International Journal of Engineering and Techniques - Volume 12 Issue 2, March-April - 2026
RESEARCH ARTICLE OPEN ACCESS

Verixa: A Secure Blockchain-Based Video Evidence Verification Framework Using Trusted Hardware and Cryptographic Signatures

Kirthiga B[1], Narmadha U [2], Nandhini D[3], Harishwaran P[4], Dinesh S[5]

[1] *Artificial Intelligence & Data Science ,DMICE-600123*
Email: kirthiga1215@gmail.com
[2] *Artificial Intelligence & Data Science ,DMICE-600123*
Email: narmadha1310u@gmail.com
[3] *Artificial Intelligence & Data Science ,DMICE-600123*
Email: nandhuraj205@gmail.com
[4] *Artificial Intelligence & Data Science ,DMICE-600123*
Email:harishwaranpetchimuthu@gmail.com
[5] *Artificial Intelligence & Data Science ,DMICE-600123*
Email: personalaccdinesh@gmail.com

Abstract:
With the rapid advancement of artificial intelligence and video editing technologies, it has become increasingly easy to manipulate digital videos without leaving visible traces. This creates serious challenges in domains such as journalism, legal investigations, surveillance systems, and digital forensics, where video evidence must be trusted. Existing video verification approaches mainly rely on cryptographic signatures and blockchain storage to detect tampering and maintain an immutable record of video data. However, many current systems verify videos only at the file level and may not provide fine-grained detection of frame-level modifications. This paper proposes Verixa, a secure video proofing architecture designed to ensure the authenticity and integrity of digital videos from the moment of capture. In the proposed system, the recorded video is first divided into frames, and each frame is processed as pixel data to generate a cryptographic hash using the SHA-256 algorithm. These frame hashes are then organized into a Merkle tree, producing a single root hash that represents the entire video sequence. The root hash is digitally signed using the Elliptic Curve Digital Signature Algorithm (ECDSA) within secure hardware environments such as Trusted Platform Modules (TPM) or Trusted Execution Environments (TEE). The generated proof, along with metadata such as timestamp and device ID, is stored on a blockchain ledger, while the actual video is stored in cloud storage. During verification, the video is reprocessed to reconstruct the Merkle tree and validate the signature against the blockchain record. If the values match, the video is confirmed as authentic. The proposed approach

Keywords: Video Integrity Verification, Digital Video Authentication, SHA-256 Hashing, Merkle Tree, Elliptic Curve Digital Signature Algorithm (ECDSA),Trusted Platform, Trusted Execution Environment (TEE), Blockchain-based Verification

I. INTRODUCTION

Digital videos are widely used today in areas such as surveillance systems, journalism, legal investigations, and forensic analysis. Cameras installed in public spaces, mobile devices, and Internet-of-Things (IoT) systems continuously generate large volumes of video data that may later serve as important evidence. However, with the rapid advancement of video editing software and artificial intelligence technologies, manipulating video content has become easier than ever. Even small changes such as frame insertion, deletion, or pixel modification can alter the meaning of recorded events. Therefore, verifying the authenticity and integrity of digital videos has become an important research challenge. Several

cryptographic and blockchain-based approaches have been proposed to address this issue. For instance, Lawrence and

Shreelekshmi proposed a blockchain-based framework that uses elliptic curve digital signatures to ensure secure video integrity verification and tamper detection [1]. Similarly, blockchain-enabled forensic frameworks have been developed to verify video evidence collected from wireless IoT devices, ensuring that the captured data remains trustworthy throughout its lifecycle [2]. Other research has explored multimedia protection techniques such as perceptual hashing and watermarking integrated with blockchain technology to protect video copyright and forensic evidence [3]. In addition to multimedia protection methods, data provenance systems have been introduced to ensure the traceability and reliability of large IoT data streams. For example, blockchain-based provenance models have been proposed to manage and verify large-scale IoT data stored within distributed computing environments [4].

At the same time, the emergence of deepfake technologies has created new threats to digital media authenticity. Public datasets such as Celeb-DF have been developed to support research on detecting manipulated videos and evaluating deepfake detection algorithms [5]. Furthermore, research in video forensics has introduced techniques for detecting video manipulation and locating forged regions in video sequences. Frameworks such as FOCAL analyze inconsistencies in video coding artifacts to identify tampered regions [6]. Blockchain-based digital forensic architectures have also been proposed to enhance evidence reliability by combining cryptographic hashing with distributed ledgers [7]. Other studies have explored combining blockchain with watermarking, perceptual hashing, and digital signatures to create secure systems for verifying the authenticity of multimedia content [8]. Recent developments also include decentralized frameworks designed to protect video ownership and copyright using blockchain technology, enabling transparent tracking of multimedia content [9]. In addition, cryptographic methods continue to play a key role in protecting digital evidence and ensuring privacy within forensic investigations [10]. Surveys of blockchain-based video integrity solutions highlight the growing interest in using distributed ledgers to maintain trustworthy multimedia records [11]. Beyond integrity verification, researchers are also exploring blockchain-supported deepfake detection methods that integrate federated learning and deep neural networks to detect manipulated videos while preserving data privacy [12]. Hybrid systems combining blockchain with machine learning techniques have also been proposed to improve the accuracy and reliability of deepfake detection systems [13]. Moreover, the integration of IoT systems with blockchain technology has been studied across multiple domains, including supply chain management and secure data sharing, demonstrating the broader applicability of decentralized trust mechanisms [14].

Early work in this area also explored using blockchain to guarantee the integrity of videos captured by wireless devices, highlighting the potential of distributed ledgers for secure multimedia verification [15].

Despite these advancements, ensuring reliable and scalable verification of digital video content remains a challenging task. The increasing sophistication of media manipulation techniques demands more robust and efficient frameworks capable of providing trustworthy verification mechanisms.

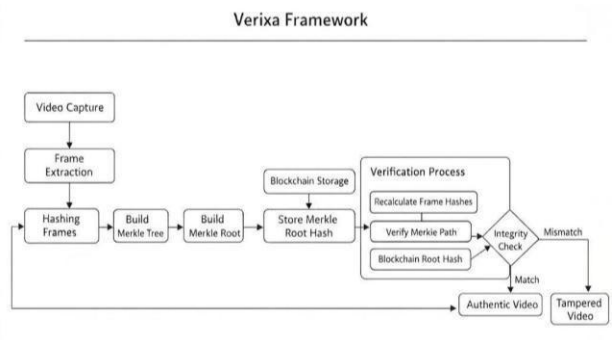
II. RELATED WORKS

Research on digital video authenticity has gained significant attention in recent years due to the growing risks associated with video manipulation and deepfake technologies. One of the earliest approaches to address this problem involved integrating cryptographic signatures with blockchain technology. Lawrence and Shreelekshmi introduced a blockchain-based video integrity verification system that uses elliptic curve digital signatures to ensure secure storage and validation of video data [1]. Their approach links signatures across video segments, making it possible to detect tampering even at a fine-grained level. Blockchain technology has also been applied to video forensics in IoT environments. Mercan et al. proposed a blockchain-based video forensic framework designed for wireless IoT devices, where video recordings are stored and verified using distributed ledger technology to maintain integrity and transparency [2]. Similarly, multimedia copyright protection mechanisms have been proposed that combine blockchain with perceptual hashing and watermarking to secure digital video content and prevent unauthorized modifications [3]. In large-scale IoT ecosystems, ensuring the reliability of generated data is another important challenge. Pajouh et al. developed a blockchain-based data provenance system that enables secure tracking and verification of IoT data within big data infrastructures such as Hadoop ecosystems [4]. While such approaches focus on data provenance, other studies concentrate on detecting manipulated video content. The Celeb-DF dataset, for example, provides a large-scale benchmark for evaluating deepfake detection algorithms and has become an important resource for video forensic research [5]. Several methods have also been proposed to detect video forgeries directly from video content. The FOCAL framework analyzes inconsistencies in video compression artifacts to localize forged regions within video sequences [6]. Other research has focused on improving digital forensic architectures by integrating blockchain with cryptographic hashing techniques to ensure secure and verifiable digital evidence management [7]. More recent work explores combining multiple security techniques for

multimedia authentication. Blake proposed a framework that integrates blockchain, perceptual hashing, digital signatures, and watermarking to strengthen media authentication mechanisms [8]. In addition, decentralized blockchain-based platforms have been developed to manage video ownership and copyright protection through transparent and immutable records [9]. Cryptographic security techniques also play a crucial role in digital forensic investigations. Studies have examined various cryptographic mechanisms that can enhance privacy and integrity protection in digital evidence systems [10]. Surveys of blockchain-based video integrity research further emphasize the potential of distributed ledger technology to improve trust in multimedia evidence [11]. With the increasing sophistication of deepfake technologies, researchers are exploring advanced detection mechanisms. Blockchain-based deepfake detection methods using federated learning and deep neural networks have been proposed to improve detection accuracy while maintaining data privacy [12]. Similarly, hybrid systems combining blockchain, machine learning, and distributed verification mechanisms have been introduced to strengthen deepfake detection frameworks [13]. Beyond video authentication, blockchain technology has also been widely studied in IoT environments to improve transparency, traceability, and trust in distributed systems [14]. Early studies demonstrated that blockchain could be used to ensure the integrity of video streams captured by wireless devices, highlighting its potential for secure multimedia verification systems [15].

III. PROPOSED SYSTEM

Although the proposed solution addresses digital video manipulation challenges, this research introduces a secure verification framework named Verixa. The primary objective of Verixa is to ensure the authenticity and integrity of digital video evidence through the application of cryptographic techniques and structured verification mechanisms. In the proposed system, video recordings generated from surveillance cameras or other recording devices undergo processing to create cryptographic fingerprints that uniquely represent the video content. The system initiates by extracting individual frames from the recorded video stream. Each frame contains pixel-level information that reflects the visual content of the video at a specific moment in time. To preserve the integrity of the video, a cryptographic hash function such as SHA-256 is applied to each extracted frame. The resulting hash values serve as unique digital fingerprints. Since even a minor change in the frame's pixel values will produce a completely different hash output, any modification to the video content can be readily detected. Since videos can contain thousands of individual frames, keeping separate hash values for each frame would create storage inefficiencies. To address this challenge, the system uses a Merkle Tree data structure to organize these hash values. This approach places frame hashes at the leaf positions, then systematically combines and hashes pairs of values until reaching a single root hash. This root hash serves as a condensed fingerprint representing the integrity of the complete video. The system stores the resulting Merkle root hash in a blockchain ledger to guarantee tamper-resistant preservation of integrity data. Additional information like timestamps and video identifiers accompanies the hash in storage. Blockchain technology delivers both immutability and transparency, making it impossible to modify stored records without detection. When verification takes place, the system calculates



fresh hashes from the video frames and rebuilds the Merkle tree structure. The system then compares this newly created root hash against the root hash previously recorded in the blockchain. Matching values confirm the video remains authentic and unaltered. When the values differ, the system detects that tampering has occurred. This method allows the Verixa framework to offer a dependable way to identify altered videos while keeping the system both scalable and computationally efficient. The system proves especially valuable for digital evidence applications, including surveillance monitoring, forensic analysis, and court cases where preserving video authenticity is essential.

Fig 1. System Architecture

The Verixa framework uses an architecture built to safely handle, store, and authenticate digital video evidence. Raw video data moves through several connected stages that convert it into cryptographically verifiable records. Video acquisition starts the process when surveillance cameras or recording equipment capture footage. A frame extraction module then processes this video by breaking it down into separate frames. Each frame captures the video at one moment in time and holds pixel-level data that supports integrity checks. After frame extraction, the system runs each frame through a cryptographic hashing function. This hashing converts frame data into a hash value of fixed length that uniquely identifies that specific

frame. Hash functions create an avalanche effect where any tiny modification to frame content produces an entirely different hash value, which makes this method highly effective for detecting tampering. The system then arranges these frame hashes using a Merkle Tree structure. This tree-like hierarchy combines pairs of frame hashes and hashes them again to create intermediate points. The process repeats until it produces one final root hash called the Merkle Root. This root hash works as a condensed summary of the complete video's integrity and enables quick verification of individual frames without needing to recalculate hashes for the whole video. A blockchain-based storage layer preserves the Merkle root hash to prevent any changes to the integrity information. Blockchain creates an unchangeable record system where each entry connects cryptographically to the one before it. This structure ensures that integrity data stays unmodifiable once recorded, and any tampering attempts become detectable. When verification begins, the system extracts frames again from the video being examined and recalculates their hash values. These new hashes rebuild the Merkle tree and create a fresh root hash. The system then compares this newly created root hash against the hash stored in the blockchain. Matching values confirm the video as authentic, while different values indicate tampering has occurred. By combining hashing techniques, Merkle trees, and blockchain storage, the Verixa architecture delivers a dependable and scalable approach to protecting digital video evidence integrity.

IV. FUTURE WORK

While the proposed Verixa framework offers a robust architecture for verifying digital video evidence integrity, several enhancements warrant exploration in future research. One potential extension involves integrating blockchain-based timestamping mechanisms to establish immutable public records of video integrity proofs. This approach would enhance the transparency and traceability of recorded media. Future research may also concentrate on developing optimized real-time implementations suitable for direct embedding into camera hardware or mobile devices. Integration of the Verixa framework with edge computing systems could facilitate secure hashing and verification at the point of video capture. An additional potential improvement encompasses the incorporation of privacy-preserving verification techniques, such as zero-knowledge proofs, which would allow specific video segments (including sensitive faces or locations) to remain concealed while preserving overall authenticity verification. Finally, comprehensive experimental evaluation utilizing real surveillance datasets could yield valuable insights into system performance, storage overhead, and verification speed under actual operational conditions.

V. RESULT AND DISCUSSION

The Verixa framework is designed to enhance the reliability and integrity verification of digital video evidence by integrating cryptographic hashing, hierarchical data structures, and secure hardware-based key protection. The system focuses on generating verifiable integrity proofs for recorded video while maintaining efficient verification even for large video datasets. Analysis of the architecture shows strong tamper-detection capabilities. Each frame of the recorded video is converted into a cryptographic hash using the SHA-256 algorithm. Since hash functions are highly sensitive to data changes, even a minor modification to a single pixel produces a completely different hash value. This property enables the system to detect even subtle alterations in video data. To improve scalability and efficiency, the generated frame hashes are organized using a Merkle tree structure. This hierarchical approach allows the system to verify only the required branch of the tree instead of recomputing hashes for the entire video file, significantly reducing verification time for large recordings. Additionally, secure hardware modules such as TPM or TEE protect the private cryptographic keys used for digital signatures, ensuring that video authenticity can be traced back to the original recording device. Overall, the Verixa framework provides a reliable and scalable method for detecting video tampering in surveillance and forensic applications.

VI. CONCLUSION

The authenticity and integrity of digital video evidence have emerged as critical challenges in contemporary surveillance and forensic investigations. Given the rapid advancement of video editing technologies and artificial intelligence-based media manipulation techniques, ensuring the reliability of digital recordings has gained increasing importance. This paper presents Verixa, a secure video integrity verification framework developed to protect digital evidence from tampering and unauthorized modification. The proposed system employs cryptographic hashing to generate unique digital fingerprints for video frames and organizes these hashes through a Merkle-tree structure to facilitate efficient integrity verification. Additionally, secure hardware modules such as Trusted Platform Modules (TPM) or Trusted Execution Environments (TEE) are utilized to safeguard private cryptographic keys and enable trusted digital signatures. The proposed architecture enhances the reliability of video authentication by providing rapid verification, scalable data handling, and robust tamper detection capabilities. The integration of cryptographic security techniques with structured data verification offers a promising solution for ensuring the authenticity and reliability of digital video recordings.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to all those who supported the development of this work. We thank our mentors and faculty members for their valuable guidance and encouragement throughout the project. We also acknowledge the support of our institution for providing the necessary resources and facilities. Finally, we appreciate the contributions of our peers and reviewers for their helpful feedback.

REFERENCES

[1] L. Lawrence and S. R. Shreelekshmi, "VECDSigL: Video integrity verification using elliptic curve digital signature links," Software Impacts, vol. 15, p. 100474, 2023.

[2] S. Mercan, M. Cebe, R. A. Aygun, K. Akkaya, and E. Toussaint, "Blockchain-based video forensics and integrity verification framework for wireless Internet-of-Things devices," Marquette University, 2021.

[3] S. M. Darwish, M. M. Abu-Deif, and S. M. Elkafas, "Blockchain for video watermarking: An enhanced copyright protection approach for video forensics based on perceptual hash function," PLOS ONE, 2024.

[4] H. H. Pajouh, M. A. Rashid, F. Alam, and S. Demidenko, "IoT big data provenance scheme using blockchain on Hadoop ecosystem," Journal of Big Data, 2021.

[5] Y. Li, X. Yang, P. Sun, H. Qi, and S. Lyu, "Celeb-DF: A large-scale challenging dataset for deepfake forensics," Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR), 2020.

[6] S. Verdoliva, P. Bestagini, M. Tagliasacchi, and S. Tubaro, "FOCAL: A forgery localization framework based on video coding self-consistency," arXiv preprint arXiv:2008.10454, 2020.

[7] W. A. Mahrous, M. Farouk, and S. M. Darwish, "An enhanced blockchain-based IoT digital forensics architecture using fuzzy hash," IEEE Access, vol. 9, pp. 151327–151342, 2021.

[8] S. Blake, "Embedded blockchains: A synthesis of blockchains, spread spectrum watermarking, perceptual hashing and digital signatures," arXiv preprint, 2024.

[9] S. L. Madapati and N. H. Pradhan, "Decentralizing video copyright protection: A novel blockchain-enabled framework with performance evaluation," Frontiers in Artificial Intelligence, 2025.

[10] T. B. Ogunseyi and O. M. Adeyodo, "Cryptographic techniques for data privacy in digital forensics," IEEE Access, vol. 11, 2023.

[11] J. Ceron, C. Tinupucla, and P. Shiguihara, "A survey of blockchain for video integrity," Engineering Proceedings, vol. 42, 2023.

[12] A. Heidari, N. J. Navimipour, H. Dag, S. Talebi, and M. Unal, "A novel blockchain-based deepfake detection method using federated and deep learning models," Cognitive Computation, 2024.

[13] A. Prathap and B. M. Beena, "Blockchain based deep fake detection and verification," Journal of Electrical Systems, 2025.

[14] A. Rejeb, J. G. Keogh, and H. Treiblmaier, "Leveraging the Internet of Things and blockchain technology in supply chain management," Future Internet, vol. 11, no. 7, 2019.

[15] D. Danko, S. Mercan, M. Cebe, and K. Akkaya, "Assuring the integrity of videos from wireless-based IoT devices using blockchain," Proc. IEEE MASS Workshops,2019