FORENSIC ANALYSIS OF TEMPORAL INCONSISTENCIES AND METADATA DISCREPANCIES IN CCTV FOOTAGE: A CASE STUDY

PRASOON, P.[1*] – MAHESWARI, M.[1] – ARSHAD, P. M. M.[1] – YADAV, A. K.[1]

[1] *Directorate of Forensic Science Services, Government of India, Telangana State, India.*

**Corresponding author*
e-mail: prakhar.prasoon01[at]gmail.com

(Received 03rd August 2025; revised 18th October 2025; accepted 11th November 2025)

Abstract. The forensic reliability of closed-circuit television (CCTV) footage is central to contemporary criminal investigations; yet temporal irregularities in recorded video often generate disputes regarding authenticity and alleged tampering. This case study critically examines temporal inconsistencies and metadata discrepancies observed in CCTV footage submitted for forensic evaluation, where the primary investigative question concerned potential digital manipulation. Two video clips captured from different camera angles (Cam3 and Cam5) were analysed using Dahua Smart Player Version 4.0.0 through a systematic methodology combining real-time playback, frame-by-frame examination, stopwatch-based time verification, cross-angle synchronization assessment, and metadata analysis. The findings reveal measurable discrepancies between on-screen time progression, real-time measurement, and metadata-reported durations, alongside fluctuating synchronization between camera feeds. However, no visual discontinuities, frame deletions, insertions, or compression artefacts indicative of deliberate tampering were detected. Instead, the anomalies are attributable to technical factors inherent to CCTV systems, including variable bit rate compression, frame rate fluctuations, system clock desynchronization, and recording load constraints. Critically, this study demonstrates that temporal drift and metadata-playback mismatches can arise even in authentic and continuous footage, challenging simplistic assumptions that equate timing irregularities with manipulation. The findings underscore the necessity for forensic practitioners to adopt a holistic, technically informed interpretive framework that integrates system architecture, encoding behaviour, and metadata structure before reaching conclusions on video authenticity. By distinguishing system-induced artefacts from intentional interference, this study contributes to improving the evidentiary assessment of CCTV footage and mitigating the risk of wrongful exclusion or misinterpretation of digital video evidence in judicial proceedings.
Keywords: *video forensics, time stamp inconsistency, metadata analysis, video authenticity verification*

Introduction

Closed-circuit television (CCTV) systems have become an indispensable component of contemporary surveillance and forensic investigations, providing critical visual evidence that often determines the outcome of criminal and civil cases. The reliability of this evidence, however, rests upon the integrity of the recorded data, particularly the accuracy of time stamps, frame sequences, and associated metadata. Any inconsistency in these parameters can undermine the evidentiary value of the footage, raising questions about its authenticity and continuity. Such anomalies may result either from technical limitations inherent in recording systems, such as frame rate fluctuations, storage compression, or bandwidth constraints, or from deliberate acts of tampering, including frame deletion, insertion, or metadata alteration (Huang et al., 2021). In forensic investigations, distinguishing between these two origins is essential to ensure accurate interpretation and admissibility of video evidence. CCTV systems generally rely on Digital Video Recorders (DVRs) or Network Video Recorders (NVRs) to capture and store visual data. DVR-based systems convert analog signals from

traditional cameras into digital format, while NVRs receive direct digital streams from IP cameras, enabling higher resolution and scalability (Saini et al., 2021). The recorded footage is typically encoded using compression algorithms such as H.264 or H.265, which significantly reduce file size but can introduce timing variations and frame dependencies. The encoding process may operate under constant bit rate (CBR) or variable bit rate (VBR) modes; the latter dynamically allocates bandwidth depending on motion or scene complexity, often leading to non-linear time progression during playback (Honovich, 2009). These compression mechanisms, while efficient, can create subtle inconsistencies in timing and frame intervals, an issue of particular concern when verifying the authenticity of surveillance footage.

Moreover, the quality and reliability of CCTV recordings depend on several system-level parameters, including the number of concurrent video feeds, camera resolution, network bandwidth, and the write speed of the storage medium. High system load can lead to frame drops or buffer delays, resulting in footage that appears visually continuous but exhibits irregular time progression (Bourouis et al., 2020; Sitara and Mehtre, 2016). The presence of dual-streaming configurations, where one high-resolution stream is recorded locally and a lower-resolution substream is transmitted for remote monitoring, can further complicate synchronization and time consistency. Additionally, variations in frames per second (fps), typically 25 fps (PAL) or 30 fps (NTSC), may be dynamically adjusted by the recording system, affecting both playback smoothness and time accuracy (Alexander, 2023). Beyond these technical aspects, intentional tampering remains a significant forensic concern. Manipulative acts such as frame insertion, frame deletion, timestamp alteration, or metadata falsification can misrepresent the sequence or timing of recorded events (Mohiuddin et al., 2023). Although modern editing techniques can conceal such modifications seamlessly within continuous footage, forensic analysts can often identify traces through inconsistencies in frame structure, double compression signatures, or mismatched metadata (Li et al., 2015; Shanableh, 2013; Wang and Farid, 2006). Therefore, comprehensive forensic evaluation, combining metadata extraction, frame-level analysis, and cross-referencing with external time sources, is vital to determine whether anomalies are a result of system limitations or deliberate interference.

In this case study, CCTV footage submitted by an investigative agency was examined to determine whether the video had been tampered with, as per the agency's specific query. During the course of this analysis, while examining the footage for any signs of tampering, discrepancies were observed in the progression of time displayed within the video, specifically, variations in the speed and continuity of the on-screen clock when compared with real-time measurement. Two clips recorded from distinct camera angles (Cam3 and Cam5) were selected for detailed analysis using Dahua Smart Player Version 4.0.0. The analytical process involved frame-by-frame examination, stopwatch-based timing verification, and metadata comparison to identify inconsistencies in time progression and total duration. Although the primary purpose of the analysis was to evaluate potential tampering, the study also revealed notable timing anomalies, underscoring the importance of understanding how technical characteristics of CCTV systems, such as compression algorithms, bit rate control, and recording limitations, can produce such discrepancies that might otherwise be misinterpreted as deliberate manipulation.

Materials and Methods

A pen drive containing several CCTV video footages was received in the forensic laboratory for analysis. Among the files, two video clips recorded from different camera angles, identified as Cam3 and Cam5, were found to be relevant to the investigation and were subsequently selected for detailed examination. The investigative agency's query focused solely on determining whether the provided videos had been tampered with in any manner. However, during the analytical process, while assessing the footage for indications of manipulation, discrepancies were observed in the progression of the on-screen time displayed in the footage, prompting a deeper evaluation of potential timing irregularities. For the purpose of examination, the analysis was conducted using Dahua Smart Player Version 4.0.0 compatible with the format of the submitted footage. Both videos were loaded into the software to assess their integrity and to detect any visual or temporal anomalies. The examination was carried out systematically in several stages (*Figure 1*). Initially, the videos were observed in real-time playback mode to identify any visible discontinuities, abrupt transitions, or skipped frames that might indicate tampering. Following this, the "Continuous Shots" feature available in Dahua Smart Player was employed to perform a frame-by-frame analysis (*Figure 2*), allowing close inspection of every frame transition to detect potential frame deletions, insertions, or duplications.

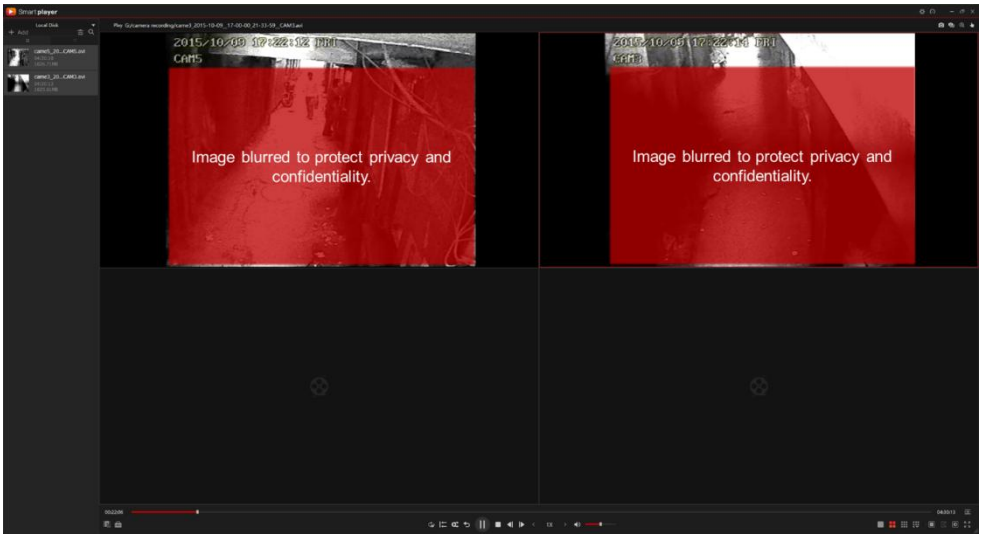

Figure 1. *Side-by-side playback of CCTV footage captured from two different camera angles (Cam3 and Cam5) showing the same scene for comparative analysis. This simultaneous viewing facilitated the assessment of temporal synchronization and continuity between the camera feeds.*

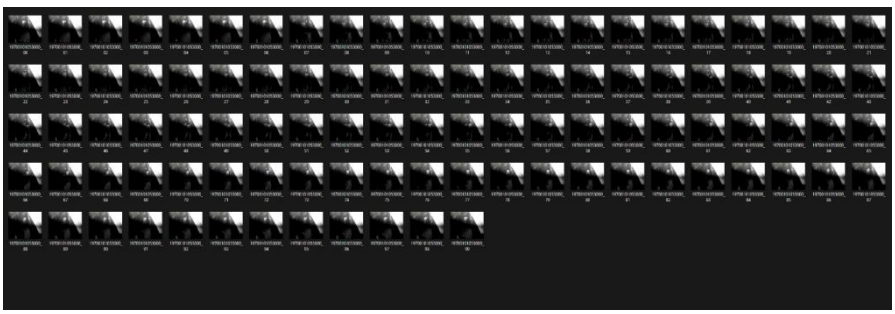

Figure 2. *Frame-by-frame examination of CCTV footage using the "Continuous Shots" feature in Dahua Smart Player Version 4.0.0. This process enabled detailed inspection of*

consecutive frames to detect potential insertions, deletions, or visual discontinuities indicative of tampering.

In the next stage, the on-screen clock displayed in the video was cross-referenced with the system stopwatch to compare the rate of time progression (*Figure 3*). This comparative approach was designed to identify whether the seconds and minutes in the footage advanced consistently with real-time measurement. During this phase, it was observed that the time progression in the CCTV footage was inconsistent when compared with the standard stopwatch. At the beginning of playback, the on-screen clock appeared synchronized with real-time measurement; however, as the video continued, the progression gradually became slower, and fluctuations in the timing rate were observed when matched against the standard stopwatch. Additionally, both video clips were played simultaneously to evaluate their temporal continuity (*Figure 4*). As the two cameras were recording the same scene from different perspectives, any temporal deviation between the two footages could indicate potential system desynchronization or file-level alterations.

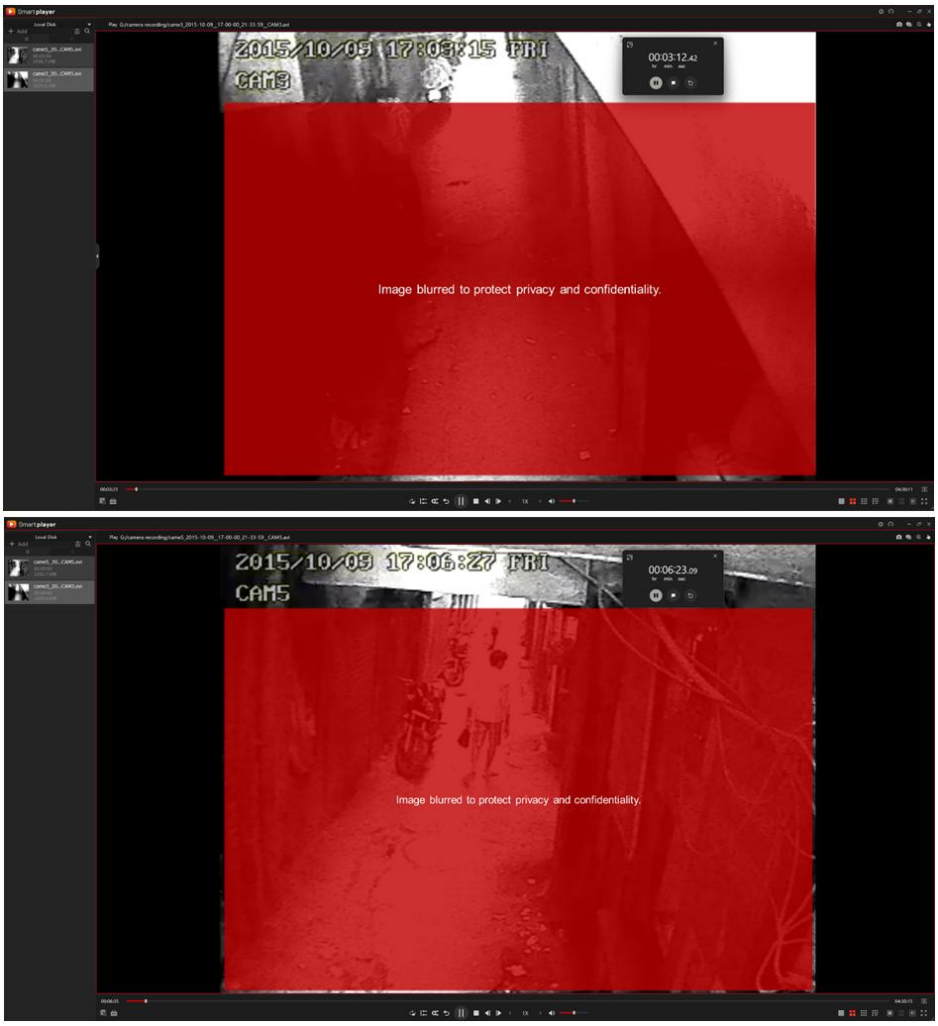

Figure 3. *Comparison of individual CCTV footage against a standard stopwatch to verify the accuracy of the on-screen time progression. This test was performed to identify variations in the rate of seconds and minutes in the footage relative to real-time measurement.*

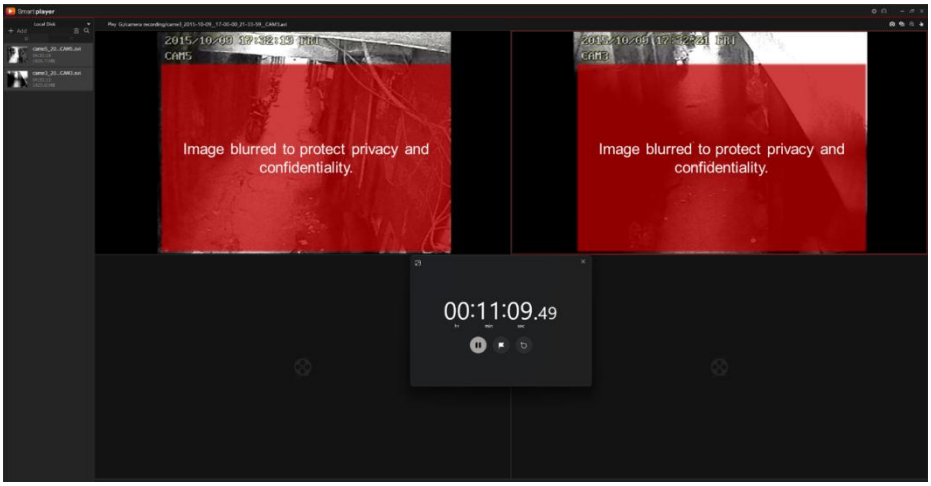

Figure 4. *Simultaneous comparison of two CCTV recordings from different camera angles alongside a standard stopwatch to assess the relative progression of time. The analysis revealed differing rates of time advancement between the recordings, suggesting possible system-level desynchronization.*

Subsequently, the metadata of both video files was extracted and analyzed. Parameters such as file creation time, modification time, codec information, total duration, and frame rate were recorded. Notably, differences were identified between the duration values reported in the metadata and the durations calculated from the frame sequence during playback. All observations, including the timing inconsistencies, frame transitions, and metadata discrepancies, were meticulously documented. These findings were later correlated with the known technical behaviour of CCTV recording systems to ascertain whether the anomalies resulted from system-level limitations, compression artifacts, or potential tampering attempts.

Results and Discussion

Upon detailed forensic examination of the CCTV footage using Dahua Smart Player Version 4.0.0, several key observations were recorded. The two selected video clips, Cam3 and Cam5, were analyzed independently and in parallel to assess both their internal consistency and their temporal correlation with one another. The primary focus of the investigation was to determine whether the videos exhibited signs of tampering or digital manipulation; however, during this analysis, additional inconsistencies relating to the timing and duration of the footage were also identified.

Time progression discrepancies

When the progression of the on-screen time displayed in the footage was compared against a system stopwatch, irregularities in the rate at which the seconds advanced were observed. In both Cam3 and Cam5, the on-screen clock displayed within the footage exhibited irregular time progression when compared with the standard stopwatch. At the start of playback, the footage appeared synchronized with real-time measurement; however, as the videos continued, the progression of seconds gradually became inconsistent, showing intermittent fluctuations in timing relative to the stopwatch. These irregularities indicate that the footage did not maintain a stable synchronization with real time throughout playback, suggesting possible variations in

frame rate or recording synchronization within the CCTV system. This variation in the rate of time progression between the two camera angles suggested the presence of recording desynchronization within the CCTV system. Despite these discrepancies, there were no abrupt visual interruptions, dropped frames, or distortions in the continuous playback of the footage. This indicates that the timing anomalies likely originated from technical inconsistencies in the recording or encoding process, rather than deliberate editing or manipulation.

Frame continuity and visual analysis

Using the Continuous Shots feature within the Dahua Smart Player, a frame-by-frame analysis was conducted for both clips. This method allowed for close inspection of transitions between consecutive frames to detect possible signs of tampering, such as frame insertions, deletions, or duplications. The results of this frame-level examination revealed no evidence of discontinuity or visual distortion between frames. The motion within the footage appeared natural and consistent, and there were no abrupt jumps or missing intervals that would suggest intentional alteration. The footage maintained logical spatial and temporal coherence across both clips.

Simultaneous playback and cross-angle comparison

Both video clips were then played simultaneously to evaluate the temporal alignment between the two camera angles. Since the cameras were positioned to record the same location from different viewpoints, synchronization between their timelines was expected. However, during this simultaneous playback, it was observed that the two recordings did not maintain perfect synchronization. The footage from Cam3 lagged slightly behind Cam5 at certain intervals, and this time difference fluctuated throughout playback. Such a pattern is consistent with variable frame rate (VFR) recording or system clock desynchronization, both of which can occur in multi-camera CCTV setups, particularly when devices share a common recording system but operate under differing load conditions.

Metadata and duration discrepancies

The metadata analysis of the video files revealed that the total duration values recorded in the metadata were consistent across both clips. Parameters such as file creation time, codec type, and total duration were extracted and compared with the playback characteristics observed within Dahua Smart Player Version 4.0.0. While the metadata for each clip indicated a total playback duration of approximately four hours, a detailed comparison with real-time measurement using a stopwatch showed a slight extension of about six to eight seconds beyond the metadata-reported duration. This variation was consistently observed in both Cam3 and Cam5 footage across multiple playback instances. These minor differences between the metadata duration and the actual real-time playback suggest the presence of temporal drift or synchronization lag, likely caused by system-level encoding or buffering processes during recording. As the metadata values themselves were accurate and no inconsistencies were found within the encoded file structure, the observed variations are interpreted as technical artifacts rather than indicators of intentional tampering.

Conclusion

The forensic analysis of the submitted CCTV footage revealed that while temporal inconsistencies were present in the form of varying time progression and duration discrepancies between camera angles, there was no evidence of deliberate tampering or frame manipulation. Both video clips were found to be visually continuous, with no signs of frame addition or deletion. The anomalies observed in the time stamps and playback duration were determined to be the result of technical irregularities such as system desynchronization, variable bit rate compression, or hardware-related recording delays. This case emphasizes the necessity of a comprehensive forensic approach in the evaluation of digital video evidence. Analysts must consider not only the visual content but also the underlying technical parameters, including metadata, compression behavior, and recording system limitations, before concluding that a video has been tampered with. Misinterpretation of system-generated anomalies as signs of editing could lead to the erroneous rejection of authentic evidence, potentially affecting the integrity of judicial proceedings. Therefore, this study reinforces that timing discrepancies alone do not constitute proof of manipulation. Instead, they highlight the complex interaction between digital recording mechanisms and playback interpretation. The careful documentation and explanation of such findings are crucial in maintaining the credibility and admissibility of CCTV evidence in forensic practice.

Acknowledgement

The authors express their sincere gratitude to Dr. S.K. Jain, Director-Cum-Chief Forensic Scientist, DFSS, and Dr. Rajiv Giroti, Director, CFSL Hyderabad, for their constant encouragement and support in carrying out research and development activities.

Conflict of interest

The authors confirm that there is no conflict of interest involve with any parties in this research study.

REFERENCES

[1] Alexander, R. (2023): Telling stories with data: With applications in R. – Chapman and Hall/CRC 622p.
[2] Bourouis, S., Alroobaea, R., Alharbi, A.M., Andejany, M., Rubaiee, S. (2020): Recent advances in digital multimedia tampering detection for forensics analysis. – Symmetry 12(11): 26p.
[3] Honovich, J. (2009): Security manager's guide to video surveillance. – IPVideoMarket 139p.
[4] Huang, Y., Li, X., Wang, W., Jiang, T., Zhang, Q. (2021): Forgery attack detection in surveillance video streams using wi-fi channel state information. – IEEE Transactions on Wireless Communications 21(6): 4340-4349.
[5] Li, S., Dhami, M.K., Ho, A.T. (2015): Standards and Best Practices in Digital and Multimedia Forensics. – Handbook of Digital Forensics of Multimedia Data and Devices 56p.

[6] Mohiuddin, S., Malakar, S., Kumar, M., Sarkar, R. (2023): A comprehensive survey on state-of-the-art video forgery detection techniques. – Multimedia Tools and Applications 82(22): 33499-33539.
[7] Saini, A., Kapoor, D., Manchanda, M., Gupta, P., Goyal, D. (2021): A Comparative Analysis of Various Forensic Tools used in Secure Digital Transmission. – Turkish Online Journal of Qualitative Inquiry 12(9): 2004-2015.
[8] Shanableh, T. (2013): Detection of frame deletion for digital video forensics. – Digital Investigation 10(4): 350-360.
[9] Sitara, K., Mehtre, B.M. (2016): Digital video tampering detection: An overview of passive techniques. – Digital Investigation 18: 8-22.
[10] Wang, W., Farid, H. (2006): Exposing digital forgeries in video by detecting double MPEG compression. – In Proceedings of the 8th workshop on Multimedia and security 10p.