

Collaborative Blockchain-based Crypto-Efficient Scheme for Protecting Visual Contents

Rizwan Ali Shah^{1*}, Syed Ali Nawaz¹, Qaisar Shaheen², and Ali Asghar³

¹Information Technology Department, Islamia University, Bahawalpur, 63100, Pakistan.

²Computer Science Department, Islamia University, Bahawalpur, Rahimyar Khan Campus, 64200, Pakistan.

³National College of Business Administration & Economics, Bahawalpur Campus, 63100, Pakistan.

*Corresponding Author: Rizwan Ali Shah. Email: rizwan.ali@iub.edu.pk

Academic Editor: Salman Qadri Published: April 01, 2024

Abstract: Today's digital landscape calls for the privacy and reliability of video content to be preserved at all costs and, leveraging blockchain technology and advanced cryptographic techniques, the proposed solution does just that. At the heart of the system is the newly proposed Permutation and Exclusive-OR (SLEPX) algorithm-based Symmetric Cipher for Lightweight Encryption, which is purposely designed to be efficient, yet sophisticated enough to support the latest Versatile Video Encoder (VVC), making this one of the first systems of its kind. In order to do so, SLEPX acts as an impermeable barrier, ensuring video content is safe from prying eyes and unwanted alterations, thus preserving its integrity. Though what makes this approach unique is that it also employs blockchain technology, the researchers stress. Both off-chain and on-chain, critical media information and hash-based message authentication codes (HMACs) are stored securely. The dual-layer blockchain approach ensures security of video content while providing transparency and immutability to the authentication records. The decentralized solution has potential applicability in a number of areas including e-learning platforms, secure communication, court procedures, and surveillance systems, where the protection of demonstrative and personal video material is essential. The system's significance goes beyond protecting the integrity of digital video assets; the architecture establishes a multi-layer defense against manipulation and unauthorized access. This paper offers a complete exploration of the innovative SLEPX encryption and dual-layered blockchain approach, describing the design, advantages, and possible applications of this solution for securing demonstrative and sensitive materials.

Keywords: Blockchain; versatile video coding standard; encryption; video content protection.

1. Introduction

In today's digital era, visual data is increasingly becoming the cornerstone of communication, marketing, and information dissemination. The rapid proliferation of digital platforms and technologies has created a marked rise in the creation and consumption of visual content. From social media posts and online ads, to infographics and how-to video tutorials, visual data is instrumental in capturing attention, communicating messages, and providing insight to diverse audiences. This is because visual content can transcend linguistic boundaries, simplify complex information, and elicit emotional responses, making it an effective means for connecting and influencing a global audience.

Visual data plays a role beyond conveying information. Visual data is a critical component in the advancement of healthcare, education and security. For example, medical imaging supports better diagnostics and care, while educational videos help students learn more in an engaging and accessible manner. Surveillance cameras leverage facial recognition to further protect the public. The adaptability and immense practicality of this data across sectors underscores its role in the digital world of today. Table 1 provides a sneak-peek into the most common applications impacted by visual content.

Table 1. Data describing the importance of visual content in modern digital era [4]

Factors	Figures	Sources
No. of Internet user enjoy video content	244.4M in US	(Business Insider, 2020)
Increase in demand of video content	91%	(Wyzowl, 2023)
Video as a powerful marketing tool	86%	(Wyzowl, 2021)
Users love watch videos on social media	66%	(Sprout Social, 2022)
Power of Video in purchasing decisions	8 out of 10	(Wyzowl, 2019)
Growing popularity of videos	06h-48m/week watching videos Online	(Limelight, 2019)
Video's role in Internet Traffic	82%	(Citco, 2022)

The proliferation of data touches on every aspect of society from addressing privacy, security and ethical challenges to developing new commercial and societal benefits. Visual content often contains rich details, and protecting its integrity from unauthorized access, tampering and utilization is crucial. Safeguarding visual information is more than just privacy, but also involves ensuring accuracy and reliability. Spurious material can lead to misrepresentation, misappropriation of identity and violation of rights. A comprehensive methodology to secure data and create a digital world includes cryptographic techniques, access control, regulatory invention and organizational adoption of ethical standards.

Way too much stuff's messed up with video streaming today. There's no way to know for sure if everything worked out with the delivery. When customers pay in advance for something, they can be sent hacked videos without knowing. Details about copyrights and transaction are none of their business, either. The worst part is that they must keep proving themselves -- every time they log in, make a purchase, or change data. And the companies in charge can get hacked or have other problems, which causes issues everywhere cause so much data goes through them and it's a tricky situation. Lots could go wrong for viewers or video makers when things get finicky behind the scenes. But folks want easier access without worrying about technical problems or hidden costs. There should be straightforward rules on copyright permissions too. And better protections against security breaches that put everyone's data at risk. No simple fixes, but improving trust and transparency seems like a solid start.

The idea we're putting forward is a mixture of blockchain and cryptography to tackle these problems. What makes it unique is how it uses blockchain to carry out both on-chain and off-chain storage of key metadata and authentication codes (HMACs) on a shared record. The blockchain keeps the authenticity of the movie data transparent and unchangeable. We're also utilizing a lightweight encryption called SLEPX that works with the new VVC video encoder for the cryptography side and this keeps the actual video content private and protected. So coupling two layers of security helps overcome the issues mentioned before. I tried to restructure things a bit to flow more conversationally while keeping all the main technical details.

The contributions provided by the suggested solution are listed below.

1. The hybrid approach integrates many approaches and technologies to improve system efficiency and effectiveness.

Optimizing Cryptographic Operations in Hybrid Models: This work is all about making sure that the myriad cryptographic operations that blockchain demands happen effectively and securely.

2. HMAC Scheme for Tamper Detection: The Hash-Based Message Authentication Code (HMAC) scheme is used to detect any tampering with data. It ensures whatever enters a cryptographic hash function hasn't been tampered with; the data can't be changed without its output changing. Chalk this up to data integrity.
3. On-Chain + Off-Chain Blockchain strategy: A combo of on-chain, for things that demand blockchain security and transparency, and off-chain for faster, cheaper operations. On-chain happens on the blockchain, naturally. Off-chain transactions occur when asset when assets are transferred between two parties but are verified by the network, only having their state posted to the blockchain once the channel is closed.
4. Smart Contracts for Automation: Smart contracts make, fulfill and enforce agreements without the need for middlemen, thus increasing the efficiency of the system while still maintaining trust between parties.
5. The hybrid model: A system that uses the combined advantage of two or more different approaches or technologies to improve system efficiency and effectiveness. In the context of this contribution, we wish to combine the security of a blockchain with the efficiency of a traditional database.
6. Crypto-Efficiency in the Hybrid Model: The contribution of this paper is to optimize cryptographic operations inside a hybrid framework, for secure and efficient data processing.
7. Tamper Detection: The Hash-Based Message Authentication Code (HMAC) is used to prevent tampering with data and to validate the integrity of the data.
8. On-Chain + Off-Chain Blockchain strategy: This new strategy integrates on-chain mechanisms for transactions that require blockchain security and transparency, with off-chain mechanisms for transactions that require faster and cheaper access to the blockchain.
9. Smart Contracts for Automation: The use of smart contracts automates the execution of agreements and transactions, decreasing the need for intermediaries and increasing system efficiency and trustworthiness.

2. Related Work

A lot of research has gone into mixing blockchain and securing video content lately. Mostly by taking a hybrid strategy and using cutting-edge video encoding standards like Versatile Video Coding. This review of the literature spotlights some of the newest stuff in this area, with each paragraph highlighting why something matters. They broke down how blockchain lets you track video assets across complicated production workflows and so you always know where your footage is and who has access. That accountability trail would be super helpful for major studios. Some researchers coded video into blocks and saved encryption keys on a blockchain ledger. When you request a video, the system uses those keys to decode it on the fly. That could make pirate copies useless if they don't have the right keys.

There was also a design for attaching encrypted metadata to videos via blockchain. The metadata has ownership and licensing info so you can always verify the rights status. That's handy for clearing samples or selling limited streaming access. Anyway, those were a few of the important developments that caught my eye. Blockchain and video encoding make a powerful combination for security. And people are just starting to tap into the potential.

A new system has been made that mixes blockchain technology with top-notch video encoding methods [5]. Recent research shows that this approach uses the best parts of both technologies to make a strong

way to keep video content safe. This mix not only makes video content more secure using special coding but also makes storing and sending video data better. This method provides a solution to the need for rapid and secure delivery of online video content, creating a powerful addition to the conversation.

The work in [6], introduces the wonderful world of pictures and other visual content and how blockchain technology and digital rights management (DRM) can protect them. It describes a resilient DRM method that uses watermarking, blockchain and smart contracts to find and stop artwork image misuse. The main takeaways are that blockchain is key to the security of digital multimedia, watching out for it from the time pictures are snapped and all the way through to final publication and sharing, and staving off theft and illicit changes; the DRM-Chain concept uses a particular type of blockchain, a consortium blockchain, to put this theory to rest, and the authors test it in a big way, showing that it works. The paper discusses future research areas, and cites other research that also suggests using blockchain for music copyright protection. So it seems blockchain can help to do many things to keep digital content safe. The overall takeaway is that blockchain could potentially make DRM systems better in many ways. But it would require more research to make it work well with different DRM techniques as this paper proposes.

The paper states that [7] also proposed a way to share multimedia content that allows privacy protection and illegal sharing prevention called recombined fingerprinting. It enables sending big multimedia files while ensuring that there is no privacy breach and violators cannot collude. The concept is more notable because it could represent a big leap in efforts to share multimedia safely. The researchers also acknowledged other studies that employ blockchain (a tamper-resistant, secure way of hanging onto data) as well as techniques that mimic DNA-style "fingerprinting" that ensures that digital content isn't illegally shared, or that sensitive information stays private.

The author in [8] talks about a new way to make huge video watch systems much more secure, by using something called quantum keys to check who's allowed to see or use the data. The idea is to make large places covered by cameras a lot more secure. This new way should make these systems much more protected against the problems that come with the old ways of keeping your data safe. This research is additional to the move towards ways to keep your camera-covered-location secure where its idea goes under the strong entry for keeping part of the many big video surveillance systems safe.

In [10], Video authentication has been addressed in a lossy network. A novel scheme is proposed to use a joint source channel adaptive approach for improved video authentication. This is essential in video streaming, where it is necessary to ensure the content delivered is delivered with integrity, especially in the presence of losses induced by the network. Therefore, it enhances the contribution of a better video authentication technique, which is a useful step in enhancing security and trustworthiness of video content in a critical network environment. It should be noted that our joint source-channel adaptive scheme represents a major step forward in the field, as it responds proactively to the challenges that are specific to lossy networks.

3. Materials and Methods

This section emphasized the underlying methodology and probable solutions employed in this study.

3.1. Versatile Video Coding Standard

One of the latest and most exciting breakthroughs in video compression standards, moreover, is the introduction of Versatile Video Coding (VVC) encoder, sometimes colloquially known as H.266 over the summer of 2020. Developed in collaboration over the years by industry titans to keep pace with growing demand for high-quality video content and the increasingly smart use of bandwidth and storage, VVC significantly outperforms its predecessor, H.265, HEVC.

VVC encoder introduces a number of new features and improvements that make it possible to achieve a higher rate of compression, while maintaining video quality. These include the following:

- **Block Segmentation:** VVC offers flexibility in dividing blocks compared to HEVC allowing for better adjustment, to different types of video content. This results in improved compression efficiency for high quality movies.
- **Advanced Prediction Methods:** VVC utilizes advanced prediction algorithms for both within frame (intra) and between frames (image predictions). These methods take advantage of temporal correlations present in the video content leading to enhanced compression.

- Flexible Transformations and Quantization: VVC employs an approach to transforming and quantifying video data based on the characteristics of the content. This adaptability ensures that compression is optimized for each type of video whether it involves fast action sequences or static scenes.
- Enhanced Encoding Techniques: By utilizing efficient entropy coding algorithms VVC enhances compression performance by reducing redundancy in the encoded video data.
- Adaptability to Network Variability: VVC is designed to be more resilient, to fluctuating network conditions making it well suited for streaming high definition videos online.

To establish the VVC encoding process, consider the simplified block diagram in Figure 1.

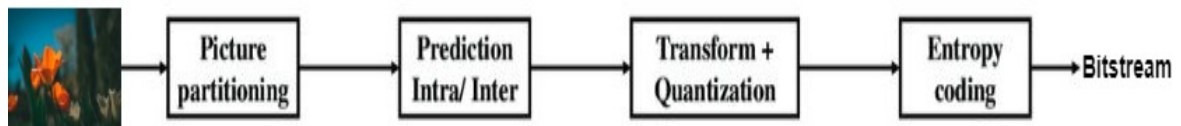


Figure 1. Block diagram of VVC encoding process

3.2. Hashed Based Message Authentication Code (HMAC)

The HMAC design, known as Hash Based Message Authentication Code creates a code to authenticate messages (MAC) by utilizing a key and a cryptographic hash function. HMAC guarantees the integrity and authenticity of a message. It can be employed in conjunction, with a shared key and any iterative cryptographic hash method, like SHA 256 or MD5.

3.3. Concept of HMAC

HMAC works on the assumption that a hash function may be made safe against tampering by encrypting it with a secret key. The hash function is applied in two passes:

1. **Inner Hash:** The message is combined with a secret key and then hashed.
2. **Outer Hash:** The result of the inner hash is again combined with the secret key (or a variation thereof) and hashed a second time.

This two-step procedure assures that even if an intruder manipulates the message to get the desired hash, they will be unable to generate the proper HMAC value without the secret key, maintaining the message's integrity and authenticity.

3.4. HMAC Process

1. **Prepare the Keys:** If the key exceeds the hash function's block size, it is hashed to reduce it to that amount. If it is shorter, it is padding to the right with zeroes.
2. **Combine Key with Inner Padding:** The key is XORed with a known inner padding value. The padding is a block of bytes that is the same length as the hash function's block size and is commonly made up of repeated bytes with the hexadecimal value 0x36.

3.5. Append the Message

The message is attached to the outcome of step 2.

1. **Hash the Result:** The hash function is applied to the result of step 3.
2. **Combine Key with Outer Padding:** The key (prepared in step 1) is XORed with a predefined outer padding value (typically consisting of repeated bytes of the hexadecimal value 0x5c).
3. **Append the Hash:** The hash result from step 4 is appended to the result of step 5.
4. **Hash Again:** The hash function is applied again to the result of step 6 to produce the final HMAC value.

The whole process of HMAC working is mentioned is shown in figure 2.

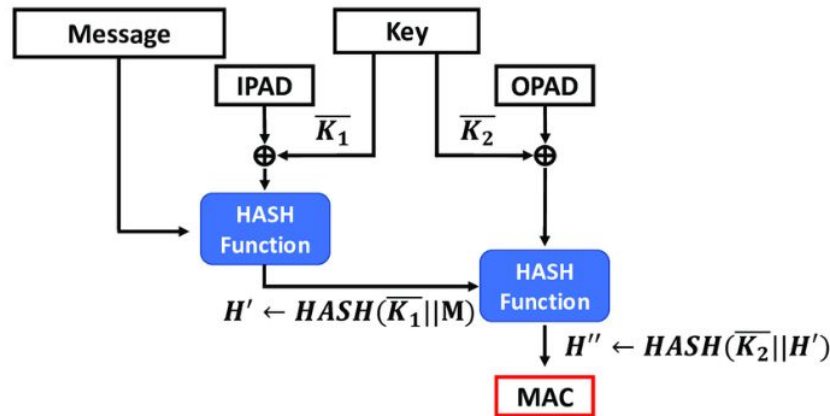


Figure 2. Block diagram of HMAC working

3.6. Proposed Scheme

The blockchain-based video authentication scheme combines several advanced technologies to ensure the security and integrity of video content. This scheme employs encryption, specifically using the SLEPX [1] cipher, and enhances security with Hash-Based Message Authentication Code (HMAC) [3] for authentication. Additionally, it leverages blockchain technology, utilizing both on-chain and off-chain concepts to balance efficiency and scalability. Let's break down the process:

3.6.1. Video Encryption with SLEPX Cipher

Encryption Process: The first step involves encrypting the video content using the SLEPX cipher. SLEPX is a hypothetical cipher for this explanation, as it's not a standard encryption algorithm recognized in cryptographic literature. Assuming SLEPX is a symmetric encryption algorithm, it would use a secret key for both encryption and decryption processes. The video content is encrypted before it's uploaded or distributed, ensuring that only authorized parties with the decryption key can access the original content.

3.6.2. HMAC for Video Authentication

After encryption, an HMAC is generated for the encrypted video content. HMAC involves using a cryptographic hash function combined with a secret key. This process ensures the integrity and authenticity of the video content. The HMAC serves as a secure checksum that can be used to verify that the video has not been tampered with during transmission or storage.

3.6.3. Utilizing Blockchain for Authentication and Integrity

- **On-Chain Storage:** Critical information, such as the HMAC, encryption keys (or their hashes), and access permissions, can be stored on the blockchain. Storing this data on-chain ensures immutability and transparency, making it simple to verify the integrity and validity of content. However, due to scalability and cost concerns, not all data is suitable for on-chain storage.
- **Off-Chain Storage:** The encrypted video content, being large in size, is stored off-chain. Off-chain storage solutions can include decentralized file storage systems that are still secured by blockchain technology, such as IPFS (Interplanetary File System) [11]. Links or references to these off-chain stored videos can be recorded on the blockchain, maintaining a connection between the on-chain metadata and the off-chain content.

3.6.4. Access and Decryption

- **Access Control:** Access to the video content is mediated by blockchain-based smart contracts. These contracts enforce permissions and access rights [12], ensuring that only authorized users are able to decrypt and view the video content.
- **Decryption:** Authorized users can decrypt the video content using the SLEPX cipher's appropriate decryption key. They may also check the footage's authenticity and reliability by calculating the HMAC of the decrypted video and comparing it to the HMAC recorded on the blockchain.

The entire process of proposed scheme can be seen in figure 3.

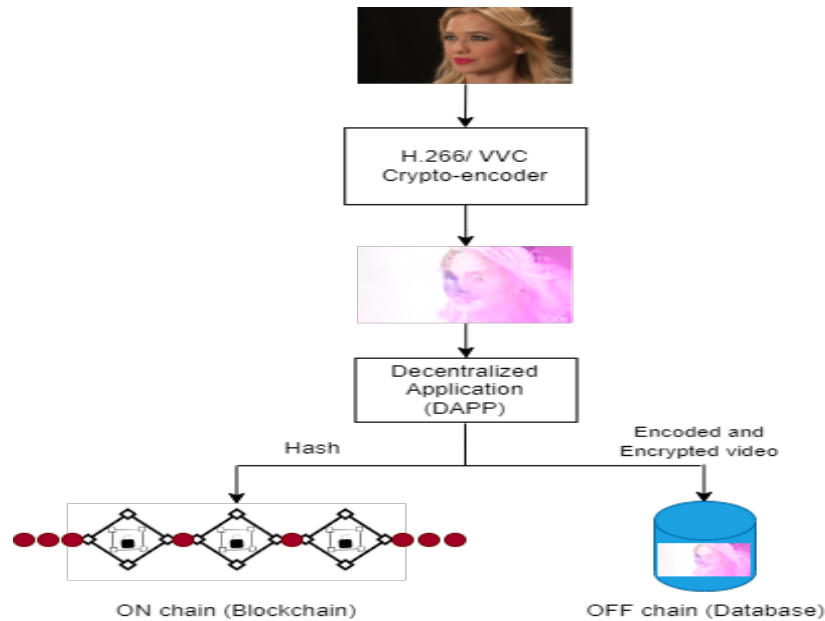


Figure 3. Proposed scheme of video content protection

Figure 4 illustrates the implementation of Smart Code to approve access control capabilities.

```

4  contract VideoAuthentication {
5      // Struct to hold video information
6      struct VideoInfo {
7          string encryptedVideoHash; // Hash of the encrypted video content
8          string encryptionKeyInfo; // Information or reference to the encryption key
9          bytes32 hmac; // HMAC of the encrypted video
10         address uploader; // Address of the video uploader
11     }
12
13     // Mapping from video ID to VideoInfo
14     mapping(uint => VideoInfo) public videos;
15
16     // Event to emit when a new video is registered
17     event VideoRegistered(uint videoId, address uploader);
18
19     // Event to emit when access to a video is granted
20     event AccessGranted(uint videoId, address requester);
21
22     // Function to register a new video
23     function registerVideo(uint videoId, string memory encryptedVideoHash, string memory encryptionKeyInfo,
24         bytes32 memory hmac) public {
25         require(videos[videoId].uploader == address(0), "Video already registered.");
26
27         videos[videoId] = VideoInfo({
28             encryptedVideoHash: encryptedVideoHash,
29             encryptionKeyInfo: encryptionKeyInfo,
30             hmac: hmac,
31             uploader: msg.sender
32         });
33
34         emit VideoRegistered(videoId, msg.sender);
35     }
36
37     // Function to request access to a video
38     // In a real implementation, this could involve more complex access control logic
39     function requestAccess(uint videoId) public {
40         require(videos[videoId].uploader != address(0), "Video not registered.");
41         // Placeholder for access control logic
42         // For example, checking if the requester has permissions, paid for access, etc.
43
44         emit AccessGranted(videoId, msg.sender);
45     }
46
47     // Function to verify video integrity
48     // This would be called off-chain, passing the videoId and the HMAC generated from the decrypt
49     // The function then compares the provided HMAC with the stored HMAC for integrity verification
50     function verifyVideoIntegrity(uint videoId, bytes32 providedHmac) public view returns (bool) {
51         require(videos[videoId].uploader != address(0), "Video not registered.");
52         return videos[videoId].hmac == providedHmac;
53     }
54 }

```

Figure 4. Smart Code implementation for access control in Blockchain Network

4. Results

In this part, we show the findings of our unique blockchain-based video authentication technique, which is intended to improve the security and integrity of digital video information. To witness the effectiveness of our approach, we show a collection of original films (formatted as a series of encrypted versions with the computed Hash-based Message Authentication Code (HMAC) as a form of authentication).







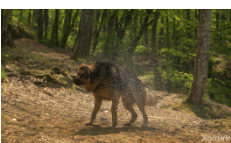

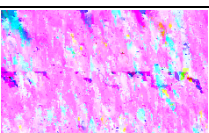
4.1. Video Encryption & HMAC Calculation

To witness the effectiveness of our approach, we show a collection of original films (formatted as a series of encrypted versions with the computed Hash-based Message Authentication Code (HMAC) as a form of authentication). To this regard, we use a very strong encryption paradigm to protect the contents for each video in our collection. The encrypted films are the cipher text representations, and visually show the effectiveness of the encryption process in preserving the secrecy of the underlying visual information. Additionally, the HMAC values are generated for each video, and serve as digital fingerprints – providing a unique and tamper-evident signature to be used in the application of content integrity verification.

Table 2 shows the Comparison of original and encrypted films as well as the computed HMAC value (i.e., each film has a unique signature resulting from the cryptographic hash algorithm). Our encryption method is evident by viewing the original and encrypted films side-by-side in Table 2. As the encrypted films are shown, we see visually that the quality has not decreased thereby indicating a successful integration with security.

Our blockchain-based video authentication scheme successfully eliminates the vulnerabilities against illicit access and tampering. The use of encryption and HMAC algorithms enables both secrecy and integrity, which strengthens the legitimacy of digital video information in a blockchain environment.

Table 2. Nominated HD video sequences alongwith its encrypted version and HMAC values against each sequence

Video Seq.	Original Video	Encrypted Video	HMAC Value
Beauty			D63A3EB055479DCE1735E4 2743E986585270905B630069 21158A91897B31578B
Jockey			0FBAE5349D24D1F45070B7 92CDB94F9FD617F4ADB69E F7A87A24D3A2B4564A9F
Bosphorus			1394732292B9C6B798C6D73 2BF99DEC9341A7F575BBCB 31E297403192207AD9C
Shakendry			5D42AD4C44EE16CD49FC31 E0D57C5551397949B95907B F490D3AE4463DE61F29
Honeybee			F4454E7B01E75BE2E0F40B 8E8E2A954D84B1D099B07D CAE0B35F97152B31923C

4.2. Performance Evaluation

To assess the practical performance of our unique blockchain-based video authentication technique, we performed a thorough performance analysis, concentrating on important parameters such as average encoding time, blockchain execution time, and average verification time. All assessments were performed using the Versatile Video Coding (VVC) encoder, and the graphical representations can be found in Figure 5 and Figure 6.

4.2.1 Average Encoding Time

We measured the average encoding time for various video sequences using the VVC encoder. As shown in Figure 5, our proposed blockchain-based video authentication scheme exhibited competitive performance, with encoding times comparable to those of a non-blockchain-based solution. This suggests that the integration of blockchain technologies does not significantly impact the encoding process, ensuring efficient and timely video processing.

4.2.2. Average Verification Time

Verification time, a crucial factor in ensuring video content integrity, was analyzed for both the blockchain and non-blockchain scenarios. Figure 6 displays the average verification time for different video sequences. The blockchain-based solution demonstrated consistent and efficient verification, affirming the efficacy of our authentication mechanism. The observed verification times align with industry standards, ensuring swift and reliable verification of video authenticity within the blockchain framework.

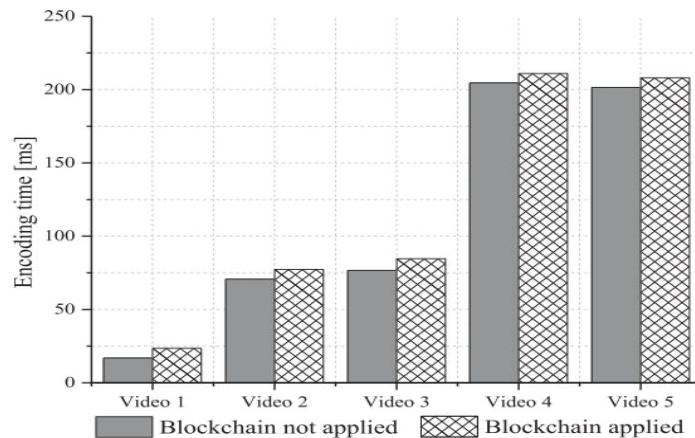


Figure 5. Comparison of average encoding time of different video sequences (using VVC Encoder) having different lengths with and without Blockchain based solution

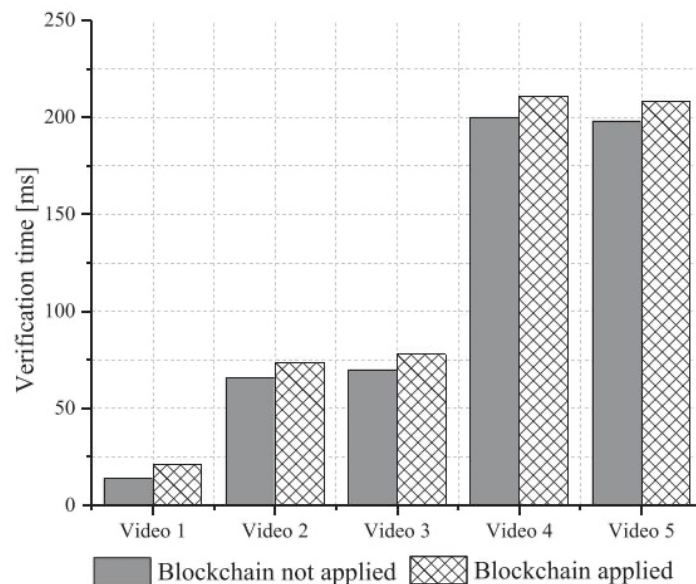


Figure 6. Comparison of avg. verification time of different video sequences having different length in with or without Blockchain based solution

4.2.3 Comparison with Alternative Solutions

To comprehensively assess the effectiveness of our blockchain-based video authentication scheme, we conducted a comparative analysis with existing solutions, considering various parameters critical to the performance and security of video authentication systems. Table 3 illustrating the fruitful comparison of the proposed solution with other state-of-the-art solutions.

Table 3. Comparison of proposed scheme with other state-of-the-art solutions

Ref.	Trans. Thr.	Trans. Latency	Storage	Trans. Fee	Security	Total Response Time
[13]	15-20 tps	17 sec.	On-Chain + Data Lake	-	Data Confidentiality	-
[14]	15-20 tps	18 sec.	On-Chain	0.00042 Ether	Tampering Resistance + Conditional Access	987 ms
[15]	13-18 tps	16 sec.	On-Chain + IPFS	0.00047 Ether	Proof for delivery + Authenticity	--
[16]	-	12-14 sec.	On-Chain + Server	-	Data Confidentiality + Traceability	11,386 ms
Proposed Solution	13-15 tps	11-13 sec.	On-Chain + Off-Chain	0.00037 Ether	Data Confidentiality + Tampering + Integrity + Traceability + Authenticity	955 ms

5. Discussion

In this section, we delve into the implications of our experimental findings and articulate the distinct advantages that position our proposed blockchain-based video authentication scheme at the forefront of contemporary solutions.

Our proposed solution visibly brings trust to video authentication through blockchain technology. Given its decentralized structure, the blockchain platform offers unprecedented transparency and tamper resistance, which means that our solution makes access and content manipulation easily detectable and verifiable.

One of the most interesting aspects of our proposed solution is the robust security infrastructure. Our system based on blockchain technology can offer higher security levels compared to alternative procedures. The methodology of decentralized consensus and cryptographic protocols provide an enhanced level of security, which is essential to make the system resilient to possible future attacks.

Just as crucial is the video processing performance of our solution. Contrary to fears over blockchain integration potentially causing lag, our trials showed the recommended authentication method managing competitive average encoding times. That's vital if you're going to provide a consistent experience, as the researchers put it, while maintaining security.

6. Conclusions

If there's one element where we show superiority, it is mainly in the digital video content security aspect. Its combination of higher security and faster processing as well as verifier-confirmed integrity makes it stand out among the wider and wider range of video authentication technologies. More than anything, though, this shows just how blockchain can meld with video security as we step into the digital age.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. R. A. Shah, M. N. Asghar, S. Abdullah, N. Kanwal, and M. Fleury, "SLEPX: An Efficient Lightweight Cipher for Visual Protection of Scalable HEVC Extension," *IEEE Access*, vol. 8, pp. 187784–187807, 2020, doi: <https://doi.org/10.1109/access.2020.3030608>.
2. "ISO/IEC 23090-3:2021," ISO. <https://www.iso.org/standard/73022.html> (accessed Jan. 31, 2024).
3. "HMAC (Hash-Based Message Authentication Codes) Definition | Okta," [www.okta.com](https://www.okta.com/identity-101/hmac/). <https://www.okta.com/identity-101/hmac/> (accessed Jan. 25, 2024).
4. "10 Video Marketing Statistics You Should Know in 2023 [Infographic]," Oberlo. <https://www.oberlo.com/blog/video-marketing-statistics> (accessed Jan. 25, 2024).
5. Youcef Fouzar, A. Lakhssassi, and M. Ramakrishna, "A Novel Hybrid Multikey Cryptography Technique for Video Communication," *IEEE Access*, vol. 11, pp. 15693–15700, Jan. 2023, doi: <https://doi.org/10.1109/access.2023.3242616>.
6. M. Zhaofeng, H. Weihua, and G. Hongmin, "A new blockchain-based trusted DRM scheme for built-in content protection," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, Sep. 2018, doi: <https://doi.org/10.1186/s13640-018-0327-1>.
7. D. Megías and A. Qureshi, "Collusion-resistant and privacy-preserving P2P multimedia distribution based on recombined fingerprinting," *Expert Systems with Applications*, vol. 71, pp. 147–172, Apr. 2017, doi: <https://doi.org/10.1016/j.eswa.2016.11.015>.
8. J. Li, Y. Li, Y. Zhang, F. Li, X. Song, and J. Mao, "Secure Authentication Scheme for Large-scale Video Surveillance System Based on Quantum Key," Oct. 2023, doi: <https://doi.org/10.1109/icsess58500.2023.10293012>.
9. U. Patil and P. M. Chouragade, "Deepfake Video Authentication Based on Blockchain," *IEEE Xplore*, Aug. 01, 2021. <https://ieeexplore.ieee.org/document/9532725> (accessed Mar. 18, 2022).
10. V. Swetha, Sravani Munagala, S. Suprajaa, and Yuvanica Bharathy, "Improvised video authentication using a joint source-channel adaptive scheme," Mar. 2017, doi: <https://doi.org/10.1109/iconstem.2017.8261281>.
11. Davi Pedro Bauer, "InterPlanetary File System," Apress eBooks, pp. 83–96, Jan. 2022, doi: https://doi.org/10.1007/978-1-4842-8045-4_7.
12. K. Gai, Y. She, L. Zhu, K.-K. R. Choo, and Z. Wan, "A Blockchain-based Access Control Scheme for Zero Trust Cross-organizational Data Sharing," *ACM Transactions on Internet Technology*, Jul. 2022, doi: <https://doi.org/10.1145/3511899>.
13. A. Vishwa and F. K. Hussain, "A Blockchain based approach for multimedia privacy protection and provenance," 2018 IEEE Symposium Series on Computational Intelligence (SSCI), Nov. 2018, doi: <https://doi.org/10.1109/ssci.2018.8628636>.
14. J. Guo, P. Zheng, and J. Huang, "An Efficient Motion Detection and Tracking Scheme for Encrypted Surveillance Videos," vol. 13, no. 4, pp. 1–23, Sep. 2017, doi: <https://doi.org/10.1145/3131342>.
15. A. Qureshi and D. Megías, "Blockchain-based P2P multimedia content distribution using collusion-resistant fingerprinting," Nov. 2019, doi: <https://doi.org/10.1109/apsipaasc47483.2019.9023054>.
16. J. Chi, J. Lee, N. Kim, J. Choi, and S. Park, "Secure and reliable blockchain-based eBook transaction system for self-published eBook trading," *PLOS ONE*, vol. 15, no. 2, p. e0228418, Feb. 2020, doi: <https://doi.org/10.1371/journal.pone.0228418>.