INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 6 AND ISSUE 9 OF 2026

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 6 and Issue 9 of 2026 (Access Full Issue on - https://ijlr.iledu.in/volume-6-and-issue-9-of-2026/)

Publisher

Prasanna S,

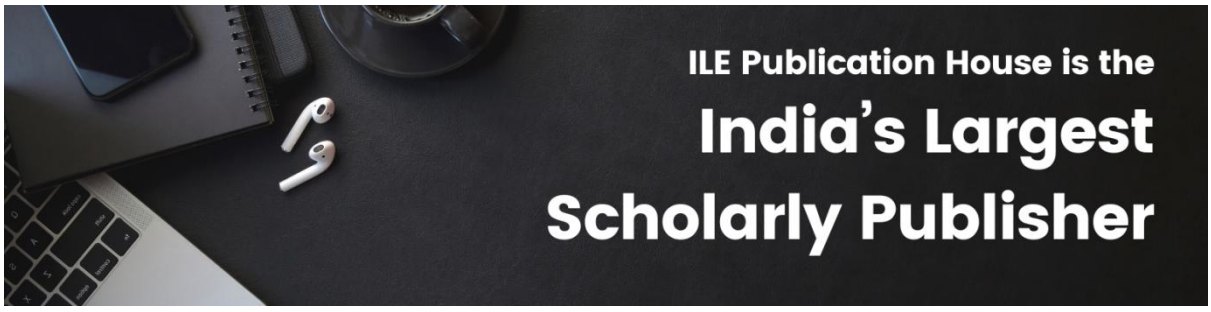
Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in



INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

FORENSIC AUDIO-VIDEO EXAMINATION AND SPEAKER IDENTIFICATION: INVESTIGATIVE AND EVIDENTIARY CHALLENGES IN INDIA

AUTHOR - YAZHINI V, LL.M., DEPARTMENT OF CRIMINAL LAW, TAMIL NADU DR. AMBEDKAR LAW UNIVERSITY, CHENNAI

BEST CITATION – YAZHINI V, FORENSIC AUDIO-VIDEO EXAMINATION AND SPEAKER IDENTIFICATION: INVESTIGATIVE AND EVIDENTIARY CHALLENGES IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 6 (9) OF 2026, PG. 312-322, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/IJLRV6I936

ABSTRACT:

Technology has changed the way of crimes that are committed and investigated nowadays. In recent years, audio and video recordings are playing an important role as a sources of evidence in criminal investigations. CCTV footage, mobile phone recordings, social media videos, online communications, and voice recordings are frequently used by investigating agencies to identify suspects and understand criminal activities.

Forensic audio-video examination helps the experts to analyse, improve, and verify the authenticity of audio and video recordings. Speaker identification helps investigators to identify a person by comparing voice samples and analysing speech characteristics. These techniques are commonly used in cases involving terrorism, kidnapping, cybercrime, organised crime, corruption, extortion, and financial fraud. They assist investigating agencies in identifying the suspects, reconstructing crime scenes, and collecting reliable evidence.

However, the increasing use of digital evidence has also created many challenges. Audio and video recordings can be edited, manipulated, or fabricated using modern software and artificial intelligence. Deepfake technology has made it easier to create fake voices and videos that looks genuine. Issues relating to authenticity, privacy, reliability, and admissibility of electronic evidence have become major concerns in criminal investigations and court proceedings.

This paper examines the role of forensic audio-video examination and speaker identification in criminal investigations in India. It analyses the methods, tools and techniques used in forensic examination, the importance of digital evidence, and the challenges faced by investigators and courts. The paper also discusses the legal framework governing electronic evidence and important judicial decisions relating to admissibility.

Keywords Forensic Audio Analysis, Video Forensics, Speaker Identification, Electronic Evidence, Criminal Investigation.

CHAPTER I

1.1 INTRODUCTION:

Mostly no person could escape from using technology, as it has changed almost every aspect of human life, including the way crimes are committed and investigated. Earlier, criminal investigations mainly depended on eyewitness testimony, confessions, fingerprints, and other physical evidence. But, with the rapid growth of digital technology, audio and video recordings have become important sources of evidence in criminal cases. Mobile phones, CCTV cameras, surveillance systems, social media platforms, and internet-based communication have made

it easier to record and store information related to criminal activities.

In modern criminal investigations, audio and video recordings are commonly used to identify suspects, establish facts, and reconstruct crime scenes. CCTV footage can help investigators trace the movements of accused persons, while audio recordings can reveal important conversations related to criminal activities. These digital records often provide valuable evidence that supports the investigation process and helps courts reach fair decisions.

Forensic audio-video examination is a branch of forensic science that focuses on the scientific analysis of audio recordings and video footage. It includes processes such as authentication, enhancement, noise reduction, transcription, speaker identification, and detection of tampering. The main purpose of forensic examination is to determine whether a recording they need to analyse is genuine, to identify the individuals that are involved in the recording to connect it with crime, and to extract useful information for investigation purposes.

Speaker identification is another important forensic technique used in criminal investigations. It involves comparing a questioned voice recording with a known voice sample to determine whether the voices in both recordings belong to the same person. Since every individual has unique vocal cords and different length of vocal tracts the voice characteristics differs from person to persom, speaker identification can help investigators to identify suspects in cases involving ransom calls, threat calls, terrorism, cybercrime, organised crime, and corruption.

In India, the legal recognition of electronic evidence has increased significantly in recent years especially after the enactment of Bharatiya Sakshya Adhiniyam, 2023 which contains legal provisions relating to the admissibility of electronic records. Courts have also delivered important judgments that clarify the requirements for accepting audio-video evidence and voice recordings during criminal proceedings. Despite these developments, challenges relating to lack of proper forensic infrastructure, shortage of trained experts, delay in forensic reports, and technological advancements affects the criminal justice system.

Therefore, forensic audio-video examination and speaker identification have become important tools in modern criminal investigations. They help investigating agencies collect evidence, identify suspects, and support criminal prosecutions. At the same time, proper scientific methods, legal safeguards, and technological advancements are necessary to ensure fairness, reliability, and accuracy in the administration of justice.

1.2 RESEARCH OBJECTIVES

1. To study the concept and importance of forensic audio-video examination in criminal investigations.
2. To examine the scientific methods and techniques used in forensic audio and video analysis.
3. To analyse the role of speaker identification in criminal investigations.
4. To study the evidentiary value and admissibility of audio-video evidence in India.

1.3 RESEARCH QUESTIONS

1. What is the role of forensic audio-video examination in criminal investigations?
2. How does speaker identification assist investigating agencies in identifying suspects?
3. What are the important tools and techniques used in forensic audio and video examination?
4. What are the legal requirements for the admissibility of audio-video evidence in India?

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

1.4 RESEARCH METHODOLOGY

The present study is doctrinal and analytical in nature. The research is based mainly on secondary sources such as books, journal articles, research papers, case laws, statutes, forensic reports, government publications, and online databases. The study analyses the role of forensic audio-video examination and speaker identification in criminal investigations and examines the legal framework governing electronic evidence in India.

1.5 SCOPE OF THE STUDY

This study examines forensic audio-video examination and speaker identification in criminal investigations with special reference to India. It covers the techniques, tools, evidentiary value, and admissibility of audio-video evidence under the Bharatiya Sakshya Adhiniyam, 2023. The study also analyses the challenges relating to authenticity, reliability, deepfakes, and digital manipulation, along with important judicial decisions governing electronic evidence in India.

1.6 LIMITATIONS OF THE STUDY

The study is limited to the analysis of forensic audio-video examination and speaker identification within the Indian criminal justice system. It relies primarily on secondary sources and does not include field research, interviews, or empirical data collection. The study focuses mainly on investigative and evidentiary aspects and does not provide a detailed technical analysis of forensic software and digital systems. Due to continuous developments in technology, some forensic methods and tools discussed in the study may evolve in the future.

CHAPTER II

FORENSIC AUDIO ANALYSIS

2.1 Meaning and Importance

Forensic audio analysis is the scientific examination of audio recordings by the forensic experts for investigative and legal purposes. It involves the analysis, enhancement, authentication, and interpretation of recorded sounds and speech. Audio recordings are often collected from devices like mobile phones, surveillance devices, CCTV systems, social media platforms, and online communication. These recordings help investigators to gather evidence, identify suspects, and understand criminal activities.[380]

The importance of forensic audio analysis has increased because most of the crimes that are happening requires electronic communication which leaves a digital trace. Criminals often use mobile phones, internet calls, voice messages, and digital platforms to communicate. As a result, audio recordings have become valuable sources of evidence in criminal investigations. Audio forensic analysis helps law enforcement agencies to determine the authenticity of recordings, identify speakers, and recover important information even if the recordings are not audible in some cases.[381]

Forensic audio analysis is widely used in cases involving kidnapping, ransom demands, terrorism, organised crime, cybercrime, corruption, extortion, and financial fraud, where the criminals use electronic medium to communicate in many cases. Audio recordings provide important evidence that supports investigations and assists courts in determining the truth.[382]

2.2 Process of Audio Forensic Analysis

The process of forensic audio analysis begins with the collection and preservation of audio evidence. Investigators must ensure that the original recording is protected from damage, alteration, or unauthorised access. Once the recording is secured, forensic experts create multiple working copies for examination while preserving the original file.[383]

[380] Harry hollien, *Forensic Voice Identification* 1–4 (2002).
[381] Robert C. Maher, Audio Forensic Examination, 1 IEEE Signal Processing Mag. 84, 85–87 (2009).
[382] N. Rudresh & V. M. Patel, Forensic Speaker Recognition: A Review, 10 Int'l J. Computer Applications 12, 13–15 (2011).
[383] Paul C. Giannelli & Edward J. Imwinkelried, *Scientific Evidence* 79–83 (6th ed. 2016).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

The recording is then subjected to different forensic processes such as authentication, enhancement, transcription, speaker identification, and comparison. Each step is carried out using specialised software and scientific methods.[384]

The final stage involves preparing a forensic report as a document which includes the methods used, findings obtained, and conclusions reached during the examination. This report may later presented before courts as expert evidence.[385]

2.3 Authentication

Authentication is one of the most important stages in forensic audio analysis. It is the first procedure before analysing the recording. It refers to the process of determining whether an audio recording is genuine and free from editing, tampering, or manipulation. Before a recording can be accepted as evidence, investigators and courts must be satisfied that the recording is original conversation or event.[386]

Forensic experts examine various aspects of the recording, including continuity of speech, background sounds, recording quality, metadata, and waveform patterns. They look for signs of splicing, deletion, insertion, or alteration that may indicate manipulation. Authentication helps establish the reliability and evidentiary value of audio recordings.[387]

The importance of authentication has increased with the development of advanced editing software and artificial intelligence technologies, which can create highly convincing fake recordings. Therefore, proper authentication is necessary to protect the integrity of criminal investigations and judicial proceedings.[388]

2.4 Audio Enhancement

Audio enhancement is to the process of improving quality and clarity of recordings. In many criminal investigations, audio evidence contain disturbances, low volume, or background noise that make conversations difficult to understand. Enhancement techniques help make important speech more audible without changing original content of the recording.[389]

Forensic experts use specialised software to increase voice clarity, adjust volume levels, filter unwanted sounds, and improve overall quality. Enhanced recordings often help investigators identify suspects, understand conversations, and recover important details that may otherwise remain unnoticed.[390]

2.5 Noise Reduction

Noise reduction is a specialised technique used to remove or reduce unwanted background sounds from audio recordings. Common sources of noise include traffic, machinery, wind, crowd conversations, and electronic interference. Such noises often interfere with speech and make forensic examination difficult.[391]

Although noise reduction can improve clarity, it can be done only to some extent. Recordings with high background noises and interferences cannot be filtered fully. Excessive filtering may affect the original characteristics of the recording.[392]

2.6 Voice Analysis

Voice analysis is the examination of vocal characteristics for the purpose of identifying or comparing speakers. Every individual has unique voice features influenced by physical, linguistic, and behavioural factors. Characteristics such as pitch, tone, frequency, pronunciation, accent, and speaking style can assist forensic experts in distinguishing one speaker from another.[393]

---

[384] Eoghan Casey, *Digital Evidence and Computer Crime* 52–58 (3d ed. 2011).
[385] Amit Dubey & G. S. Bajpai, Digital Evidence and Criminal Investigation in India, 58 J. Indian L. Inst. 450, 456–58 (2016).
[386] Christian A. Meuwly, Forensic Authentication of Audio Recordings, 46 J. Audio Eng'g Soc'y 885, 886–89 (1998).
[387] Maher, supra note 2, at 88–91.
[388] hew B. Hoy, Deepfake Videos: When Seeing Isn't Believing, 64 Med. Reference Servs. Q. 109, 110–13 (2020).
[389] Robert C. Maher, *Principles of Forensic Audio Analysis* 117–22 (2010).
[390] Lawrence Abu Hamdan, The Right to Hearing: Noise and the Law, 14 Sound Stud. 23, 25–29 (2018).
[391] Maher, supra note 10, at 88–91.
[392] Abu Hamdan, *supra* note 11, at 29–31.
[393] Hollien, *supra* note 1, at 23–29.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

In forensic investigations, voice analysis used to compare questioned recordings with known voice samples. Experts employ various scientific methods, including auditory analysis, spectrographic analysis, acoustic measurement, and linguistic examination. The objective is to determine whether the recordings are likely to have originated from the same speaker. However, factors such as illness, stress, emotional condition, age may affect the accuracy of voice comparisons. Therefore, conclusions are generally expressed in terms of probability rather than absolute certainty.[394]

CHAPTER III

FEATURES AND TECHNIQUES OF AUDIO FORENSIC ANALYSIS

3.1 Speaker Identification

Speaker identification is one of the most important techniques used in forensic audio analysis. It involves identifying a person by comparing a questioned voice recording with known voice samples. Every individual has unique speech characteristics such as pitch, tone, pronunciation, speaking style, and frequency patterns. These characteristics help forensic experts distinguish one speaker from another.[395]

In criminal investigations, speaker identification is commonly used when investigators have a recorded conversation but do not know who is the speaker in such recording. In such cases the questioned recording will be compared with the voice samples collected from suspects. Forensic experts can provide an opinion regarding the likely identity of the speaker. This technique is frequently used in cases involving kidnapping, ransom demands, extortion, terrorism, cybercrime, and organised crime.

Although speaker identification is a useful investigative tool, experts generally avoid claiming it as **"100% match**." Instead, conclusions are expressed in terms such as strong support, moderate support, limited support, or inconclusive findings.[396]

3.2 Voiceprint Analysis

Voiceprint analysis is a scientific method used to examine the unique acoustic characteristics of a person's voice. It is based on the idea that every individual produces speech differently because of differences in vocal organs, speech habits, and pronunciation patterns. These differences create unique patterns that can be visually examined and compared.[397]

In voiceprint analysis, forensic experts convert speech signals into visual representations called voiceprints. These voiceprints display frequency patterns, pitch variations, and speech characteristics. By comparing the voiceprints of a questioned recording with a known sample, experts can determine similarities and differences between speakers.[398]

Voiceprint analysis has been widely used in forensic investigations; however, experts generally consider it as one part of a broader examination process rather than a standalone method. Modern forensic practice often combines voiceprint analysis with acoustic, auditory, and linguistic analysis to improve reliability.[399]

3.3 Transcription

Transcription is the process of converting spoken words in an audio recording into written text. It is an important part of forensic audio analysis because it helps investigators, lawyers, judges, and other legal professionals understand recorded conversations clearly.[400]

In many criminal cases, audio recordings may contain lengthy conversations or unclear speech. A properly prepared transcript allows investigators to review the content of conversations more effectively. It also assists

[394] C. R. Rao & S. V. Rao, Speaker Identification and Its Forensic Applications, 42 Indian Police J. 35, 38–42 (1995).
[395] Hollien, *supra* note 1, at 23–29.
[396] International Association for Forensic Phonetics and Acoustics, Best Practice Guide for Forensic Speaker Comparison 5–8 (2015).
[397] Lawrence G. Kersta, Voiceprint Identification, 196 Nature 1253, 1253–57 (1962).
[398] Hollien, *supra* note 1, at 104-10.
[399] Rao & Rao, *supra* note 16, at 42-43.
[400] Roger W. Shuy, *Linguistics in the Courtroom* 45–48 (2006).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 9 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

during trial proceedings by providing a written version of the recorded communication.[401]

However, transcription must be carried out carefully because errors in interpretation may affect the meaning of conversations. Forensic experts often review recordings multiple times before preparing final transcripts to ensure accuracy and reliability.[402]

3.4 Linguistic Analysis

Linguistic analysis is the study of language, speech patterns, vocabulary, pronunciation, and communication style. In forensic audio analysis, linguistic examination helps experts understand how a person speaks and whether certain speech characteristics can be linked to a particular individual or group.[403]

Experts examine factors such as accent, dialect, grammar, vocabulary, pronunciation, and speaking habits. These characteristics may provide useful information about to which country speaker belongs to, his geographical background, education level, social environment, or language influences.[404]

Linguistic analysis is particularly useful when traditional acoustic methods alone cannot provide clear conclusions. In some investigations, the way a person speaks may provide valuable clues that support other forensic findings.[405]

3.5 Spectrogram Analysis

A spectrogram is a visual representation of sound that shows frequency, intensity, and time. Spectrogram analysis is one of the most commonly used techniques in forensic audio examination because it allows experts to study speech patterns visually.[406]

When a voice recording is converted into a spectrogram, different speech characteristics become visible. Experts can examine pitch patterns, pauses, sound frequencies, and pronunciation features. These observations help in speaker comparison and voice identification. Spectrogram analysis is particularly useful because it combines both visual and acoustic examination.[407]

3.6 Legal and Ethical Considerations

The use of audio recordings in criminal investigations raises several legal and ethical issues. One important concern is privacy. Individuals have a reasonable expectation that their private conversations will not be recorded or monitored without lawful authority. Therefore, investigating agencies must follow legal procedures while collecting audio evidence.[408]

Another important issue relates to authenticity and reliability is courts require assurance that audio recordings have not been edited, manipulated, or fabricated. Improper handling of evidence may affect its admissibility and reduce its evidentiary value.[409]

Investigators must balance the need for effective law enforcement with the protection of individual rights and freedoms. Therefore, legal safeguards and professional standards are necessary to ensure fairness in forensic investigations.[410]

CHAPTER IV

SPEAKER IDENTIFICATION IN CRIMINAL INVESTIGATION

4.1 Meaning of Speaker Recognition

Speaker recognition is the process of recognising or identifying a person through their voice. It is based on the principle that every individual has unique vocal characteristics that can be analysed and compared. These characteristics are influenced by physical features, speaking habits, pronunciation, accent,

[401] Casey, *supra* note 5, at 58-61.
[402] Roger W. Shuy, *Language Crimes* 77–82 (2005).
[403] Malcolm Coulthard & Alison Johnson, *An Introduction to Forensic Linguistics* 73–79 (2007).
[404] Shuy, *supra* note 24, at 93–101.
[405] Malcolm Coulthard, Author Identification, Idiolect, and Linguistic Uniqueness, 4 Applied Linguistics 45, 49–53 (2004).
[406] Kersta, *supra* note 19, at 1254-56.
[407] Hollien, *supra* note 1, at 111–17.
[408] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[409] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[410] G. S. Bajpai & Amit Dubey, Electronic Evidence and Criminal Justice Administration in India, 58 J. Indian L. Inst. 450, 460–63 (2016).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

and behavioural patterns. As a result, a person's voice can be used as a means of identification in criminal investigations.[411]

With the increasing use of digital communication, speaker recognition has become an important forensic tool. Voice recordings collected from mobile phones, surveillance systems, social media platforms, internet calls, and other electronic sources often provide valuable evidence. Speaker recognition helps investigators determine the identity of individuals involved in criminal activities and establish links between suspects and recorded conversations.[412]

4.2 Speaker Identification and Speaker Verification

Speaker recognition is generally divided into two categories:

- Speaker identification
- Speaker verification.

Although both methods involve voice comparison, their objectives are different.

Speaker identification answers the question, **"Who is speaking?"** In this method, an unknown voice recording is compared with several known voice samples stored in a database. The purpose is to determine the identity of the speaker from among multiple possible individuals.[413]

Speaker verification, on the other hand, answers the question, **"Is this person really who they claim to be?"** In this method, a questioned voice sample is compared with the other known voice sample of a particular individual. The aim is to verify whether both recordings belong to the same person. This method is commonly used in security systems, banking services, and criminal investigations involving known suspects.[414]

4.3 Closed-Set and Open-Set Identification

Speaker identification can further be classified into **closed-set identification** and **open-set identification.** These methods are used depending on the nature of the investigation and the availability of voice samples.[415]

In closed-set identification, the unknown speaker is assumed to be present within a known group of speakers. The forensic expert compares the questioned recording with voice samples available in the database and identifies the most likely speaker. This method is commonly used in forensic investigations because investigators usually have a limited number of suspects.[416]

In open-set identification, the system must first determine whether a matching speaker exists and then identify the person if a match is found. The unknown speaker may or may not be match with the available database. This method is more complex and generally produces less certain results than closed-set identification. [417]

4.4 Process of Speaker Identification

The process of speaker identification begins with the collection of a questioned voice recording and one or more known voice samples. Investigators must ensure that the recordings are collected legally and preserved properly to maintain their evidentiary value.[418]

The next step involves authentication and quality assessment of the recordings. Forensic experts examine whether the recordings are genuine and suitable for comparison. Poor-quality recordings may require enhancement and noise reduction before detailed analysis can be carried out.[419]

After this, experts analyse various voice characteristics such as pitch, tone, frequency, pronunciation, speaking rate, accent, and speech patterns. Scientific methods such as auditory analysis, spectrographic analysis, acoustic measurements, and linguistic

[411] Hollien, *supra* note 1, at 15–18.
[412] Geoffrey Stewart Morrison, Forensic Voice Comparison and the Paradigm Shift in Forensic Science, 51 Sci. & Just. 298, 299–302 (2011).
[413] Hollien, *supra* note 1, at 28–32.
[414] Joseph P. Campbell, Speaker Recognition: A Tutorial, 85 Proc. IEEE 1437, 1441–44 (1997).
[415] Xiaoyi Lu & Jianhua Tao, Speaker Recognition in Challenging Conditions, 7 IEEE Trans. Audio, Speech & Language Processing 221, 223–25 (2015).
[416] Hollien, *supra* note 1, at 35–37.
[417] Morrison, *supra* note 34, at 304-06.
[418] Giannelli & Imwinkelried, supra note 4, at 83-89.
[419] Maher, supra note 10, at 88–91

examination are used to compare the recordings.

Finally, the expert evaluates the similarities and differences between the samples and prepares a forensic report. The findings are expressed in terms of probability rather than certainty because voice comparison cannot provide absolute identification in every case.

4.5 Standard of Proof

Unlike fingerprints or DNA evidence, speaker identification generally cannot provide absolute certainty. Human voice may change because of age, illness, emotional condition, stress, intoxication, or intentional disguise. Therefore, forensic experts usually avoid stating that two recordings are a "100% match."

Instead, experts express their conclusions using terms such as "strong support," "moderate support," "limited support," or "inconclusive." These terms indicate the degree of confidence in the comparison results. Courts consider such opinions along with other evidence available in the case.[420]

The purpose of forensic speaker identification is not to replace other forms of evidence but to provide scientific assistance during investigations and judicial proceedings. Therefore, speaker identification is generally treated as corroborative evidence rather than conclusive proof of guilt.[421]

CHAPTER V

TYPES, TOOLS, AND EVIDENCE HANDLING IN AUDIO FORENSICS

5.1 Types of Audio Analysed

Forensic audio experts examine different types of audio recordings depending on the nature of the investigation. One of the most common sources is mobile phone recordings, including call recordings, voice messages, and intercepted communications. These recordings often provide important evidence in criminal cases involving threats, extortion, kidnapping, and organised crime.

Audio files stored in digital formats such as MP3, WAV, AAC, and other media formats are also frequently examined. These files may be recovered from computers, mobile devices, storage media, or online platforms during investigations.[422]

Surveillance recordings collected through hidden microphones, body wires, and monitoring systems are another important source of forensic evidence. Such recordings are commonly used in corruption, bribery, and undercover operations.

With the growth of internet-based communication, forensic experts increasingly analyse Voice over Internet Protocol (VoIP) calls, online meeting recordings, and social media audio clips. These recordings often play an important role in cybercrime, terrorism, and transnational criminal investigations.[423]

5.2 Specialized Forensic Audio Tools

Modern forensic investigations depend heavily on specialised software tools that help experts analyse, enhance, authenticate, and compare audio recordings. These tools assist investigators in extracting important information from recordings and improving the accuracy of forensic examinations.

Advanced software applications can identify tampering, remove unwanted noise, enhance speech quality, and perform speaker comparison. They have become essential because modern digital recordings are often affected by poor quality, environmental noise, and manipulation.

Some of the most commonly used forensic audio tools include **Amped Authenticate, Amped FIVE, iZotope RX, and Praat.** Each tool serves a

[420] Geoffrey Stewart Morrison, The Likelihood-Ratio Framework and Forensic Voice Comparison, 58 Austl. J. Forensic Sci. 1, 3–7 (2014).
[421] Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
[422] Casey, *supra* note 5, at 71-75.
[423] Rudresh & Patel, supra note 3, at 16–18.

specific purpose in forensic investigations and contributes to the reliability of audio evidence.[424]

5.2.1 Amped Authenticate

Amped Authenticate is a forensic software tool used to verify the authenticity of digital recordings. It helps experts determine whether an audio file has been edited, manipulated, or tampered with. The software examines metadata, file structure, compression patterns, and other technical characteristics of recordings.[425]

This tool is particularly useful in criminal cases where the authenticity of an audio recording is questioned. By identifying possible signs of editing or alteration, Amped Authenticate helps investigators and courts assess the reliability of electronic evidence.[426]

5.2.2 Amped FIVE

Amped FIVE is primarily known as a forensic video analysis tool, but it also supports certain audio examination functions. The software assists forensic experts in enhancing recordings, examining evidence, and presenting findings in a clear and understandable manner.[427]

Investigators often use Amped FIVE in cases involving both audio and video evidence because it allows simultaneous examination of multimedia files. Its ability to document forensic procedures also improves transparency and reliability during investigations and court proceedings.

5.2.3 iZotope RX

iZotope RX is one of the most widely used audio enhancement tools in forensic audio examination. The software is designed to improve audio quality by reducing background noise, removing unwanted sounds, isolating speech, and repairing damaged recordings.

Forensic experts frequently use iZotope RX when dealing with recordings that contain environmental noise, overlapping voices, or poor sound quality. The software enables investigators to recover information that may not be clearly audible in the original recording.[428]

5.2.4 Praat

Praat is a specialised software application widely used for speech and voice analysis. It is commonly employed in forensic speaker identification because it allows experts to analyse pitch, frequency, formants, intensity, and other speech characteristics.[429]

Praat helps forensic experts compare voice samples scientifically and identify similarities or differences between speakers. The software is frequently used in academic research, forensic laboratories, and speaker comparison investigations.[430]

5.3 Chain of Custody and Evidence Handling

The chain of custody refers to the documented process of collecting, preserving, transferring, examining, and storing evidence. It is one of the most important requirements in forensic investigations because it ensures that evidence remains authentic and reliable throughout the investigation process.[431]

The chain of custody usually begins when investigators collect an audio recording or electronic device. Every transfer of evidence from one person to another must be recorded to maintain transparency and accountability.

Forensic experts generally conduct examinations on duplicate copies while preserving the original recording. This reduces the risk of accidental modification or damage to the original evidence. Proper storage and security measures are also necessary to prevent unauthorised access or tampering.[432]

[424] Amit Dubey, Digital Forensics and Electronic Evidence in Criminal Investigations, 3 Indian J. Forensic Res. 45, 49–52 (2021).
[425] Amped Software, *Amped Authenticate User Guide* 10–18 (2024).
[426] Amit Dubey, Digital Evidence and Forensic Authentication in India, 14 Indian Police J. 72, 75–78 (2022).
[427] Amped Software, *Amped FIVE Technical Documentation* 15–22 (2024).
[428] Hollien, *supra* note 1, at 92–95.
[429] Paul Boersma & David Weenink, *Praat: Doing Phonetics by Computer* (2024).
[430] Morrison, *supra* note 34, at 304-06
[431] Giannelli & Imwinkelried, supra note 4, at 79-83.
[432] Dubey & Bajpai, *supra* note 6, at 454–57.

Failure to maintain a proper chain of custody create doubts regarding authenticity of evidence and may affect its admissibility before courts. Therefore, strict compliance with evidence-handling procedures is essential for ensuring the integrity of forensic audio examinations.[433]

CHAPTER VI

CHALLENGES AND LIMITATIONS IN AUDIO FORENSIC EXAMINATION

Forensic audio examination has become an important tool in modern criminal investigations. It helps investigators analyse recorded conversations, identify speakers, and collect evidence for criminal cases. However, despite its usefulness, forensic audio analysis faces several practical and technical challenges. These challenges may affect the accuracy, reliability, and admissibility of audio evidence before courts.

I) Poor Recording Quality

One of the most common problems in forensic audio examination is poor recording quality. Audio recordings collected during investigations are often recorded in uncontrolled environments. As a result, they may contain low volume, distortion, interruptions, or unclear speech. Poor-quality recordings make it difficult for forensic experts to identify speakers and understand conversations accurately. In some cases, important words or phrases may become impossible to recover. Although audio enhancement software can improve recording quality, it cannot completely restore severely damaged recordings.[434]

ii) Background Noise

Background noise is another major challenge in forensic audio analysis. Many recordings contain unwanted sounds such as traffic noise, crowd conversations, machinery, wind, television sounds, or electronic interference. These noises often overlap with speech and reduce the clarity of recordings.[435]

Forensic experts use noise reduction techniques to minimise unwanted sounds and improve speech intelligibility. However, excessive filtering may affect the original recording and create the risk of losing important information. Therefore, experts must carefully balance enhancement and preservation of evidence.

iii) Voice Disguise

In some criminal cases, suspects intentionally change their voices to avoid identification. This practice is known as voice disguise. A person may alter their pitch, accent, pronunciation, speaking speed, or tone to make recognition difficult.

Voice disguise creates significant challenges for forensic experts because the altered voice may differ substantially from the speaker's natural voice. Although forensic techniques can detect certain signs of disguise, accurate identification becomes more difficult when the speaker deliberately modifies speech characteristics.[436]

iv) Deepfakes

Criminals may use deepfake technology to create false evidence, spread misinformation, commit fraud, or impersonate individuals. As deepfake technology becomes more advanced, it becomes increasingly difficult to distinguish between genuine and fabricated recordings. This creates serious concerns regarding the reliability of digital evidence.[437]

To address this challenge, forensic experts are developing advanced techniques for detecting artificial manipulation and verifying the authenticity of recordings. However, the rapid development of artificial intelligence continues to create new difficulties for investigators and courts.[438]

v) Metadata Alteration

Metadata refers to information stored within a digital file, such as the date, time, device details,

[433] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[434] Meuwly, *supra* note 27, at 889-91.
[435] Abu Hamdan, *supra* note 11, at 25-30.
[436] Morrison, *supra* note 34, at 304-06.
[437] R. K. Sharma, Artificial Intelligence and Challenges to Digital Evidence, 12 Indian J. Criminology 41, 45–48 (2022).
[438] Hany Farid, Fake Images and Deepfakes: Challenges for Digital Forensics, 36 J. Digital Investigation 1, 3–7 (2021).

file format, and recording history. Metadata often provides important information regarding the origin and authenticity of audio recordings.[439]

However, metadata can be altered using specialised software. A person may modify timestamps, file information, or device details to conceal the true origin of a recording. Such alterations can mislead investigators and affect the reliability of evidence.[440]

vi) Health and Emotional Conditions Affecting Voice

A person's voice is not always constant. Various health conditions such as fever, cold, throat infections, respiratory problems, and ageing can affect speech characteristics. Similarly, emotional conditions such as fear, anger, stress, anxiety, and excitement may influence the way a person speaks.[441]

These factors may cause temporary or permanent changes in pitch, tone, pronunciation, and speaking patterns. As a result, voice recordings collected at different times may show noticeable differences even when they belong to the same person.[442]

CHAPTER VII

VIDEO FORENSIC ANALYSIS

7.1 Meaning and Importance

Video forensic analysis is the scientific examination of video recordings for investigation and legal purposes. It involves analysing, enhancing, authenticating, and interpreting video evidence collected from different sources. The main objective of video forensic analysis is to obtain useful information from recordings and assist investigators in understanding events related to a crime.[443]

In modern criminal investigations, video evidence plays a very important role. CCTV cameras, mobile phones, body cameras, dashboard cameras, drones, and surveillance systems continuously record activities in public and private spaces. These recordings often provide crucial evidence that helps investigators identify suspects, establish timelines, reconstruct crime scenes, and verify witness statements.

The importance of video forensic analysis has increased significantly because many crimes are now captured on camera. Video recordings often provide objective evidence that supports criminal investigations and judicial proceedings. As a result, video forensic examination has become an essential part of modern forensic science.

7.2 Features of Video Forensic Analysis

Video forensic analysis includes several techniques that help investigators examine recordings scientifically. These techniques allow experts to improve video quality, verify authenticity, identify objects, analyse movements, and establish the sequence of events shown in a recording. [444]

The major features of video forensic analysis include video enhancement, authentication, object tracking, time and motion analysis, video stabilization, and metadata examination. Each of these techniques contributes to the reliability and usefulness of video evidence in criminal investigations.[445]

7.3 Video Enhancement

Video enhancement is the process of improving the visual quality of a recording. In many investigations, video footage may be blurry, dark, distorted, or affected by poor camera quality. Video enhancement techniques help improve visibility and make important details easier to examine. Forensic experts use specialised software to adjust brightness, contrast, colour balance, sharpness, and resolution. Enhancement may help investigators identify faces, vehicles, objects, or activities that are difficult to observe in the original recording.[446]

[439] Casey, *supra* note 5, at 102-08.
[440] Dubey & Bajpai, *supra* note 6, at 458–61.
[441] Hollien, *supra* note 1, at 54–61.
[442] Morrison, *supra* note 34, at 301-04.
[443] Keith J. Cooper, Video Forensics: Enhancing and Authenticating Digital Video Evidence, 45 J. Forensic Identification 312, 315–18 (1995).
[444] *Id.* at 318–21.
[445] Amped Software, *Fundamentals of Video Forensics* 12–18 (2023).
[446] Cooper, *supra* note 65, at 320-24.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

7.4 Authentication

Authentication is the process of verifying whether a video recording is genuine and has not been edited, manipulated, or fabricated. It is one of the most important stages of forensic examination because courts require assurance that video evidence accurately represents the events shown in the recording.

Forensic experts examine metadata, file structure, compression patterns, frame continuity, and technical characteristics of the video. These examinations help identify signs of editing, splicing, deletion, insertion, or manipulation.

Authentication has become increasingly important because modern editing software and artificial intelligence technologies can create highly realistic fake videos. Therefore, proper authentication is necessary to maintain the reliability of digital evidence.[447]

7.5 Object Tracking

Object tracking refers to the process of monitoring the movement of a person, vehicle, or object throughout a video recording. This technique helps investigators understand the actions and movements of individuals involved in criminal activities.[448]

For example, in theft, murder, or kidnapping cases, object tracking may help investigators determine the route taken by a suspect or identify interactions between different individuals. Advanced forensic software can automatically track movements across multiple frames of a recording. Object tracking is particularly useful when large amounts of CCTV footage need to be analysed. It saves time and improves the efficiency of investigations.

7.6 Time and Motion Analysis

Time and motion analysis involves examining the timing, speed, and sequence of events shown in a video recording. This technique helps investigators establish a chronological order of events and reconstruct incidents accurately.[449]

7.7 Video Stabilization

Video stabilization is a technique used to reduce unwanted camera movements and shaking in video recordings. Many recordings collected during investigations may be unstable because they were captured using handheld devices or moving cameras.

By stabilizing a video, forensic experts can improve viewing quality and make important details easier to examine. Stabilization helps investigators observe facial features, vehicle registration numbers, and other visual details more accurately.

7.8 Metadata Analysis

Metadata analysis involves examining information stored within a video file. Metadata may include details such as the date and time of recording, device information, file format, location data, and editing history. Metadata often provides valuable information about the origin and authenticity of a video recording. Investigators use metadata to verify timelines, identify recording devices, and detect possible manipulation.[450]

However, metadata can also be altered or deleted using specialised software. Therefore, forensic experts must compare metadata with other technical characteristics of the recording to determine its reliability. Metadata analysis has become increasingly important in modern digital investigations because it often reveals information that is not visible in the video itself.[451]

[447] Hoy, *supra* note 9, at 112-15.
[448] Richard Szeliski, *Computer Vision: Algorithms and Applications* 323–28 (2011).
[449] Hany Farid, Digital Image and Video Forensics, 5 IEEE Signal Processing Mag. 16, 20–23 (2009).
[450] Dubey & Bajpai, *supra* note 6, at 458–62.
[451] Farid, *supra* note 71, at 21-24.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CHAPTER VIII

TYPES, TOOLS, AND CHALLENGES IN VIDEO FORENSICS

8.1 TYPES

8.1.1 CCTV Footage

Closed-Circuit Television (CCTV) footage is one of the most commonly used forms of video evidence in criminal investigations. CCTV cameras are installed in public places, commercial establishments, offices, banks, railway stations, airports, and residential areas. These cameras continuously record activities and often provide important evidence relating to criminal incidents.

However, CCTV footage is not always perfect. Poor lighting conditions, low camera resolution, improper camera angles, and storage limitations may affect the quality of recordings. These factors sometimes make identification difficult and require forensic enhancement techniques.

8.1.2 Mobile Phone Videos

Mobile phones have become one of the most important sources of video evidence in modern criminal investigations. Almost every individual carries a smartphone capable of recording high-quality videos. As a result, many criminal incidents are captured by victims, witnesses, or bystanders using mobile phones.

Despite their usefulness, mobile phone videos may be edited, compressed, or altered before being shared. Therefore, forensic experts must carefully examine these recordings to verify their authenticity and reliability.[452]

8.1.3 Drone Footage

Drones are now used by law enforcement agencies, government authorities, journalists, and private individuals for surveillance and monitoring purposes. Drone footage often provides a wider view of locations and events that may not be captured by traditional cameras.[453]

In criminal investigations, drone recordings can help examine crime scenes, monitor large public gatherings, track suspects, and document evidence from difficult-to-access locations. They are particularly useful in disaster management, border security, and environmental crime investigations. However, drone footage also raises concerns regarding privacy, surveillance, and data protection. Improper use of drone technology may result in violations of individual rights and legal safeguards.[454]

8.2. Specialized Video Forensic Tools

Modern forensic investigations depend on specialised software applications to analyse and enhance video evidence. These tools help experts improve video quality, detect manipulation, authenticate recordings, and present findings in a scientifically reliable manner.

8.2.1 Amped FIVE

It is one of the most widely used forensic video analysis software applications in the world. It is specifically designed for law enforcement agencies and forensic laboratories. The software assists experts in video enhancement, image clarification, authentication, object tracking, and evidence presentation.[455]

Amped FIVE provides various tools for adjusting brightness, contrast, colour balance, and sharpness. It also allows forensic experts to document every step of the examination process, which improves transparency and reliability.[456]

Because of its advanced features and forensic reporting capabilities, Amped FIVE is commonly used in criminal investigations involving CCTV footage, surveillance recordings, and mobile phone videos.

[452] Farid, *supra* note 71, at 20-22.
[453] K. V. Prasad, Emerging Role of Drones in Criminal Investigation, 11 Indian Police J. 51, 54–57 (2021).
[454] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[455] Amped Software, *Amped FIVE Technical Documentation* 20–28 (2024).
[456] Amped Software, *Video Enhancement Principles and Practice* 30–38 (2023).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

8..2.2 Input ACE

Input ACE is another forensic video analysis software used for examining and enhancing digital video evidence. The software allows investigators to process recordings from different devices and formats while preserving evidentiary integrity.[457]

It is commonly used to improve image clarity, analyse video content, and recover details that may not be visible in the original recording. The software is also useful in examining surveillance footage collected from security systems and CCTV cameras.

8.2.3 Pestell FVA

Pestell FVA is a forensic video analysis software developed specifically for law enforcement and forensic professionals. It provides tools for video enhancement, image clarification, measurement, and evidence comparison.[458]

The software assists investigators in examining digital recordings and identifying important visual details that may be relevant to criminal investigations. Its features help experts produce clearer and more reliable forensic findings.

8.3 Challenges and Limitations

Despite significant technological advancements, video forensic analysis faces several challenges. One major challenge is poor video quality caused by low-resolution cameras, poor lighting, weather conditions, and improper camera positioning. Such factors may affect the ability to identify individuals and objects accurately.

Another challenge is the increasing use of artificial intelligence and deepfake technology. Deepfake videos can create realistic but false visual content, making it difficult for investigators to distinguish genuine recordings from fabricated ones.

Metadata manipulation, video compression, frame loss, and editing also create difficulties in forensic examination. Additionally, privacy concerns and legal restrictions may affect the collection and use of video evidence.

CHAPTER IX

ADMISSIBILITY OF AUDIO-VIDEO EVIDENCE IN INDIA

9.1 Bharatiya Sakshya Adhiniyam, 2023

The admissibility of electronic evidence is important because digital records can be easily copied, altered, manipulated, or fabricated. Therefore, courts require safeguards to ensure the authenticity and reliability of electronic evidence.

In India, the admissibility of electronic evidence is governed by the Bharatiya Sakshya Adhiniyam, 2023, which replaced the Indian Evidence Act, 1872. The Act recognises electronic records as valid evidence and provides conditions for their admissibility before courts.

The Bharatiya Sakshya Adhiniyam, 2023 modernises the law relating to evidence and gives specific recognition to electronic records. The Act acknowledges that digital evidence has become an essential part of modern investigations and judicial proceedings. As a result, electronic records are treated at par with traditional documentary evidence, subject to certain conditions and procedural safeguards.[459]

9.2 Section 61: Admissibility of Electronic Records

Section 61 of the Bharatiya Sakshya Adhiniyam, 2023 recognises electronic records as documents and provides that the contents of electronic records may be proved in accordance with the provisions of the Act. This section is important because it gives legal recognition to electronic evidence and places it within the framework of documentary evidence.[460]

Section 61 therefore serves as the foundation for the admissibility of electronic records in India.

[457] Input-Ace Documentation, Forensic Video Analysis Manual 15–19 (2023).
[458] Pestell FVA User Guide 8–12 (2023).
[459] Bharatiya Sakshya Adhiniyam, No. 47 of 2023
[460] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 61.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 9 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

9.3 Section 63: Special Provisions Relating to Electronic Records

Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 contains special provisions relating to the admissibility of electronic records. This section corresponds to the earlier Section 65B of the Indian Evidence Act, 1872. It provides the conditions that must be satisfied before electronic records can be admitted as evidence before courts.[461]

The purpose of Section 63 is to ensure that electronic records presented before courts are reliable and have not been manipulated. Since digital evidence can be altered more easily than traditional documents, the law requires additional safeguards before admitting such evidence.[462]

9.4 Electronic Evidence Certification

Certification of electronic evidence is one of the most important requirements under Indian law. The certificate serves as proof that the electronic record was produced from a computer or electronic device in the ordinary course of its operation and that the information contained in the record is accurate.[463]

The requirement of certification helps courts ensure that electronic evidence has not been altered or manipulated. It also establishes the source and authenticity of the electronic record. In cases involving audio and video evidence, certification becomes particularly important because recordings can be edited using modern technology.[464]

9.5 Judicial Approach

Indian courts have played an important role in shaping the law relating to electronic evidence. Through various judicial decisions, courts have clarified the requirements for admissibility and the importance of maintaining authenticity and reliability.

Judicial decisions such as ***Anvar P.V. v. P.K. Basheer, (2014)***[465] and ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020)*** [466]have significantly influenced the law relating to electronic evidence. These decisions clarified the importance of statutory compliance and the evidentiary value of electronic records.

As technology continues to evolve, courts are likely to face new challenges relating to artificial intelligence, deepfakes, and digital manipulation. Therefore, judicial interpretation will continue to play an important role in ensuring the fair use of electronic evidence in the criminal justice system.

CHAPTER X

IMPORTANT CASE LAWS

I) R.M. Malkani v. State of Maharashtra

The issue before the Supreme Court was whether a secretly recorded telephone conversation could be admitted as evidence in a criminal trial. The Court held that tape-recorded conversations are admissible if they are relevant, authentic, and properly proved. The Court further observed that the recording was not obtained through coercion and could therefore be relied upon as evidence.[467]

ii) Sachin Jagdish Joshi v. State of Maharashtra, 2018

The issue in this case was the admissibility and reliability of electronic audio and video recordings. The Court held that electronic recordings can be relied upon as evidence if their authenticity and integrity are properly established through legal procedures.[468]

iii) Rajiv Gandhi Assassination Case

The case involved the assassination of former Prime Minister Rajiv Gandhi. The issue was whether photographic and video evidence collected during the investigation could be used to identify the accused and establish the conspiracy. The Court accepted the visual

[461] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63.
[462] Bajpai & Dubey, *supra* note 32, at 459–61.
[463] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63.
[464] Aparna Chandra, Understanding the Bharatiya Sakshya Adhiniyam, 2023, 65 J. Indian L. Inst. 214, 223–25 (2024).
[465] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
[466] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[467] R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.
[468] Sachin Jagdish Joshi v. State of Maharashtra, 2018 SCC OnLine Bom 2070.

evidence and relied upon it to reconstruct the sequence of events and identify the persons involved.[469]

iv) Mumbai Attacks Case

The issue before the Court was whether CCTV footage, intercepted communications, and other electronic records could be used to prove the involvement of the accused in the 2008 Mumbai terrorist attacks. The Court accepted the electronic evidence and held that it strongly supported the prosecution's case.[470]

v) Nirbhaya Case

The issue in this case was whether electronic evidence such as CCTV footage and digital records could be relied upon in establishing the guilt of the accused. The Court accepted the electronic evidence and used it along with other evidence to confirm the conviction of the accused persons.[471]

vi) Anvar P.V. v. P.K. Basheer, (2014)

The issue was whether electronic records could be admitted as evidence without complying with the statutory requirements relating to certification. The Supreme Court held that electronic evidence must satisfy the prescribed legal requirements and be accompanied by the necessary certificate to be admissible.[472]

CHAPTER XI

SUGGESTIONS AND REFORMS

1. Forensic audio-video examination and speaker identification have become important tools in modern criminal investigations. However, there are still many practical and legal challenges that affect their effectiveness. Therefore, certain reforms are necessary to improve the reliability and use of digital evidence in India.
2. One of the most important requirements is the strengthening of forensic infrastructure. Many forensic laboratories in India face shortages of equipment, technology, and trained personnel. The government should establish more modern forensic laboratories and provide advanced software and technical resources for audio and video examination.
3. Training of police officers and investigating agencies is also necessary. In many cases, electronic evidence is not collected or preserved properly, which affects its evidentiary value. Regular training programmes should be conducted to educate investigators about digital evidence collection, preservation, chain of custody, and forensic procedures.
4. The growing use of artificial intelligence and deepfake technology creates new challenges for criminal investigations. Therefore, specialised techniques and software should be developed to detect manipulated audio and video recordings. Research in forensic technology should be encouraged so that investigators can effectively identify fake digital evidence.
5. Another important reform is reducing delays in forensic examinations. In many criminal cases, forensic reports take several months to be completed. Such delays affect investigations and judicial proceedings. Increasing the number of forensic experts and improving laboratory facilities can help address this problem.
6. Legal awareness regarding electronic evidence should also be improved. Investigators, lawyers, judges, and prosecutors should receive regular training on developments in digital evidence and forensic science. This will help ensure the proper use and evaluation of electronic evidence during criminal proceedings.
7. Privacy and data protection must also be given importance. While surveillance technologies and digital investigations

[469] State v. Nalini, (1999) 5 SCC 253.
[470] Mohammed Ajmal Amir Kasab v. State of Maharashtra, (2012) 9 SCC 1.
[471] Mukesh v. State (NCT of Delhi), (2017) 6 SCC 1.
[472] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

are useful for law enforcement, they should not result in unnecessary violations of individual rights. Proper safeguards should be maintained to balance public safety and personal privacy.

8. Finally, cooperation between forensic scientists, investigating agencies, prosecutors, and judicial officers should be strengthened. A coordinated approach can improve the quality of investigations and increase public confidence in the criminal justice system.

CONCLUSION

Technology has significantly changed the nature of criminal investigations. Audio recordings, video footage, CCTV recordings, mobile phone data, and other forms of electronic evidence now play an important role in solving crimes and assisting courts in the administration of justice. As a result, forensic audio-video examination and speaker identification have become valuable tools in modern criminal investigations This study examined the concept, methods, and importance of forensic audio and video examination. It discussed various techniques used in audio analysis, speaker identification, voice comparison, video enhancement, authentication, and forensic examination of digital evidence. The study also analysed the different tools and technologies used by forensic experts for examining electronic records. The research found that forensic audio-video examination provides significant assistance in identifying suspects, reconstructing crime scenes, verifying evidence, and supporting criminal prosecutions. Speaker identification has become particularly useful in cases involving terrorism, kidnapping, extortion, cybercrime, organised crime, and corruption. Similarly, video evidence has become an important source of information in criminal investigations. At the same time, the study identified several challenges that affect the reliability of forensic evidence. Poor recording quality, background noise, voice disguise, metadata manipulation, deepfake technology, and limitations of forensic tools create difficulties for investigators and courts. These challenges demonstrate that digital evidence cannot always be accepted without careful examination and verification. The study also examined the legal framework governing electronic evidence in India. The Bharatiya Sakshya Adhiniyam, 2023 provides legal recognition to electronic records and establishes conditions for their admissibility. Judicial decisions have further clarified the requirements relating to authenticity, certification, and reliability of electronic evidence. Overall, forensic audio-video examination and speaker identification have become essential components of the modern criminal justice system. As technology continues to develop, their importance will continue to increase. However, effective use of these techniques requires proper forensic infrastructure, trained experts, technological advancements, legal safeguards, and adherence to scientific standards. With these improvements, forensic audio-video evidence can contribute significantly to fair investigations and the effective administration of justice in India.

REFERENCES

BIBLIOGRAPHY

Books

1. EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (3d ed. 2011).
2. HARRY HOLLIEN, FORENSIC VOICE IDENTIFICATION (2002).
3. MALCOLM COULTHARD & ALISON JOHNSON, AN INTRODUCTION TO FORENSIC LINGUISTICS (2007).
4. PAUL C. GIANNELLI & EDWARD J. IMWINKELRIED, SCIENTIFIC EVIDENCE (6th ed. 2016).
5. RICHARD SZELISKI, COMPUTER VISION: ALGORITHMS AND APPLICATIONS (2011).
6. ROBERT C. MAHER, PRINCIPLES OF FORENSIC AUDIO ANALYSIS (2010).

7. ROGER W. SHUY, LANGUAGE CRIMES (2005).
8. ROGER W. SHUY, LINGUISTICS IN THE COURTROOM (2006).

Journal Articles

1. Amit Dubey & G. S. Bajpai, Digital Evidence and Criminal Investigation in India, 58 J. INDIAN L. INST. 450 (2016).
2. Aparna Chandra, Understanding the Bharatiya Sakshya Adhiniyam, 2023, 65 J. INDIAN L. INST. 214 (2024).
3. C. R. Rao & S. V. Rao, Speaker Identification and Its Forensic Applications, 42 INDIAN POLICE J. 35 (1995).
4. Christian A. Meuwly, Forensic Authentication of Audio Recordings, 46 J. AUDIO ENG'G SOC'Y 885 (1998).
5. Christian A. Meuwly, The Use of Noise Reduction in Forensic Audio Analysis, 12 FORENSIC SCI. INT'L 51 (2001).
6. Geoffrey Stewart Morrison, Forensic Voice Comparison and the Paradigm Shift in Forensic Science, 51 SCI. & JUST. 298 (2011).
7. Geoffrey Stewart Morrison, The Likelihood-Ratio Framework and Forensic Voice Comparison, 58 AUSTL. J. FORENSIC SCI. 1 (2014).
8. Hany Farid, Digital Image and Video Forensics, 5 IEEE SIGNAL PROCESSING MAG. 16 (2009).
9. Hany Farid, Fake Images and Deepfakes: Challenges for Digital Forensics, 36 J. DIGITAL INVESTIGATION 1 (2021).
10. Joseph P. Campbell, Speaker Recognition: A Tutorial, 85 PROC. IEEE 1437 (1997).
11. Keith J. Cooper, Video Forensics: Enhancing and Authenticating Digital Video Evidence, 45 J. FORENSIC IDENTIFICATION 312 (1995).
12. K. V. Prasad, Emerging Role of Drones in Criminal Investigation, 11 INDIAN POLICE J. 51 (2021).
13. Lawrence Abu Hamdan, The Right to Hearing: Noise and the Law, 14 SOUND STUD. 23 (2018).
14. Lawrence G. Kersta, Voiceprint Identification, 196 NATURE 1253 (1962).
15. Malcolm Coulthard, Author Identification, Idiolect, and Linguistic Uniqueness, 4 APPLIED LINGUISTICS 45 (2004).
16. Matthew B. Hoy, Deepfake Videos: When Seeing Isn't Believing, 64 MED. REFERENCE SERVS. Q. 109 (2020).
17. N. Rudresh & V. M. Patel, Forensic Speaker Recognition: A Review, 10 INT'L J. COMPUTER APPLICATIONS 12 (2011).
18. R. K. Sharma, Artificial Intelligence and Challenges to Digital Evidence, 12 INDIAN J. CRIMINOLOGY 41 (2022).
19. Robert C. Maher, Audio Forensic Examination, 1 IEEE SIGNAL PROCESSING MAG. 84 (2009).

Case Laws:

1. Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
2. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
3. Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
4. Mohammed Ajmal Amir Kasab v. State of Maharashtra, (2012) 9 SCC 1.
5. Mukesh v. State (NCT of Delhi), (2017) 6 SCC 1.
6. R.M. Malkani v. State of Maharashtra, (1973) 1 SCC 471.
7. Ritesh Sinha v. State of Uttar Pradesh, (2019) 8 SCC 1.
8. Sachin Jagdish Joshi v. State of Maharashtra, 2018 SCC OnLine Bom 2070.
9. State v. Nalini, (1999) 5 SCC 253.

Webliography

1. Amped Software, Amped Authenticate User Guide, https://ampedsoftware.com.
2. Amped Software, Amped FIVE Technical Documentation, https://ampedsoftware.com.
3. Input-Ace Documentation, Forensic Video Analysis Manual, https://input-ace.com.
4. Paul Boersma & David Weenink, Praat: Doing Phonetics by Computer, https://www.praat.org.
5. Pestell FVA User Guide, https://www.pestell.com.

INSTITUTE OF LEGAL EDUCATION

(Managed by L TO J LAW ASSOCIATES)

NO. 08, ARUL NAGAR, SEERA THOPPU,
MARUDHAANDA KURICHI, SRIRANGAM - 620102,
TAMILNADU, INDIA.

ISSN 2583-2344