Multimedia Forensics: Preserving Video Integrity with Blockchain

Sahilkumar K. Ahir
Applied Computer Science
University of Winnipeg
Winnipeg, Canada
ahir-s@webmail.uwinnipeg.ca

Oluwasola Mary Adedayo
Applied Computer Science
University of Winnipeg
Winnipeg, Canada
m.adedayo@uwinnipeg.ca

Abstract — **This paper addresses some of the challenges of video forgery detection in multimedia forensics. It presents a solution that enhances video verification by utilizing the non-alterable features of blockchain technology and video hashing algorithms. The proposed approach is applicable in different application areas and can be used to increase video credibility, identify manipulations, and improve the storage process of tracking changes to video data. The paper describes our experiments and results of the proposed solution for video integrity preservation and verification, providing an alternative way to the quality assurance and security of video content in different industries.**

Keywords—multimedia forensics, video forgery detection, digital forensics, blockchain, hashing.

I. Introduction

Video analysis and multimedia forensics play an integral role in the evolving environment of digital forensics and computer security. Video content abounds in many media platforms, and the ease of modifying video content with many existing video editing software creates challenges in verifying their integrity. And has led to an increase in illegal changes to video content. Deepfakes [1] have also made it possible to produce very realistic counterfeit videos to publish falsehoods or ruin the names of individuals in public. Many examples of video manipulations point to the growing complexity of video forgery and have spurred the need to develop enhanced forensic techniques for reliable verification of video forgeries. This paper establishes a robust technique for detecting and preventing video alterations using a combination of blockchain and video hashing.

Blockchain [2] is a decentralized, immutable, and distributed network that provides an excellent way of safeguarding digital assets. The transparency and auditability of the technology have lent to its application in many domain areas, particularly for cryptocurrencies. Hashing [3] has long been used to verify the integrity of data. Although hashing may be used in isolation to verify individual videos, the need for a robust framework that allows videos to be compared at a large scale and suitable for both verification and preservation of video integrity is paramount in addressing the current challenges of video forgery and their detection.

This work harnesses the collective strength of blockchain and hashing techniques in formulating a robust framework for preserving video integrity and addressing video falsification. It contributes to the field of multimedia forensics by providing a new approach for video integrity checks. It supports the evidence admissibility requirements of having a verifiable chain of custody in a court of law. Our proposed solution also reaches beyond the digital forensics perimeter, by providing a secure way of maintaining video data in many digital platforms. Although some existing work has suggested the use of blockchain for video verification in Internet of Things (IoT) devices and other areas [2, 4], the uniqueness of our approach comes from the usability of the method in different areas including IoT and any platform involving video integrity preservation or video authentication.

In section II, we provide some of the related works to this paper. Section III describes our approach to video preservation and verification. In section IV, we discuss our experiments and results. Section V discusses some of the possible considerations and provides insight into how these may be addressed. The conclusion is presented in section VI.

This section provides a brief introduction to multimedia and video forensics, hashing, blockchain technology, and how these concepts can be used to protect video content. In addition, we discuss some of the relevant work that also employs blockchains and highlight the uniqueness of our approach.

Multimedia forensics is a branch of forensic science that deals with the examination and analysis of multimedia evidence (including audio, video, and images) to determine their integrity and authenticity. Existing approaches for multimedia forensics involve the use of various techniques, including signal processing, pattern recognition, machine learning, and image processing techniques to analyze digital media. Although issues of video integrity and authentication can have multiple perspectives, multimedia forensics is essential where legal concerns are involved [5]. As a subset of this domain, video forensics concentrates on videos and deals with unique issues surrounding video content. This involves detecting video editing, alteration, and other manipulations on video files. Although forensics focuses on a legal context, questions about the authentication of videos are crucial in many other contexts, including journalism and digital preservations. Regardless of the context, some of the approaches that have been applied encompass frame-by-frame analysis, analysis of compression artifacts, and digital watermarking. But these face the challenge of being time-consuming and the potential of accidentally confusing or removing details.

In addition to these methods, video hashing has become a fundamental part of video security. Video hashing involves an encrypted signature or hash of a video item, which may be utilized for several purposes, including content authentication, duplication detection, and safe handling of content. This involves the extraction of key features (from a video) and encoding them into a compact hash value. With this extraction and encoding process being hard enough in practice, avoiding duplication of the efforts on a platform or when dealing with a large number of videos that may get changed or compressed over time is important.

The application of blockchain in video security and forensics opens up a new way of securing the integrity of digital media. While blockchain is mainly associated with cryptocurrencies, it is an immutable and irreversible logging system. In the context of video forensics, blockchain can be used to store hashes of video content so that modifications may be easily detected. In [6], the authors show that blockchain can be used for creating a permanent record of video content and potentially support integrity verification. An approach that focuses on forgery detection [7] employed traditional approaches in video forensics together with blockchain technology. Another work that has explored the use of blockchain for video authenticity [8] focuses on anti-duplication mechanisms and the prevention of pirated videos.

These advancements in blockchain for video forensics force a change of mind about managing digital media security. Since blockchain is decentralized and highly safe, it provides a great way to guarantee video authenticity and has become a potential solution to the problems of forging digital media and fraud. Recent works have also extended these approaches to investigate the potential use of blockchain in providing more secure video databases for security camera videos [9], as well as guarantee transparency, particularly in surveillance recording management.

Several authors [10, 11] have noted a possible combination of video hashing and blockchain technology as a feasible and reliable method of authenticating and verifying video content. The authors [11] explore the use of blockchain for real-time video supervision systems and show how video content can be stored on a blockchain to enable real-time analysis and monitoring, thus improving the credibility and reliability of security footage in city surveillance systems.

II. Main Contributions

Our novel approach to hashing videos and utilizing blockchain for improved video forensics distinguishes this work. The proposed method goes beyond existing solutions to tackle more complex video forgery and tampering aspects, such as retiming, interpolation, and splicing. It builds on a combination of blockchain technology with video hashing.

We describe a hashing approach that considers several aspects of a video, including visual and time-based contents, and which varies with slight modifications. Additionally, the blockchain framework chosen for our approach and experiments is designed to rapidly process a large amount of video information necessary for real-time operations. Changing a video's content would produce an alternate hash from the one used on the blockchain record and cause alarms. A stronger resistance against video alterations is provided by the blockchain and the customized video hashing method, thus improving the effectiveness of video verification processes.

Our solution is further strengthened by the threshold determination method, which we discuss in subsection B. This approach provides an accurate standard for identifying video manipulation by establishing predetermined criteria based on an in-depth examination of video attributes. The threshold determination method provides a uniform standard for forensic investigation, negating the possibility of inaccuracy and variations of results with varying thresholds. The advantage of this static methodology is its simplicity and capacity to yield reliable, predictable results in various video-altering circumstances. The following subsections give a detailed overview of our approaches.

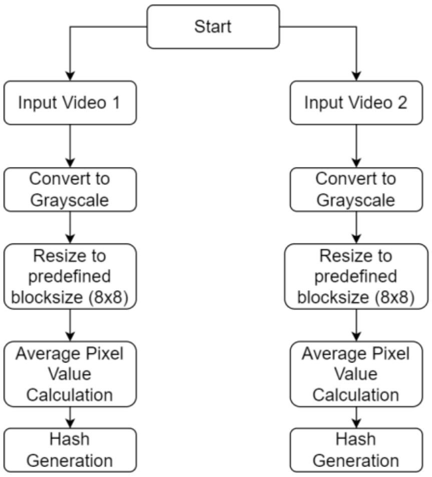

Start
Input Video 1
Input Video 2
Convert to Grayscale
Convert to Grayscale
Resize to predefined blocksize (8x8)
Resize to predefined blocksize (8x8)
Average Pixel Value Calculation
Average Pixel Value Calculation
Hash Generation
Hash Generation

Fig. 1: Flowchart of our video hashing algorithm

A. Video Hashing

The video hashing algorithm, depicted in Fig. 1 provides a way to safeguard the validity and truthfulness of video content. It accepts an input video and processes it to generate a specific hash value as its digital fingerprint.

In the initial process of the algorithm, the video frames are read for processing. This is achieved by extracting each of the video file's frame sequences to ensure that all video

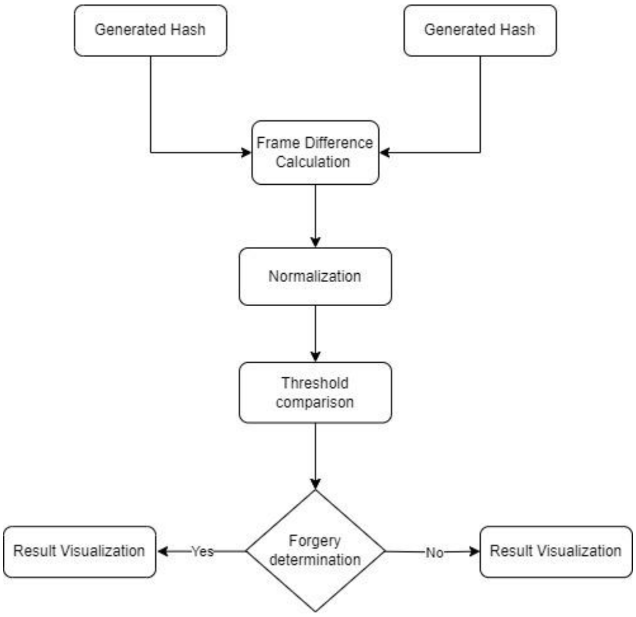


Fig. 2: Flowchart of video integrity determination

parts are included in the hash generation. Then, they get transformed into grayscale. This is to simplify the computation and emphasize the structure information of the frames instead of the color changes as they might result from nonintentional actions. It also helps to standardize the hashing process to ensure that changes in video resolutions and aspect ratios do not affect the hash values. In the next step, all the frames converted to grayscale are resized into a specified size. It is equally essential to resize frames to a smaller and uniform size to achieve an effective hashing operation and reduce the data to be processed. The computation of hash values is the very heart of hashing algorithm. It involves processing the frames and computing a string of fixed-sized characters using a cryptographic hash function. The hash values are irreversible, meaning that they cannot lead to the reconstruction of an original video from a resulting hash value.

A critical step in verifying the legitimacy of the video lies in the post-hash generation stage shown in Fig. 2, where possible falsification is detected using a rigorous hash comparison technique. This approach involves comparing the hash of a 'suspicious' video to that of an actual or known video. Inconsistencies between these hashes set off a frame-by-frame investigation that reveals even the most minor changes that might go undetected by the naked eye. To ensure a consistent basis for comparison, the procedure normalizes the disparities between frames and considers variances in encoding or transfer. At this point, the threshold evaluation becomes important. The algorithm uses a predefined threshold to distinguish between permissible differences and those that may indicate tampering. An alert is raised to indicate possible video forgery or modifications, and additional investigation is required if the normalized frame difference is more significant than this predetermined limit.

This hashing method offers a robust way of preserving video integrity in conjunction with threshold-based fraud detection. Through the integration of frame analysis and hash functions, this suggested method provides an effective method for digital law enforcement and guarantees the preservation of video evidence over time by integrating this method into blockchain technology.

B. *Blockchain*

Blockchain can be compared to a shared digital notebook between several computers. Because many computers check and secure every entry, the notebook is exceptionally dependable and hard to break. It is a chain of blocks, each including a set of data records. This chain forms a link between the blocks using cryptographic hashes, which ensures the permanence and integrity of the data stored within the blockchain. As with other fields in which the technology has been employed, the use of the blockchain for video tampering detection offers many advantages: it provides the ability to safeguard video data from alteration at a large scale, guarantees a clear history of video trade activities, and is capable of exposing fraudulent activities on videos.

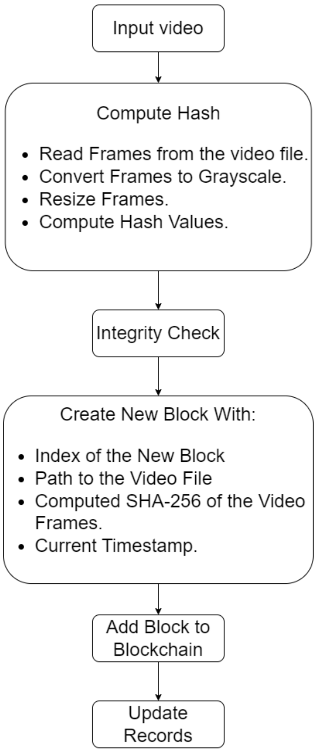
The use of blockchain in our solution is multidimensional and builds upon the fundamental benefits of a blockchain. The blockchain is an excellent tool for keeping an unchangeable record of video data since it can store video hashes indefinitely. The authenticity of a video may be verified by comparing its hash, which is maintained on the blockchain, with a freshly calculated hash from the same video. Compared to older approaches, which could be less secure and need more resources, this verification method is dependable and quick.

When there are differences, the blockchain makes it easier to quickly identify dissimilarities because each time an altered (or previously non-existent) video is identified, a new hash is generated for it and included in the blockchain, making it simple to identify and track in the future. As a result, the blockchain serves as a method for transparency as well as disallowing tampering by ensuring that all attempts to add or verify a video are tracked and recorded forever.

As Fig. 3 illustrates, a series of steps are involved when generating a new block in the blockchain once a video file is submitted. We break down the video and look at every frame individually to develop a distinctive 'fingerprint' and then convert each frame to grayscale and uniformly alter its size. Using a similar algorithm as earlier described, the hash value is calculated by utilizing these video frames. Thereafter, in order to create a new block for the video, a SHA-256 hash of the computed hash value is calculated. The hash, which functions as an identification code, captures the fundamental features of the video once it gets created. This hash is used to construct a new block that contains extra information, like the path to the video file and a timestamp indicating the precise moment the block was formed. This block, which is now a candidate for inclusion in the blockchain, protects the integrity of the network by having an index connecting it to the block before it.

The block goes through a verification process before being added to the blockchain. After the hash calculation is completed, verification within the blockchain model starts. The video's hash is matched against the blockchain ledger, looking for any previous states or alterations noted on the video. An existing entry can confirm the video's authenticity or alert if discrepancies are detected.

Next, the system extensively verifies the video lengths and other metadata as shown in Fig. 4. Video length is one


Input video

Compute Hash

- Read Frames from the video file.
- Convert Frames to Grayscale.
- Resize Frames.
- Compute Hash Values.

Integrity Check

Create New Block With:

- Index of the New Block
- Path to the Video File
- Computed SHA-256 of the Video Frames.
- Current Timestamp.

Add Block to Blockchain

Update Records

Fig. 3: Illustration of the blockchain usage

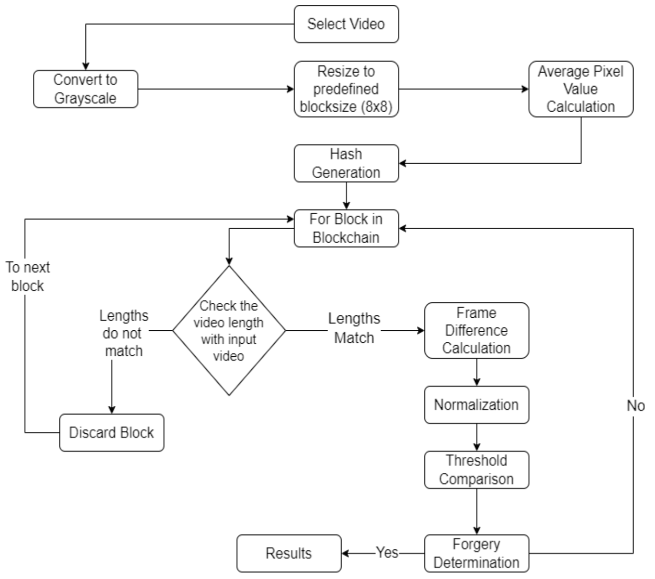


Figure 4: Forgery detection algorithm within the blockchain

primary metric. If they differ, the block is discarded. Our blockchain algorithm currently only works for videos of the same length. Therefore, the verification step entails matching the video's length and the hash value archived in the blockchain. This consistency is crucial to continue the process. If the lengths of the frames are similar, the algorithm advanced to calculate the frame difference. It compares each corresponding frame from the input video with that associated with the blockchain, identifying discrepancies. In this specific frame-by-frame approach, every manipulation will be detected and validated, no matter how small.

Normalized frame differences are calculated to guarantee accurate comparison and differentiation of authentic changes caused by tampering with the stored video data from random variations due to unavoidable alterations in the current data. These comparisons then undergo a threshold comparison. We implement a predefined threshold that is used to define tolerance levels. The sensitivity level is deliberately set to remain responsive but not vulnerable to changes and immune against false positives. The algorithm marks the video as possibly fabricated if the normalized differences exceed the threshold. This decision is not made lightly; exceeding the threshold implies noteworthy and intentional changes, which may cause significant concern and necessitate more investigative work. The blockchain is updated when the video satisfies these rigorous examinations; a new block with the hash plus metadata is then safely added. The associated entries are revised on every node upon successful validation. By doing this, the digital signature of the video is spread and maintained immutably throughout the entire network.

If a video is changed in any way after it has been recorded on the blockchain, the hash will differ from the data that has been stored, indicating that there may have been an effort at manipulation. Because of the nature of blockchain technology, this identification is rapid and unquestionable, offering a solid defense against any tampering. The design of the blockchain increases confidence in the validity of the video by preventing any one point of control from changing the data that has been recorded. Additionally, the openness of blockchain creates an atmosphere of confidence and dependability by enabling any entity with the necessary authorizations to verify on its own the authenticity of a video.

The static thresholding technique for video verification is a fundamental methodology in our approach and is selected for its dependability and consistency in identifying video manipulation. This method is based on threshold amounts that have been predefined and thoroughly specified by a thorough analysis of the features of videos under different scenarios, as described in section III.C below. These cutoff points are carefully adjusted to distinguish between acceptable deviations and deceptive changes. A significant amount of video data is analyzed by contrasting the features of natural and manipulated videos to establish threshold values. The distributions of critical statistics, including pixel frequency, frame percentage, and compression artifacts, are analyzed to set a limit that maximizes the identification of forgeries while minimizing the number of false positives.

Consistency is one of the significant benefits of using a static threshold as it implies it is not subjected to changes based on a video's content. This leads to a consistent evaluation, resulting in a simplified understanding of the outcomes of the system. The proposed solution has substantial security aspects. It features cryptographic solid hash functions that are computationally not feasible to reverse engineer. A hash function generates each video's digital signature, which is then safely recorded on the blockchain to guarantee integrity and traceability. The verification process involves accessing the video's original hash value from the blockchain network, and comparing the two derived hashes with each other, after which a determination is made on whether the hashes match.

A discrepancy in any details is always a signal for a deeper investigation. Detecting this is automated, and alerts are issued whenever the system detects potential tampering. These alerts can be further analyzed to establish the type and level of tampering. The proposed system can be applied in many situations and for different kinds of video content. The benefits associated with this system surpass current methods and the system provides a high level of dependability.

C. *Threshold Selection*

Making a strategic choice for an appropriate threshold value is a key component of our approach. Extensive testing was done before deciding on an acceptable value of 0.02. This choice was supported by thoroughly examining how our algorithm performed in various settings. Rather than making a random choice, we determined the threshold by carefully weighing the trade-off between false positives and false negatives in the video. We increased the degree of sensitivity of the video forgery recognition procedure by setting a 0.02 threshold. The detection threshold was carefully calibrated to balance the accurate identification of video forgeries and preventing false alarms to achieve optimal detection effectiveness. This optimization is essential in real-world applications, where incorrect identification might have a high-cost impact or significant impact on people's lives. The choice of this limit, made in light of actual data and logical argumentation, supports the operational efficiency and technological proficiency of our approach.

III. EXPERIMENTS & RESULTS

This section describes the result of our experiments which explores two essential tasks for authenticating videos. The crucial problem of detecting manipulated videos is addressed in the first experiment. We employ our algorithm to analyze two sample videos to assess their authenticity. This experiment demonstrates our technique's forgery detection capability and establishes a baseline for evaluating its efficacy in distinguishing manipulated videos.

The second experiment investigates the creative use of blockchain technology in conjunction with video hashing. This experiment is crucial given the growing demand for trustworthy and safe digital content across various industries, including entertainment and surveillance. Together, these experiments provide an understanding of the possible uses of our video analysis methods.

A. *Experiment 1: Video Hashing*

Our first experiment used a hashing-based method that examined two videos to determine their authenticity and identify video fraud. We calculated the average hash for every video frame and the discrepancies between the associated hashes were measured.

Two simulations were conducted for this technique: the first involved two video clips that were both genuine, and one was a copy of the other. For the second simulation, we also used two video clips, including an authorized video and an unidentified video that is assumed to be fake. Our average hash method processes input video frame by frame, scaling it to an 8x8 block (based on the block size argument), transforming it to grayscale, and then calculating the average value to create the hash. The degree of similarity was then determined by comparing the hash values of corresponding frames, calculating the disparity in the total amount of different bits, normalizing that difference to compare it with the threshold value, and then processing the result.

Fig. 5 and Fig. 6 show the normalized differences in the hash values of related frames and represent the outcomes of the hash comparisons. Fig. 5 shows that there is no indication of fabrication, as with the first experiment. The result shows a constant pattern of very minor to no differences across all frames. A striking contrast can be seen in the output of the second simulation shown in Fig. 6, where several red-marked frames show variations more significant than the predetermined 0.02 threshold. The spikes in the normalized difference point to possible forgeries since they show differences between the two videos.

The first simulation has no fluctuations, and the frame normalized difference is below the threshold, showing that neither of the compared videos was forged. For the second simulation, the visualization confirms that the video differs significantly from the original material suggesting that it is most likely a fake. The criteria used for this decision is the graphs' cutoff line. Frames with normalized differences less than this cutoff are regarded as genuine (green bars); those with differences more than this indicate possible manipulation (red bars). Since the hashing method is straightforward and facilitates rapid and computationally effective evaluation, it is a good choice for preliminary forgery testing.

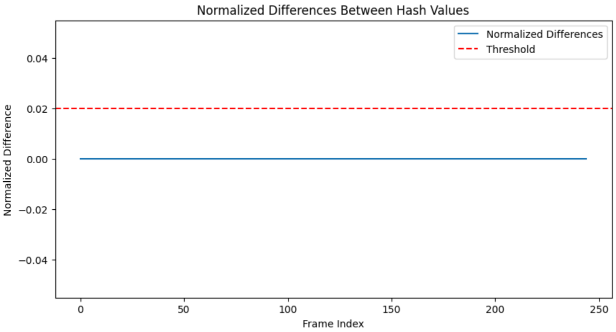


Fig. 5: Output from two videos with no forgery

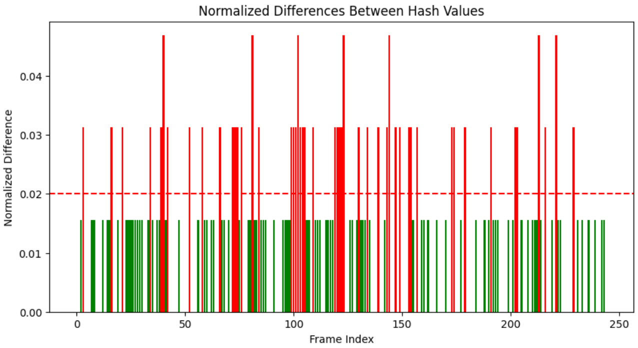
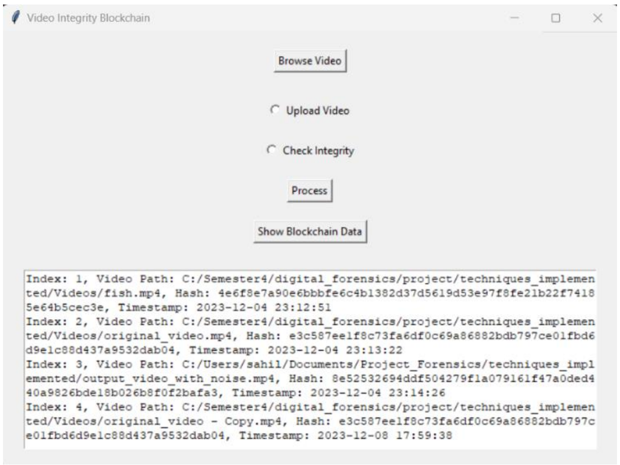


Fig. 6: Forged sample video output

B. *Experiment 2: Video Hashing & Blockchain*

The use of blockchain technology with video authenticity assessment is the main focus of our second experiment. The goal was to store video hashes using a blockchain's irreversible features to establish a tamper-evident solution. This process guarantees that any alterations are openly recorded and simple to identify, in addition to helping to confirm the videos' authenticity.

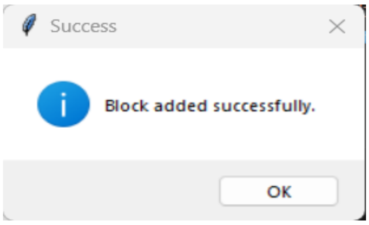
A graphical user interface (GUI) in the platform designed for this research project, shown in Fig. 7, allows users to participate in submitting videos and verifying their authenticity using blockchain records. As a decentralized ledger, the blockchain preserves the accuracy and sequential arrangement of the records by storing the timestamps and hashes of every video. We implemented a Python program that processes videos, generates hash values, and carries out the comparison to identify forgeries, forming the methodology's basis. The offers visual confirmation by presenting notifications like "Forgery Detected" for inconsistencies in video hashes and "Block added successfully" for newly created records (e.g., as shown in Fig. 8 and Fig. 9). The UI visually represents the blockchain information, showing each block's index, path, hash, and timestamp. The system verifies the authenticity of a video by comparing its hash with the blockchain data. A notice indicating potential forgery and inability to include a video (or a successful block addition) in the blockchain is also shown for ease of usability.



```
Index: 1, Video Path: C:/Semester4/digital_forensics/project/techniques_implemen
ted/Videos/fish.mp4, Hash: 4e6f8e7a90e6bbbfe6c4b1382d37d5619d53e97f8fe21b22f7418
5e64b5cec3e, Timestamp: 2023-12-04 23:12:51
Index: 2, Video Path: C:/Semester4/digital_forensics/project/techniques_implemen
ted/Videos/original_video.mp4, Hash: e3c587ee1f8c73fa6df0c69a86882bdb797ce01fbd6
d9e1c88d437a9532dab04, Timestamp: 2023-12-04 23:13:22
Index: 3, Video Path: C:/Users/sahil/Documents/Project_Forensics/techniques_impl
emented/output_video_with_noise.mp4, Hash: 8e52532694ddf504279f1a079161f47a0ded4
40a9826bde18b026b8f0f2bafa3, Timestamp: 2023-12-04 23:14:26
Index: 4, Video Path: C:/Semester4/digital_forensics/project/techniques_implemen
ted/Videos/original_video - Copy.mp4, Hash: e3c587ee1f8c73fa6df0c69a86882bdb797c
e01fbd6d9e1c88d437a9532dab04, Timestamp: 2023-12-08 17:59:38
```

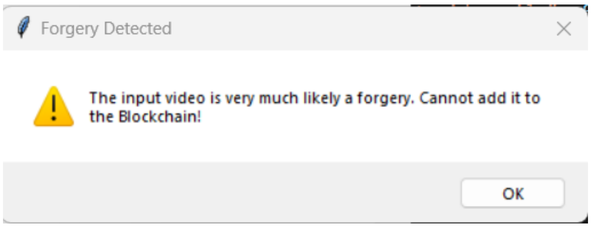
Fig. 7: Blockchain implementation UI with sample blockchain data

The blockchain's stability is demonstrated by successfully including a video hash, and discovering a forged hash presents its capacity for preventing manipulation. These feedback messages are straightforward representations of the decisions and actions made by the system as a whole. This experiment shows how video hashing alongside blockchain technology can provide a transparent, safe, and dependable way to preserve video integrity in various applications, including copyright administration and digital investigation.



Block added successfully.

Fig. 8: Successful addition of new video to blockchain



The input video is very much likely a forgery. Cannot add it to the Blockchain!

Fig. 9: Rejection from blockchain

IV. Considerations and Future Work

Although the experiment shows the applicability of our approach, the following factors will be considered as part of improving the system's functionality and user experience.

- Scalability: our experiments included a restricted set of video files to confirm the efficacy of our approach. Future improvements will assess its performance with a significantly higher number of videos.
- Video processing and blockchain overhead: Analyzing videos, particularly those of significant quality have significant processing costs. Although we currently use OpenCV [12], which is a popular video analysis tool for our frame-by-frame evaluation, we plan to explore other possible alternatives. Future work would examine integrating AI-based methods to improve video analysis proficiency. In addition, alternate blockchain architectures will also be considered.
- Video length and format constraint: We currently only consider videos of similar length, given that videos of different lengths already indicate some modification. Only some predetermined video formats were also included in our tests. Additional video formats will be tested by enabling our system to accommodate more video encodings in future works.

V. Conclusion

This paper discusses our approach of using blockchain technology's immutability with video hashing algorithms, in the validation of video authenticity. The results show that such technology can be successfully used to identify video forgeries and track video records safely. As described in section V, some of the constraints imposed on our experiments may be removed to further test the scalability of the design and the speed at which video records are processed.

The proposed method has applicability in both legal and security perspectives and contributes to the discipline of digital forensics. As digital media becomes more and more essential to communication, court procedures, and information distribution in the modern world, further study and advancement in the field of multimedia forensics are needed and this work contributes to addressing some of the challenges in the field.

References

[1] M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung, "Deepfake Detection: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 25494-25513, 2022, doi: 10.1109/ACCESS.2022.3154404.

[2] A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[3] Lianhua Chi and Xingquan Zhu. 2017. Hashing Techniques: A Survey and Taxonomy. ACM Comput. Surv. 50, 1, Article 11 (January 2018), 36 pages. https://doi.org/10.1145/3047307.

[4] Mercan, Suat; Cebe, Mumin; Aygun, Ramazan S.; Akkaya, Kemal; Toussaint, Elijah; and Danko, Dominik, "Blockchain-based Video Forensics and Integrity Verification Framework for Wireless Internet-of-Things Devices" (2021). *Computer Science Faculty Research and Publications*. 53.

[5] Ma, Z., Zhu, L., Yu, F. R., & James, J. (2021). Protection of surveillance recordings via blockchain-assisted multimedia security. International Journal of Sensor Networks, 37(2), 69-80.

[6] Jan, M. A., Cai, J., Gao, X. C., Khan, F., Mastorakis, S., Usman, M., ... & Watters, P. (2021). Security and blockchain convergence with Internet of Multimedia Things: Current trends, research challenges, and future directions. Journal of Network and Computer Applications, 175, 102918.

[7] Gallo, P., Nguyen, U. Q., Pongnumkul, S., & Barone, G. (2021). Blockchain for smart cities: Applications for IoT and video surveillance systems. Land, water, and energy innovations for Vietnam's sustainable development, 227-24

[8] A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," in IEEE Access, vol. 7, pp. 117134-117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[9] Lianhua Chi and Xingquan Zhu. 2017. Hashing Techniques: A Survey and Taxonomy. ACM Comput. Surv. 50, 1, Article 11 (January 2018), 36 pages. https://doi.org/10.1145/3047307.

[10] M. S. Rana, M. N. Nobi, B. Murali and A. H. Sung, "Deepfake Detection: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 25494-25513, 2022, doi: 10.1109/ACCESS.2022.3154404.

[11] Mercan, Suat; Cebe, Mumin; Aygun, Ramazan S.; Akkaya, Kemal; Toussaint, Elijah; and Danko, Dominik, "Blockchain-based Video Forensics and Integrity Verification Framework for Wireless Internet-of-Things Devices" (2021). *Computer Science Faculty Research and Publications*. 53.

[12] OpenCV. (2015). Open Source Computer Vision Library. https://opencv.org/