Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 06 | June-2026
ISSN (O) 3107-6696

AUTHENTICITY ANALYSIS OF VIDEO EVIDENCE AGAINST RERECORDING ATTACKS

JAYASURYA. S, Ms. VISHNU PRIYA

B.Sc. FORENSIC SCIENCE

----------***----------

ABSTRACT

Video evidence has become an essential component of modern forensic investigations. However, the authenticity of digital videos can be compromised through re-recording attacks, where an original video is played on a screen and captured again using another recording device. Such attacks introduce distortions and remove important forensic traces, making authenticity Verification difficult. This study focuses on analyzing video evidence against re-recording attacks using metadata analysis and frame extraction techniques. Original and re-recorded videos were examined using Metadata2Go and In VID tools. The analysis identified significant differences in metadata information, image quality, compression artifacts, noise patterns, and frame characteristics. The findings demonstrate that combining metadata examination with frame-by frame analysis is an effective approach for detecting re-recorded videos and improving the reliability of digital video evidence in forensic investigations.

INTRODUCTION

Digital videos are widely used as evidence in criminal investigations, surveillance systems, legal proceedings, and media reporting. Due to advancements in technology, videos can be easily manipulated, edited, or re-recorded without obvious visual indications. One common method of manipulation is the re-recording attack, where an original video is displayed on a screen and recorded again using another device. Re-recorded videos often lose their original metadata and introduce visual artifacts such as screen glare, moiré patterns, flickering effects, and compression distortions. These changes make it difficult to determine the authenticity of the video. Therefore, forensic investigators require reliable methods to differentiate original videos from re-recorded ones. This study examines the effectiveness of metadata analysis and frame extraction techniques in detecting re-recording attacks and ensuring the integrity of video evidence.

STATEMENT OF THE PROBLEM

The increasing use of digital video evidence in legal and forensic investigations has raised concerns regarding its authenticity. Re-recording attacks can conceal the source of a video and remove important forensic information, making manipulated videos appear genuine. Traditional visual inspection is often insufficient to identify such tampering. Therefore, there is a need for effective forensic techniques capable of detecting re-recorded videos and ensuring the reliability of video evidence presented in investigations and courts.

OBJECTIVES OF THE STUDY

1. To study the concept of video authenticity and re-recording attacks.
2. To identify forensic indicators present in re-recorded videos.
3. To analyze metadata differences between original and re-recorded videos.
4. To examine frame-level artifacts using frame extraction techniques.
5. To evaluate the effectiveness of forensic tools in detecting re-recorded videos.
6. To improve the reliability of digital video evidence used in forensic investigations.

SCOPE OF THE STUDY

The study focuses on the forensic examination of original and re-recorded videos. It is limited to the analysis of metadata information and frame extraction using freely available forensic tools such as Metadata2Go and InVID. The research aims to identify indicators of re-recording

Journal Publication of International Research for Engineering and Management (JOIREM)
Volume: 04 Issue: 06 | June-2026
ISSN (O) 3107-6696

attacks including quality degradation, metadata inconsistencies, visual distortions, and compression artifacts. The findings may assist forensic investigators, law enforcement agencies, and legal professionals in authenticating digital video evidence

RESEARCH METHODOLOGY

Research Design

An experimental research design was adopted to compare original videos with their re-recorded versions.

Sample Collection

Original videos were captured using mobile phones and digital cameras. The same videos were displayed on electronic screens and re-recorded using another recording device.

Tools Used

- Metadata2Go.com
- InVID Plugin

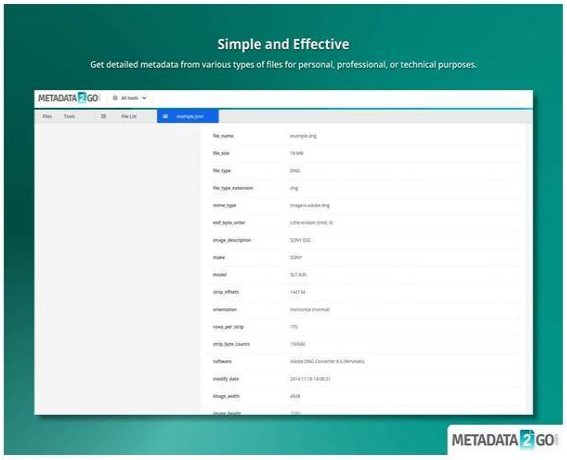
Procedure

1. Collection of original video samples.
2. Creation of re-recorded video samples.
3. Extraction of metadata from both videos.
4. Keyframe extraction using InVID.
5. Comparison of metadata and frame characteristics.
6. Recording observations and interpreting results.

DATA ANALYSIS AND INTERPRETATION

re — recorded videos

Collect the rerecorded videos and analyze metadata in metadata2go.com



Shows the frame extraction of original videos

Shows the meta data of re-recorded video

Parameters	Original Video	Re-recorded Video	Interpretation
Metadata Information	Complete and consistent	Modified or inconsistent	Indicates possible rerecording
Device Information	Original recording device present	Different recording device detected	Evidence of recapture
Video Quality	High quality	Reduced quality	Quality degradation due to re-recording
Noise Pattern	Natural sensor noise	Irregular noise pattern	Indicates video recapture
Screen Glare	Absent	Present	Common artifact in re-recorded videos
Moiré Pattern	Absent	Visible	Produced by screen recording
Compression Artifacts	Minimal	Increased	Evidence of double compression

Interpretation

The analysis revealed significant differences between original and re-recorded videos. Metadata inconsistencies were observed in re-recorded videos, including changes in device information and timestamps. Frame analysis showed screen glare, moiré patterns, brightness variations, and compression artifacts. These indicators confirmed the presence of re-recording attacks and demonstrated the effectiveness of forensic analysis techniques.

FINDINGS OF THE STUDY

1. Re-recorded videos showed clear quality degradation compared to original videos.
2. Metadata inconsistencies were observed in device information and timestamps.
3. Frame extraction revealed screen glare and moiré patterns unique to re-recorded videos.
4. Noise characteristics differed significantly between original and re-recorded videos.
5. Double compression artifacts were visible in re-recorded videos.
6. Metadata analysis alone was insufficient; combining multiple techniques improved detection accuracy.
7. The forensic tools used successfully differentiated original videos from re-recorded videos.

SUGGESTIONS

1. Investigators should use both metadata analysis and frame extraction techniques during video examination.
2. Multiple forensic tools should be employed to improve accuracy.
3. Advanced AI-based forensic techniques may be integrated into future studies.
4. Proper preservation of original video evidence should be ensured during investigations.
5. Training programs should be provided for forensic analysts to identify re-recording artifacts effectively.

Further research should include larger datasets and advanced video manipulation techniques.

LIMITATIONS OF THE STUDY

1. The study used a limited number of video samples.
2. Metadata can be altered, deleted, or manipulated.
3. High-quality re-recording devices may reduce visible distortions.
4. Detection accuracy depends on the capabilities of forensic tools.
5. Environmental factors such as lighting and recording conditions may influence results.
6. The study focused only on metadata and frame extraction techniques.

CONCLUSION

The study successfully analyzed the authenticity of video evidence against re-recording attacks. The results showed that re-recorded videos contain identifiable forensic indicators such as metadata inconsistencies, screen glare, moiré patterns, quality degradation, and compression artifacts. Metadata2Go and InVID proved effective in detecting these indicators. The findings demonstrate that combining metadata analysis with frame-by-frame examination provides a reliable approach for identifying re-recorded videos. This contributes to improving the credibility, integrity, and admissibility of digital video evidence in forensic investigations and legal proceedings.

REFERENCES

1. Sencar, H.T., & Memon, N. (2013). Digital Image and Video Forensics. Springer.

2. Casey, E. (2010). Handbook of Digital Forensics and Investigation. Academic Press.

3. Samsons, J. (2012). The Basics of Digital Forensics. Syngress.

4. Ho, A.T.S., & Li, S. (2011). Multimedia Forensics and Security. IGI Global.

5. National Institute of Standards and Technology (2014). Guidelines on Mobile Device Forensics. ISO/IEC 27037 (2012). Guidelines for Identification, Collection and Preservation of Digital Evidence.

6. Wang, W., Shi, Y.Q., & Su, W. (2010). Double Compression Detection in MPEG Videos. IEEE Transactions on Multimedia.

7. Stamm, M.C., & Liu, K.J.R. (2013). Forensic Detection of Image Manipulation Using Statistical Features. IEEE Transactions on Information Forensics and Security.

8. Bayram, S., Sencar, H.T., & Memon, N. (2005). Source Camera Identification Based on Sensor Noise. IEEE Signal Processing Letters.