of India**,** *Man held for blackmailing woman via morphed pics*, Times of India, Aug. 28, 2024, https://timesofindia.indiatimes.com/city/jaipur/man-held-forblackmailing-woman-via-morphed-pics/articleshow/124199844.cms.
9. United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014), available at https://public.fastcase.com/HAaWKTwxGB4e4tJdZb2xpLvt6T1wAsWbI1hoQpY33MZvAU3xikWlneF9uPdRxvDxi97oCOMVAtRcpogOwGJqYg%3D%3D.
10. R v. Andrews**,** [2013] EWCA Crim 2750, available at https://www.casemine.com/judgement/uk/5a8ff7ac60d03e7f57eb1156.

Statutes & Acts

1. Bharatiya Sakshya Adhiniyam, 2023, § 63, India Code, https://www.indiacode.nic.in/show-data?actid=AC_CEN_5_23_00049_202347_1719292804654&orderno=63.
2. Bharatiya Sakshya Adhiniyam, 2023, § 63(4), Indian Kanoon, https://indiankanoon.org/doc/125020475/.
3. Information Technology Act, 2000, § 66E, India Code, https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=81.
4. Information Technology Act, 2000, § 67, India Code, https://www.indiacode.nic.in/showdata?actid=AC_CEN_45_76_00001_200021_1517807324077&orderno=83.
5. Digital Personal Data Protection Act, 2023, India, https://www.indiacode.nic.in/bitstream/123456789/20063/1/a2023-47.pdf.
6. Federal Rules of Evidence Rule 901 (Fed. R. Evid. 901), https://www.law.cornell.edu/rules/fre/rule_901.
7. Civil Evidence Act 1995 (UK), https://www.legislation.gov.uk/ukpga/1995/38/contents/enacted.

Articles & Reports

1. Lawful Legal, *AI-Generated Evidence in Indian Courts: The Next Legal Frontier*, https://lawfullegal.in/ai-generated-evidence-in-indian-courts-the-next-legal-frontier/.
2. HyperVerge Blog, *Digital Signatures in Cryptography: Everything You Need to Know*, Mar. 20, 2025, https://hyperverge.co/blog/digital-signatures-in-cryptography/.
3. Vanshika Kapoor, *All About Digital Evidence*, iPleaders, Feb. 23, 2024, https://blog.ipleaders.in/all-about-digital-evidence/.
4. Sk. Shireen, *Electronic Evidence*, Dec. 2024, https://cdnbbsr.s3waas.gov.in/s3ec01a0ba2648acd23dc7a5829968ce53/uploads/2024/12/2024122766.pdf.
5. Vidhi Legal Policy, *The Evolving Enigma: Electronic Evidence in India*, Apr. 2024, https://vidhilegalpolicy.in/blog/the-evolvingenigma/#:~:text=Ultimately%2C%20the%20entire%20(older),weight%20as%20any %20tangible%20document.
6. American Express, *What Is a Standard Operating Procedure (SOP)?*,

https://www.americanexpress.com/en-us/business/trends-and-insights/articles/agilebusiness-strategy-making-room-for-standard-operating-procedures/.

7. CrowdStrike, *Pass the Hash Attack*, https://www.crowdstrike.com/enus/cybersecurity-101/cyberattacks/pass-the-hash-attack/.
8. UltraEdit Blog, *What Is a Hex Editor and How to Use It*, Dec. 20, 2022, https://www.ultraedit.com/blog/what-is-a-hex-editor-and-how-to-use-it/.
9. Information Technology Act, 2000 (full text PDF), https://www.meity.gov.in/static/uploads/2024/03/ITbill_2000.pdf