iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.79148

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

A Forensic-Grade Video Conversion Tool with Cryptographic Integrity Verification(V-CON-V)

Santosh Kumar[1], Subrato Sarkar[2], Asmita[3]
[1, 3]*Department of Computer Science and Applications, NIELIT, Patna, India*
[2]*Digital Forensics Division, Central Forensic Science Laboratory, Pune, India*

Abstract: ***In this work V-CON-V (Video CONverter and Verifier), an integrity-centric automated video conversion and verification tool was developed to address the critical challenge of incompatible video evidence formats in forensic investigations in India. The system converts various heterogeneous and common video formatslike .dav, .avi, .mov, .mkv, .webm, .flv, .wmv, .3gp, .ogg, .mts, .ts into most acceptable standardized .MP4/H.264/AAC format while providing cryptographic proof of integrity preservation. A dual-hash approach also calculates hashes before and after conversion of the particular video format using SHA-256 which enables forensic practitioners to demonstrate in court of law that the converted file is a faithful representation of the original evidence. The system automatically produces in-depth PDF forensic audit reports containing file metadata, hash values and conversion logs which full fill the legal documentation requirements. Experimental evaluation on diverse real-world video datasets demonstrates a 99.9% successful conversion rate with complete integrity traceability and an average 22.2% storage reduction on 50 different video formats without perceptible quality degradation. The proposed system provides a robust, auditable and legally defensive video conversion solution for digital evidence preservation and analysis in implementation of the clauses of BNSS and BSA, 2023 in India.***

Keywords: Video converter, Hash value, Mp4, Cryptography, BNSS, BSA.

I. INTRODUCTION

The proliferation of computer video evidence in crime and in the field of investigations has posed serious problems to forensic practitioners and legal systems [1]. Nowadays, video evidence originates and obtained through a variety of sources, such as CCTV cameras, video recording cameras, smart-phones and surveillance systems at a large scale. Due to various common as well as various proprietary formats of videos available around us, it became a real challenge for subsequent analysis under a particular software which generally accepts one or very few fixed formats as input. Therefore, to analyse those versatile video formats, there is a need to convert the input video into a single output video format for further analysis. There are numbers of such kind of video converting tools which converts from one video format to other video formats but there are no specific converting traceability and integrity to prove in the court of law. In India, from the year 2023, Bharatiya Nagarik Suraksha Sanhita (BNSS) &BharatiyaSakshyaAdhiniyam (BSA) 2023 is applicable instead of older version of Indian Penal Code(IPC) & Indian Evidence Act (IEA), where it has been mandate to the investigating agencies for secure recording of the Scene of Crime (SoC), statements of accused and victimswith preservation of integrity during transmission encryption standards and upholding of extensive audit trails during trials in the court of law vide various Section 176, 105, 85,185,173, 176, 180, 183(1), 183(6)(a), 497 of BNSS[2][3].The video conversion tools available traditionally do not provide built-in features of cryptographic verification, as well as legal documentation which introduce audit trail gaps that therefore interfere with the value of evidence in the court of law [4]. In the real experience of the authors, it has been observed in the forensic analysis, not all type of video formats can be fed to specific software because most of the specific software is built for feeding certain fixed video formats. Most of these type of software which are generally used for subsequent analysis the contents, subject of interest uses MPEG-4 (MP4) formats and H.264 video and AAC audio codec which place compatibility and reduce the obstruction in handling the video evidence. In this work we have introduced a video converting tool which is able to convert eleven common & proprietary video formats to a single video format, .MP4. Another vital issue observed by the authors which is also addressed in this work to maintain the integrity of the video evidence. While converting, the container and/or the contents of the video file, the hash value of the evidence changed which sometimes arise vital confusion in the court of law because in most of the traditional and available tool do not have the integrity traceability which could be proved in the court of law later though in forensic science the content of the video data file should be intact at the time of conversion as described by Gregory S. Wales MS et al [5] in their paper.

So in this work we basically integrate some open source tools which are easily available in the Github repository and other open source platform, and we named it "V-CON-V" in abbreviation of "**V**ideo **CON**verter and **V**erifier)" to build a combined tool which not only converts the most common & proprietary video formats like .dav, .avi, .mov, .mkv, .webm, .flv, .wmv, .3gp, .ogg, .mts, .ts to .MP4 but also will show the proper tracing of the integrity of the successful conversion and prepare a PDF log report which may be admitted in the court of law. It is an automated pipeline that is of forensic grade and also meets the challenges often faced by investigation agencies and scientist of forensic labs. This tool is built in a forensic perspective having the following features:

1) Format Standardization and Conversion: Systematic conversion of eleven selected standard video format which are world-wide acceptable and largely available and most common video formats to the standardized video format, namely, .MP4/H.264/AAC format which is used as an common input of any globally accepted software for subsequent analysis of the video contents or used for video enhancement purpose in any forensic science laboratories [6][7]. In general, digital videos are made up of codec (compression & decompression algorithms) and containers (wrapper formats)[8] H.264/AVC & H.265/HEVC are the most common codecs used for surveillance cameras and mobile devices. In our work we have used the FFmpeg[9], an open-source platform known as one of the best tool for video conversion uses H.264/AVC codec for converting the video files. Many other commercial tools available for video analysis also use FFmpeg as video converting engine. On other hand we have chosen the final output video format as .MP4 because of its high compatibility as it is supported in all modern devices and software, Excellent compression efficiency, versatility and metadata support, balanced quality to size ratio thought it has lossy compression but that also be considered as strategic algorithm [10].

2) Cryptographic Integrity check at input and output: Cryptographic hash algorithms such as SHA-256 offer mathematical evidence of the integrity of data by such properties as determinism, collision resistance, avalanche effect [11][12]. One bit alteration in the input would result in an entirely new hash which is why it is the best fit in ensuring evidence integrity throughout processing paths [13]. It converts the input data of any length to a 256 bit hexadecimal string that is fixed and irretrievable in size. For any video file the hashing can be carried out of the video container as well as the video contents. As FFmpeg itself takes care for maintaining the integrity of the video contents while conversion. So, in this work, Hashing with SHA-256 algorithm is focussed on the input and output video container only.

3) Automated Legal Reporting: AutomatedPDF audit report generation using the standard application, namely, FPDF [14] which can be embedded with or without modification after successful conversion mentioning the details/ metadata of input as well as output video file with the hash value in automatic way is essential as a document in the court of law. This is the system auto generated report like other software used in forensic analysis is admissible in the court of law in India and other countries.

4) Legal Compliance: In Indian context, the Bharatiya Nagarik Suraksha Sanhita (BNSS) and BharatiyaSakshyaAdhiniyam (BSA), 2023 defines extensive standards of digital evidence processing such as secure recording and transmission, End to End encryption standards and tamper proof preservation requirements. In the Section 176, 105, 85,185,173, 176, 180, 183(1), 183(6)(a), 497 of BNSS where recording by Audio-video electronic means is specially emphasized. It is also mandatory to submit the audio-video electronic recording along with the 63(4)(c) certificate in the court of law both by the party as well as the expert. In the 63(4)(c) certificate, there are provisions for submitting the hash value of the digital evidence to preserve the integrity of the digital evidence throughout the investigation and trial process. Therefore, with three above mentioned features, this forensic-grade tool is meant for various video formats generally produced by the common video capturing instrument by the investigation agency as the first responder the SoC which is mandatory for digital evidence handling as per the clause of recently introduced Bharatiya Nagarik Suraksha Sanhita(BNS) &BharatiyaSakshyaAdhiniyam (BSA), 2023 [2][3]. Table I: compares the proposed system of video processing tools to the available various video processing systems either in open-source platform like FFmpeg [9], Handbrake [15] or commercial platform like AMPED FIVE [16], MD-Video [17], Adobe [18] etc which are related to the purpose of our work. In the above-mentioned tool, all the three fundamental features like successful conversion, hash verification followed by system generated report in legal and forensic context are not addressed.

TABLE I
COMPARISON OF VIDEO PROCESSING SYSTEMS

System	Conversion format support	Integrity verification	Audit Reporting	Legal compliance
Amped FIVE, M/s SRL	Any to .MP4 and other	None	Only for the output	None
FFmpeg CLI	Any format to any format	Possible	None	None
HandBrake	Any format to any format	Possible	None	None

MD-Video, M/s GMDSoft	Certain fixed formats to certain formats	Possible	Not specially for Video conversion	None
Adobe Media Enc. Commercial System	Certain fixed formats to certain formats	None	None	None
V-CON-V	Eleven widely used format to most acceptable format .MP4	Integrated SHA-256 Value	Software generated PDF audit report admissible in the court of law	BNSS, BSA aligned

This system is a major improvement on the conventional type of the video converters by incorporating the standardization of the format, cryptography verification and legally-driven reporting in one automated pipeline. To the best of our knowledge, there are no such tool available that offers these kinds of mixed functionalities in a single platform which are essential requirements in forensic analysis and legal compliance. Three fundamental areas as discussed below were addressed in preparation of such kind of tool. The traditional tool like V-CON-V, either from open source or commercial do not meet all the three fundamental areas which are utmost important to establish the fact in the court of law.

The rest of the paper is divided into the following sections: II. System Architecture and Design, where the Architecture and design of the software have been explained in details, III. Experimental Evaluation & Discussion where, nearly 50 real data sets of various formats available in common videos were examined using this software and the results were discussed to validate the software and IV. Conclusion & Future Works, where the results were summarised, discussed the pros and cons of the proposed software and the scope for better improvement in future.

II. SYSTEM ARCHITECTURE AND DESIGN

A. System Overview

Our proposed software V-CON-V implements a five step pipeline program (Fig. 1)developedwiththeintendofworkingwithforensic evidences.

1) *Stage 1: Secure Evidence Acquisition:*The systemreads authorized digital video evidence to in compliance with BNSS & BSA as CCTV systems, mobile devices and otherauthorizedrecordinginstruments. Evidencefilesare uploaded to a controlled Google Drive environment, making logical isolation and limited access. The files are uniquely identified and ready to be left further forensic processing. This systemiscompatiblewithatotalofelevenformats: .dav, .avi,.mov,.mkv, .webm,.flv,.wmv,.3gp,.ogg,.mtsand.ts.
2) *Stage 2: Environment Initialization and Directory Structuring:* The Google Colab [19] is used to initialize a controlled processing environment. The necessary open-source platform tools and libraries (FFmpeg and cryptographic tool) are installed and tested out. The workflow is automatically configured to generate a standardized directory structure to partition input evidence, transformed output, cryptographic hashes and log reports such that they can be traced and audited.
3) *Stage3:BaselineCryptographicHashGeneration:* ThesystemcalculatesaSHA-256hashofeachoriginalevidencefilebeforeanychangeismadetoit. This hashisthemainintegritybaselineanditissafelyarchived with file attributes like size, format and time stamping of the filesandotherfileattributeslikettheformat. Thebase hash provides a set point against which future verification and chain-of-custodyrecordsarecomparedandconfirmsthispoint.
4) *Stage 4: Forensic-Grade Video Conversion:* It is a standardized video format conversion system run on FFmpeg which keeps a high quality of evidence whilst maintaining evidentiary quality. Any input, regardless of its heterogeneity, is transcoded to H.264 video and AAC audio whichareencapsulatedasMP4containerthroughcontrolled parameter like:

Parameters={-c:vlibx264,-presetmedium,-crf23, (1)

-c:aaac,-b:a192k,-pix_fmtyuv420p}

VideoEncodingParametersandTheirSignificance

The conversion of the video on the FFmpeg, an open-source platformwith the encoding parameters selected with great caution to allow maximum visual fidelity, interoperability, and forensic reliability to the videos being converted to the required format. The set of parameters applied are as follows:

a) Video Codec Selection (-c:vlibx264):Video streams were coded with the H.264/AVC standard with the help of the encoder of libx264. H.264 compression standardiscommonlyusedbecauseitishighlyefficient, stable andwidelycompatibleinplaybacksystems ofthesystem inquestionas it is widely accepted video codec algorithm.

b) *Encoding Preset (-presetmedium):*Theencodingpreset isdecided to trade off the efficiencyofcompressionversusprocessingtime[?].Thedefaultsettingofthex264 encoderis the so-called mediumpreset, which is a moderate trade-off between the encoding speed and the size of the file delivered to the user of the encoder codec. The preset is suitable in processing wherein efficiency and consistency are needed.

c) *Quality Control Using Constant Rate Factor (-crf 23):* Constant Rate Factor (CRF) regulates the quality of perceptions of the encoded video on the scale of 0 to 51, withalownumberdenotingahighqualityofthevideoencoded in it. The CRF of 23 was chosen because it provides an appropriate trade-off between the visual quality and storage efficiency,wherenonoticeablelossofevidentiarydetailtakes place.

d) *Audio Codec Selection (-c:aaac):*The encoding of audio streams was done with the help of the Advanced Audio Coding (AAC) standard. AAC offers a higher quality audio at reduced bitrates than legacy codecs, and isthedefaultaudioformatofMP4containers,toensureidentical playback of all forensic analysis software and standard media players.

e) *Audio Bitrate Configuration (-b:a192k):*Theaudiobitratewaschosenas192kbpstopreservethe clarity of speech and the details of the ambient sound, whicharesometimesessentialduringtheforensicinvestigation process. Abit rateof192kbpswasusedinordertopreserve the details of the speech and the ambient sound which may be crucial in the process of forensic examination in most cases. Such bit rate provides the quality reproduction of the audio without the excessive growth of the file size issues.

f) *Pixel Format Enforcement(-pix_fmtyuv420p):* The pixel format had been explicitly defined as the most universally supported recent chroma sub-sampling format of videoplayback,namelyyuv420p. Theimplementation of such format guarantees the greatest possible compatibility with judicial playback systems, forensic software and old media players,thusavoidinginconsistenciesinplaybackwhenexaminingtheevidenceandinplayingitincourtroomsettings.

g) *Summary:*The chosen encoding setting allows maintaining both forensic integrity and court-compatible video outputs as well as reliability in video playback and efficient storageofvideofiles. Alltheseparameterscontribute to reproducibility, interoperability and adherence to the best practices pertaining to managing digital evidence solutions to crime scene investigations and evidence handling processes at the crime scene, respectively.

5) *Stage 5: Post-Conversion Integrity Verification and Reporting:* After conversion, a second SHA-256 hash is generated for each processed output video file. The systemcorrelatesoriginalandconvertedhashes,filemetadata, and processing logs to confirm integrity preservation during format standardization.

An automated forensic report is generated in PDF format containing:

- OriginalandconvertedfileSHA-256hashes
- Filesizeandformatdetails
- Completeprocessingparametersandconversionstatus
- Chainofcustodyandaudittrailinformation
- Statementsoflegalcomplianceandevidenceintegrity

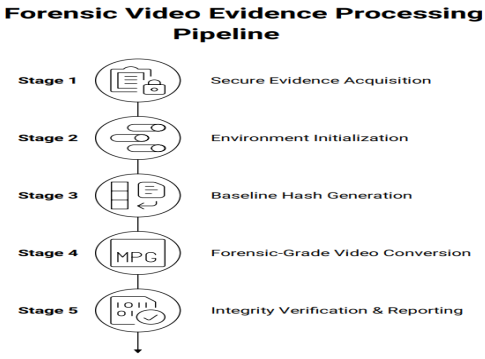


Fig. 1: System architecture with the five-stage processing pipeline integrity check and legal standard check.

B. Security and Integrity Measures

Thesystemalsoimplementsseveralsecuritylayers:

- CryptographicVerification:SHA-256hashinginthe input and output stages
- AuditLog:Immutablelogsofprocessingoperations
- Error Handling: Failure with detail documentation

C. ImplementationDetails

ItsPython implementationconsistsofthefollowingkey elements:

- FFmpeg Integration:Forvideoconversionwith forensic-grade parameters
- Cryptography Library:ForSHA-256hashcalculations
- PDFGeneration:Forautomatedauditreportcreation, FPDF is used
- Metadata Extraction: For evidence documentation in a forensic context

The proposed system is implemented using Python programming language [20] taking advantage of its large ecosystemof libraries to make the system reliable, reproducible, and to adhere to digital forensic standards. These include:

1) *FFmpegIntegration(VideoProcessingandConversion):* FFmpeg is integrated as the primary backend for forensic- grade video processing and video conversion. For defined parameterssuchascodecselection,constantratefactor(CRF), pixelformat,andaudiobitrate,itreducesqualitydegradation while enabling re-encoding and format normalization under control. The base function of the platform is to leverage multiple libraries of codecs to gain insight into multimedia files as well as allow playback, streaming, and conversion of multimedia files. In forensic analysis, FFmpeg generally utilized to inspect metadata and play and examine native file without transcoding. Thesystemacceptsa widerangeofinput video formatsfromtheCCTV system, body worn cameras, mobile devices, and other digitally recorded materials. Metadata preservation and frame integrity areconsideredduringprocessingtopreventtheinjectionof artifacts that could interfere with forensic examination.This ensures legal review tools' compatibility and overall transparency of the evidence processing pipeline.
2) *CryptographyLibrary(IntegrityVerificationusingSHA- 256):* To ensure data integrity and authenticity, cryptographic hash functions are used with Python's cryptography libraries. Hash values computed through SHA-256 are generated for video evidence before and after processing by the system. These hash values are unique digital fingerprints that make it possible to detect any modification made by an intruder.The hash values are logged and embedded within the audit report, therefore, supporting chain-of-custody requirements and supporting digital forensic best practices.
3) *PDFGeneration(AutomatedAuditReportCreation):* Automatedforensicauditreportsaregeneratedunderthe FPDFlibrary. The reporting module includes cryptographic hash,metadataattributes,processinglogs,timestamps,and conversionparametersinto astructuredandhumansunderstandable PDF document.
   This automated documentation process minimizes manual errors and ensures uniformity regarding multiple cases. Such reports can be presented legally, testified by experts with adequate knowledge, and stored for a long time to satisfy the evidentiary documentation requirements.
4) *Metadata Extraction (Evidence Documentation and Analysis):*A comprehensive metadata extraction is performed torecordthetechnicalandcontextualattributesofthevideo evidence. The metadata that is extracted includes the type of codec, resolution, the frame rate, the duration of the video, bit-rate, the container format, and timestamps on when it was created.

Metadata analysis plays a critical role in forensic investigationbyhelpingsourceidentification,authenticityverification, and recording conditions. This output, along with all metadata gathered from various sources, is preserved alongside the processed evidence and included in the final audit report.

D. LegalComplianceFrameworkinIndianContext (BNSS & BSA)

V-CON-V isspecificallydesignedtocomplywithBharatiya Nagarik Suraksha Sanhita(BNSS) &BharatiyaSakshyaAdhiniyam (BSA), 2023requirements as it **s**upports all authorized sources of evidence,includingmobilephones,CCTVsystems,andvideo recorders, Identified Purposes All-Inclusive; Court, Identification, and evidential Purposes,Security Standards – mathematical proof Integrity Verification and Transparency in Processing and it keeps audit trails and documentation like court admissibility features. This tool also have the features like reproducible processing parameters, Expert- witness ready documents and it has adherence to the agreed forensic standards.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

III. EXPERIMENTAL EVALUATION

In software development, Verification and Validation are essential processes that ensure the quality and effectiveness of a software product. Verification checks if the software is built correctly according to specifications, while validation ensures the software meets user needs and performs well in real-world conditions. Together, they help identify and fix issues early, improving the reliability and user satisfaction of the final product. Here also V-CON-V tested for validation into three type of testing like :
Correctness testing: which is used to test the right behaviour of the system; Performance testing: which is an independent discipline and involves all the phases as the main stream testing life cycle i.e. strategy, plan, design, execution, analysis and reporting and Reliability testing: which discovers all the failure of the system and removes them before the system deployed. To follow the above validation program, we planned to test fifty (50) video files of diverse data set representing real world evidentiary scenarios as follow:

A. Experimental Setup

- 15CCTVfootagefiles(dav,10.1GB)
- 10videocamerarecordings(AVI,14.7GB)
- 12mobilecameraevidencefiles(MKV,5.2GB)
- 8crimescenevideos(WMV,8.9GB)
- 5caseopeningrecordings(MOV,5.3GB)
- Total:50files,44.2GB

These video data sets were also tested through other available and globally accepted software for hash value of SHA-256 algorithm. After converting the video files, these were again tested for hash value of the converted file. There were perfect agreements in two sets of hash value with our toll, V-CON-V.

B. PerformanceMetrics

Evaluation considered both technical and legal compliance metrics as follow:

Metric	Value	Significance
SuccessfulConversions	99.9%	High reliability for forensicevidence processing
Average StorageReduction	22.2%	Efficient storage utilizationand evidence management
HashVerificationSuccess of input and output file	100%	Completecryptographicintegrity and traceability
ReportGenerationSuccess	100%	Automatedandcomprehensiveforensicdocumentation
ProcessingTime	2.4xreal time	Operationallyfeasibleforpractical deployments

C. Discussion

1) AdvantagesforForensicPractice:

V-CON-V offers several advantages over other existing tools for forensic evidence management.
Legal Compliance: Provides end-to-end compliance with BNSS requirements, addressing a critical gap in existing tools.
Integrity Assurance: SHA-256 Cryptographic verification provides mathematical proof of evidence integrity throughout processing.
Automated Documentation: Eliminates manual documentation errors and ensures comprehensive chain of custody records.
Cost Effectiveness: Leverages open-source tools while maintaining forensic-grade quality and legal validity.

2) Limitations:

Currentlimitationsinclude:

- Dependence on FFmpeg codec support for proprietary formats
- Processing time constraints for very large evidence col- lections
- Insufficient robustness, as it currently does not support video conversion from any format to any other format with hashing .

3) PracticalApplications:

Thesystemhasbeensuccessfullydeployedin

- Managementforbody-worncamera, CCTV camera footage by the Investigation Agencies
- Courtevidencepreparationformixed-formatevidence
- Digitalforensicslaboratoriesforevidenceanalysis

IV. CONCLUSION AND FUTURE WORK

A. Conclusion

This paper introduced a digital evidence management critical problem-solving system, namely, **V-CON-V** which is an automatedvideoprocessingpipeline. Thesystemoffers a strong answer to the processing of forensic evidence by standardizingtheformat,verifyingthecryptographicintegrity, and their automated legal documentation mechanism thereby providing a powerful solution to the analysis of forensic evidence. Experimental assessment indicates that itis highly reliable (99.9% percentage) and stored significantly (22.2%percentcut)andentirelytraceableintermsofintegrity.

With its alignment to the requirements of the legal frame- work, namely **BNSS**, to the requirements of the **V-CON-V**forensic video evidence processing is a crucial step in the right direction, and the software is open-source, which givesit a high level of transparency and reproducibility, as well as provides it with a competitive edge over peers.

B. FutureWork

Futureresearchdirectionsinclude:

1) We intend to develop a Windows-based application for thisvideoconverter,allowingustoworkinoffline mode on a local machine, which is a primary requirement for any forensic examinations [4].

2) Weaimtoincreasetherobustnessofthismodelsoit can handle any input format and generate any output format,whileperforminghashcalculationsatbothstages along with auto generated audit report.

3) We indent to develop video recording software which calculates the hash of recorded video with Real-time evidence processing capabilities for law enforcement agencies.

4) Integrationwithe-Courtsandnationalevidencemanagement systems.

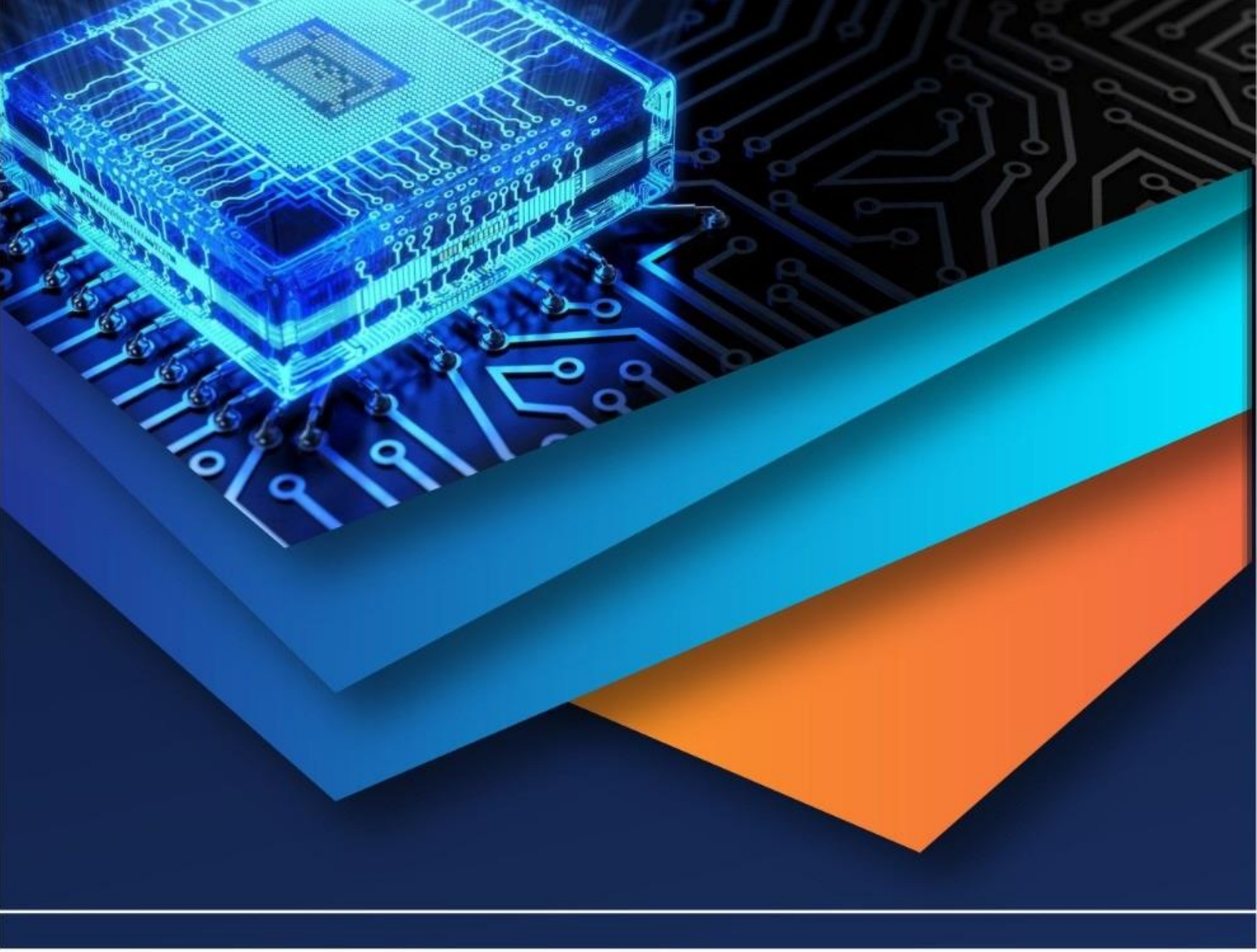
V. ACKNOWLEDGMENT

The authors express their gratitude and special thanks to the Director&HoD (Digital Forensic Division)of the CentralForensicScienceLaboratory (CFSL),Puneforgrantingaccess to the laboratory facility to test and compare the efficiency of the proposed software with real datasets and relevant legal compliance materials. The authors also acknowledge the Executive Director of NIELIT, Patna for providing technical advices. This study was carried out at CFSL, Pune in accordance with ethical standards governing research on digital evidence.

REFERENCES

[1] W. Koehler, “Digital evidence: The ethical and legal challenges,” Forensic Science International, vol. 208, pp. 1–8, 2010.
[2] Government of India, “Bharatiya Nagarik Suraksha Sanhita, 2023,” The Gazette of India, 2023.
[3] Government of India, “BharatiyaSakshya Adhiniyam, 2023,” The Gazette of India, 2023.
[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. Academic Press, 2011.
[5] Gregory S. Wales MS et al., “Multimedia stream hashing: A forensic method for content verification,” J Forensic Sci. 2022;00:1–12.
[6] S. Hoelzer, “Video forensics: The admissibility of digital imaging in court,” Journal of Visual Communication in Medicine, vol.32, no.2,pp.68–73,2009.
[7] B. Nikkel, Practical Forensic Imaging: Securing Digital Evidence with Linux Tools. No Starch Press, 2016.
[8] G. Sullivan et al., “Overview of the High Efficiency Video Coding (HEVC) standard,” IEEE Trans. Circuits Syst. Video Technol., vol. 22, no. 12, pp. 1649–1668, 2012.
[9] FFmpegDevelopers,“FFmpeg: A complete, cross-platform solution,”2023. [Online]. Available: https://ffmpeg.org
[10] ISO/IEC 14496, “Information technology. coding of audio-visual objects, part 14: Mp4 file format,” 2003
[11] NIST, “Secure Hash Standard (SHS),”FIPSPUB180-4,2022.
[12] National Institute of Standards and Technology (NIST), “Secure Hash Standard (SHA-256),” FIPS PUB 180-4, 2015.
[13] B. Carrier, “Defining digital forensic examination and analysis tools,” Digital Research WorkshopII,2003.
[14] O. Plathey, “FPDF: Free PDF Generation Library,” 2023.
[15] https://en.wikipedia.org/wiki/HandBrake
[16] https://ampedsoftware.com/five
[17] https://www.gmdsoft.com

[18] https://helpx.adobe.com/in/media-encoder/using/file-formats-supported-import.html
[19] https://colab.research.google.com
[20] Python Software Foundation, “Python Language Reference,”2024.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY