Tamper-Resistant CCTV Footage Storage System Using Digital Watermarking and Hash Verification

Mrs. Poovizhi. D[1], . Mohamed Ashif. S[2], Muralidharan. K[3], Prasath. S[4] and Jegan. S[5]

[1] Assistant Professor, Department of Computer Science and Engineering
Parisutham Institute of Technology and Science,
Thanjavur,Tamilnadu-613001, India
poo.akshaya@gmail.com

[2] UG Student, Department of Computer Science and Engineering
Parisutham Institute of Technology and Science,
Thanjavur, Tamilnadu-613001, India
Mohamedashif18se@gmail.com

[3] UG Student, Department of Computer Science and Engineering
Parisutham Institute of Technology and Science,
Thanjavur,Tamilnadu-613001, India
muraliks1203@gmail.com

[4] UG Student, Department of Computer Science and Engineering
Parisutham Institute of Technology and Science ,
Thanjavur,Tamilnadu-613001, India
prasathsenthilkumar42@gmail.com

[5] UG Student, Department of Computer Science and Engineering
Parisutham Institute of Technology and Science,
Thanjavur, Tamilnadu-613001, India
s.jegannathan2003@gmail.com

Abstract— Ensuring the integrity and authenticity of recorded CCTV footage is crucial for reliable surveillance and forensic investigations. Traditional CCTV storage systems lack robust mechanisms to detect and prevent tampering, making them vulnerable to unauthorized modifications. This paper introduces a tamper-resistant CCTV footage storage system that integrates Least Significant Bit (LSB) digital watermarking and cryptographic hash verification to enhance video security. By embedding an invisible cryptographic hash using SHA-256 within each recorded frame, the system ensures the detection of any alterations to video content. Additionally, FFV1 lossless encoding is employed to maintain video quality while enabling real-time processing and verification with minimal performance overhead. The system also includes a security and alert module that prevents playback of tampered footage and generates automated alerts when discrepancies are detected. By combining cryptographic security with digital watermarking techniques, the proposed solution strengthens the reliability of surveillance infrastructures. The scalable methodology is suitable for various security applications, including law enforcement, corporate surveillance, and forensic investigations, ensuring that recorded evidence remains authentic, secure, and legally admissible.

Keywords— Digital Watermarking, Cryptographic Hashing, CCTV Security, Tamper-Resistance, Video Forensics, FFV1 Encoding, LSB Watermarking, SHA-256, Secure Storage, Data Authentication

INTRODUCTION

Traditional surveillance systems face significant challenges in ensuring the integrity and authenticity of recorded CCTv footage. Conventional storage solutions rely primarily on metadata timestamps and access control mechanisms, which are insufficient in preventing unauthorized modifications. As a result tampered footage poses serious security risk, especially forensic investigations where the credibility of video evidence is critical. The lack of robust tamper-detection mechanisms undermines the reliability of surveillance systems, making them vulnerable to manipulation.To address these concerns, this paper presents an advanced tamper-resistant CCTV footage storage system that leverages digital watermarking and cryptographic verification. The proposed approach integrates Least Significant Bit (LSB) digital watermarking to embed an invisible cryptographic hash within each recorded video frame, ensuring real-time integrity checks. By utilizing SHA-256 hashing, a unique digital signature is generated for every video sequence, allowing secure verification during retrieval. Additionally, FFV1 lossless encoding is employed to maintain the original video quality, preventing degradation while ensuring efficient storage and playback Then system enhances security by implementing a verification module that extracts and compares the embedded hash against a securely stored reference, detecting any discrepancies that indicate tampering. An automated alert mechanism notifies administrators of any unauthorized modifications, ensuring timely intervention. Designed for computational efficiency, the system supports real-time processing without imposing significant performance overhead, making it scalable for diverse security applications, including law enforcement, corporate surveillance, and forensic analysis. By integrating cryptographic security with digital watermarking, this research aims to enhance the reliability and trustworthiness of CCTV surveillance infrastructures. The proposed methodology contributes to the development of more secure, tamper-resistant video storage systems, ensuring that recorded footage remains authentic, legally admissible, and resilient against malicious alterations Ensuring the authenticity of CCTV footage is crucial for maintaining trust in surveillance systems, particularly in forensic investigations where video evidence plays a vital role. Tampered or manipulated footage can lead to misinformation this approach reduces the risk of false evidence and enhances accountability in security operations. Additionally, the system's scalability allows for seamless integration into various surveillance infrastructures, making it a valuable tool for organizations seeking to strengthen their video security protocols.

I. Literature Survey

Cox et al. [1] provided a comprehensive overview of digital watermarking techniques and their applications in multimedia security. The authors discussed various watermarking methods, including LSB, DCT, and DWT, and their use in image and video security. LSB watermarking was identified as a simple yet effective technique for embedding data in multimedia files. This study forms the foundation for our project's use of LSB watermarking to ensure video integrity. Celik et al. [2] proposed a lossless data embedding technique using LSB for multimedia files. The authors introduced a generalized LSB technique that allows for reversible data embedding without degrading the original content. The proposed method ensures high embedding capacity while maintaining the integrity of the original video. This study supports our project's approach of using LSB watermarking for embedding cryptographic hashes in video frames in. Swanson et al. [3] explored the use of cryptographic hash functions in multimedia data embedding and watermarking. The authors discussed the role of hash functions like SHA-256 in ensuring data integrity and authenticity. Cryptographic hash functions were found to be effective in detecting tampering and ensuring the authenticity of multimedia content. This study validates our approach of using cryptographic hashes for video verification. Farid [4] discussed the challenges and solutions in digital image forensics, including tamper detection. The author reviewed various forensic techniques, including hash-based verification, for detecting tampering in digital images and videos. Hash-based verification was identified as a reliable method for ensuring the integrity of digital evidence. This study supports our use of hash verification for tamper detection in CCTV footage.Wang et al. [5] evaluated the impact of video compression on image quality and data integrity. The authors proposed a structural similarity index (SSIM) for assessing the quality of compressed videos. Lossless codecs like FFV1 were found to preserve image quality and are suitable for applications requiring high data integrity. This study supports our choice of FFV1 for video storage, as it ensures minimal data loss during compression.

II. THE PROPOSED MODEL

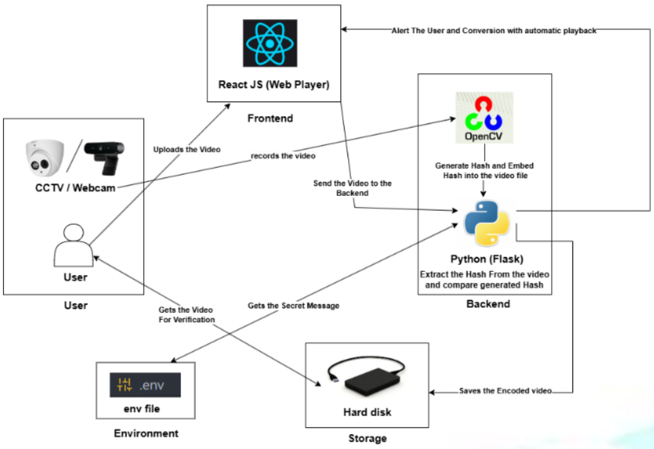
Ensuring the integrity and authenticity of CCTV footage is critical for security and forensic investigations. Traditional surveillance systems lack robust mechanisms to detect and prevent tampering, making video evidence susceptible to manipulation. The proposed model introduces a tamper-resistant CCTV footage storage system that integrates cryptographic hashing and digital watermarking to enhance video security. By embedding a SHA-256 hash into video frames using Least Significant Bit (LSB) steganography after initial storage in FFV1 format, the system ensures authenticity verification while maintaining high video quality.

A. Video Capture and Storage

In addition to ensuring lossless storage, FFV1 encoding offers several advantages that enhance the overall security and efficiency of the surveillance system. Its efficient entropy coding reduces storage requirements without sacrificing quality, making it ideal for long-term archival of CCTV footage. Furthermore, FFV1 supports error resilience, which is critical for maintaining data integrity in case of unexpected system failures or storage corruption. Once the video is stored in FFV1 format, the system proceeds with embedding a cryptographic hash using Least Significant Bit (LSB) steganography. This ensures that each frame carries a unique, invisible signature that can later be extracted for verification. The SHA-256 hashing algorithm is employed to generate a unique identifier for every video segment, which is then securely stored in a separate database for cross-referencing during integrity checks. By leveraging FFV1's lossless compression alongside cryptographic security measures, the system ensures that any attempt to manipulate or tamper with the footage—such as editing, compression, or frame deletion—can be reliably detected. This combination of technologies not only preserves forensic accuracy but also enhances the system's reliability for legal and security applications. The implementation of FFV1 encoding before any hashing or watermarking guarantees that the original video remains unaltered, providing a solid foundation for secure storage and authentication in surveillance infrastructures. Additionally, FFV1's ability to retain the exact quality of recorded footage plays a crucial role in forensic investigations. Unlike traditional lossy compression methods, which may introduce artifacts or degrade visual details, FFV1 ensures that even minute details—such as facial features, license plates, or small movements—are preserved with high fidelity. This makes it particularly valuable in legal proceedings, where even the slightest modification to video evidence can compromise its admissibility. By utilizing FFV1 as the initial storage format, the system eliminates any concerns regarding image degradation or inconsistencies caused by compression algorithms, thereby strengthening the credibility of surveillance footage.

B. Hash Generation and Embed

Once the video footage is stored in FFV1 format, the system generates a unique SHA-256 hash for each segment. This cryptographic hash serves as a digital fingerprint, ensuring the integrity of the recorded video. Even a minor change in the footage results in a completely different hash, making tampering easily detectable. The original hash is securely stored in a database for later verification. To enhance security, the system embeds the generated hash into the video frames using Least Significant Bit (LSB) steganography. This technique modifies the least significant bits of pixel values to encode data without perceptible changes in video quality. By distributing the hash across multiple frames, the system ensures redundancy, making it resilient against minor corruption or compression.in the use of tampered resistant footage


React JS (Web Player)
Frontend
Alert The User and Conversion with automatic playback
OpenCV
Generate Hash and Embed Hash into the video file
Python (Flask)
Extract the Hash From the video and compare generated Hash
Backend
CCTV / Webcam
User
User
Uploads the Video
records the video
Send the Video to the Backend
Gets the Video For Verification
Gets the Secret Message
.env
env file
Environment
Hard disk
Storage
Saves the Encoded video

The embedding process is designed to maintain video quality while ensuring robust security. Since LSB modifications do not visually alter the footage, the video remains unchanged to human observers. Additionally, any attempt to edit, trim, or compress the video disrupts the embedded hash sequence, making tampering easily detectable during verification. During playback or forensic analysis, the system extracts the embedded hash and compares it with the originally stored hash. If they match, the video is verified as authentic; otherwise, a mismatch signals tampering. This dual-layered approach enhances video security, making it reliable for forensic, surveillance, and legal applications.

C. Tamper Detection and Cross-Platform Verification

To ensure video integrity, the system employs a robust tamper detection mechanism that verifies the authenticity of every recorded segment. When a video is accessed for playback or forensic analysis, the system first extracts the embedded hash from the video frames. Simultaneously, a new SHA-256 hash is dynamically generated from the stored video file. This computed hash is then compared with the extracted hash to detect any discrepancies. If the two hashes match, the video is confirmed as untampered and remains accessible for viewing. If any form of modification—such as trimming, compression, or frame alteration—has occurred, the computed hash will differ from the embedded hash. In such cases, the system immediately flags the video as tampered and prevents its playback. Additionally, the system can generate automated alerts to notify relevant stakeholders, ensuring quick response to potential security breaches. This verification process is crucial in forensic investigations, legal proceedings, and surveillance applications where video integrity is paramount. One of the key strengths of the system is its cross-platform verification capability. Unlike traditional solutions that require specialized or proprietary software, this system enables video authenticity checks on any standard media player, such as VLC or Windows Media Player. This is achieved through the embedded hash, which remains intact regardless of the playback environment, ensuring that users can verify video integrity without technical constraints. For web-based verification, users can upload videos to the system's online platform, where the backend automatically extracts the hidden hash and compares it with the securely stored reference hash. If both hashes match, the system confirms the video as authentic and allows playback. If discrepancies are detected, the video is flagged, and an alert is triggered, preventing unauthorized or manipulated content from being misused. T his seamless verification process enhances trust and security in video evidence management. Whether used in law enforcement, corporate security, or public surveillance, the system provides a reliable way to authenticate videos across multiple platforms. By ensuring that only unaltered footage can be accessed and used, it strengthens accountability and prevents misinformation, making it an essential tool for video-based security applications.

To ensure broad compatibility, the system automatically converts FFV1-encoded video segments into MP4 format before playback. FFV1 is an efficient lossless codec that preserves the original video quality without compression artifacts, making it ideal for forensic and security applications. However, since FFV1 is not widely supported by common media players, conversion to MP4 allows seamless viewing on standard devices while maintaining the authenticity of the content During playback, the system first verifies the integrity of the video by extracting and comparing the embedded cryptographic hash. If the video passes the integrity check, it is converted to MP4 and made available for viewing. This ensures that only unaltered, authentic footage can be played, preventing any tampered or manipulated content from being accessed. This verification step is crucial in scenarios where video evidence is used for legal, forensic, or security purposes. By combining real-time verification, seamless format conversion, and proactive security monitoring, the system guarantees that only authentic, unmodified videos can be played or used as evidence. This multi-layered approach to security and integrity makes the system a powerful tool in surveillance, legal proceedings, and any application where video authenticity is critical

III. Conclusion

Ensuring the authenticity and integrity of video footage is crucial in surveillance, forensic investigations, and legal proceedings. The proposed system provides a robust solution by integrating cryptographic hashing, LSB steganography, and automated verification mechanisms. By embedding a SHA-256 hash within each video frame and storing the original hash securely, the system ensures that any modification to the footage is easily detectable. This approach effectively prevents tampering and guarantees the reliability of recorded content. The system's ability to convert FFV1-encoded footage to MP4 while maintaining authenticity ensures compatibility with standard media players. Additionally, its security module actively monitors verification attempts, blocking playback of any altered videos and generating alerts when discrepancies are detected. The implementation of an audit trail further enhances transparency, allowing organizations to track verification attempts and identify potential security breaches. By combining real-time tamper detection, cross-platform verification, and proactive security measures, this system significantly enhances the credibility of recorded footage. It serves as a vital tool in maintaining video integrity, ensuring that surveillance recordings and forensic evidence remain accurate and unaltered. This technology can be widely adopted in security-sensitive applications, providing a reliable framework for video authentication in both public and private sectors.

IV. Acknowledgement

Appreciation and gratitude to everyone who supported us make this research endeavor a success by assisting us in a variety of ways. Thank you for the words of encouragement to push ourselves to perform and attain our full potential.

References

[1] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, 1997.

[2] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless generalized-LSB data embedding," IEEE Transactions on Image Processing, vol. 14, no. 2, pp. 253-266, 2005.

[3] J. Fridrich, M. Goljan, and R. Du, "Lossless data embedding - New paradigm in digital watermarking," EURASIP Journal on Advances in Signal Processing, vol. 2002, no. 2, pp. 1-12, 2002.

[4] H. M. Al-Otum, "Secure semi-fragile watermarking for image authentication based on a hybrid approach," Journal of Visual Communication and Image Representation, vol. 25, no. 5, pp. 1134-1147, 2014.

[5] Y. Liu and J. Zhao, "A new video watermarking algorithm based on 1D DFT and Radon transform," Signal Processing, vol. 90, no. 4, pp. 1107-1118, 2010.

[6] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd ed. New York, NY: John Wiley & Sons, 1996.

[7] H. T. Sencar and N. Memon, "Overview of state-of-the-art in digital image forensics," in Algorithms, Architectures and Information Systems Security, Singapore: World Scientific, 2009, pp. 325-347.

[8] M. K. Khan and K. Alghathbar, "Cryptography-based secure data storage and sharing using HEVC and public cloud servers," Journal of Network and Computer Applications, vol. 35, no. 3, pp. 1001-1009, 2010.

[9] W. B. Pennebaker and J. L. Mitchell, JPEG: Still Image Data Compression Standard. New York, NY: Springer, 1993.

[10] H. Farid, "Digital image forensics," Scientific American, vol. 300, no. 6, pp. 66-71, 2009.