A Video Security Verification Method Based on Blockchain

Zhenghang Zhao[1 *], Yunxia Liu[2 * †], Hongguo Zhao[2], Yonghao Wang[3]
[1]*School of Cyber Science and Engineering, Zhengzhou University*
[2]*Zhengzhou Normal University*
[3]*Birmingham City University*

***Abstract*—This paper proposes a blockchain-based video security verification method. In order to ensure the security of the video, we use data hiding technology to embed message that can ensure the security of the video into the video, at the same time, in order to improve the non-tamperability and non-forgery of data hiding. We construct the hash value of the message embedded in the original video, the hash value of the carrier video (video with embedded message) and the attribute message of the video as video metadata, and upload the video metadata to the blockchain network. Comparing the message extracted from the carrier video with the video metadata stored on the blockchain can achieve double verification of the video. At the same time, distributed storage of carrier video through IPFS can effectively store and manage large-scale video data, ensuring the security and high availability of videos.**

***Index Terms*—Blockchain, Data hiding, IPFS, Video verification**

I. Introduction

Blockchain technology was proposed by Satoshi Nakamoto in a Bitcoin paper. Blockchain technology integrates many traditional technologies, such as distributed systems, P2P networks, encryption algorithms, consensus mechanisms, etc. It is decentralized, non-tamperable, traceable, open and transparent[1]. In past research, many scholars have devoted themselves to storing the attribute message of videos in the blockchain network to ensure video security[2]-[4]. However, blockchain is open and transparent, the message stored in it is visible to everyone. Some message needs to remain private and is not suitable for public storage. Data hiding can embed these secret message into videos, so research on combining Data hiding with blockchain technology to collaboratively maintain video security is very valuable.

Data hiding embeds data into the cover video contents so that it looks identical to the original video[5]. Current video steganography algorithms can be divided into three categories according to the embedding position: the embedding position is in the original video domain[6]-[7], the embedding position is in the compressed domain[8]-[9], and the embedding position is in the bitstream domain[10]-[12]. In past research, many scholars have devoted themselves to embedding video attribute message into videos to ensure video security[13]-[14]. However, when message is embedded in the video, any unauthorized modification or forgery attempt will destroy the embedded message, making it impossible to extract the message normally. We combine video steganography with blockchain technology. The non-tamperability of blockchain records ensures the authenticity of video content, which can provide stronger video protection and ensure that video content is not subject to unauthorized modification or forgery. The impact can provide a more reliable protection mechanism for videos.

Distributed storage is an advanced data storage method that disperses data on multiple physical or virtual devices instead of centrally storing it in a single location [15]. IPFS is a system built on the principle of distributed storage. It is based on decentralization, content addressing, data redundancy and distributed network protocols, and provides powerful tools and frameworks to achieve the goal of distributed storage. IPFS adopts a data redundancy strategy to copy video files to multiple nodes. This improves the availability of video, even if some nodes are offline or inaccessible, users can still access the same video, thereby reducing the risk of service interruption due to node failure or network issues. In past research, many scholars have devoted themselves to distributed storage of videos to ensure the sustainability and high availability of videos. In order to ensure the security of the video, we embed the secret video security message into the video. In order to improve the non-tamperability and non-forgery of data hiding, We store the hash value of the carrier video, the hash value of the secret message, and the attribute information of the video in the blockchain. Extracting secret message from the carrier video under the blockchain and comparing it with the message stored on the blockchain can achieve double verification of video security and better ensure video security. At the same time, the carrier video is stored in IPFS to ensure the security and high availability of the video.

The rest of this paper is organized as follows, Section II describes the video security verification method, Section III gives the experimental results, and Section IV gives the conclusion of the paper.

II. The Proposed Method

During the process of saving video metadata to the blockchain, we first embed the secret message related to video security into the original video, and the embedded video is a carrier video. Then we will store the generated carrier video in a distributed manner to ensure the high availability and

* Zhenghang Zhao and Yunxia Liu are co-first authors.
† The corresponding author.

security of the video. Then, to verify the integrity of the video, we perform a cryptographic hash operation on the encrypted video. Because blockchain is open and transparent, the message stored in it is visible to everyone. Therefore, we also perform an encrypted hash operation on the secret message to obtain the hash value. Then, we construct these two hash values and video attribute message into a video metadata object and store it in the blockchain. Video attribute message includes but is not limited to video title, video author, video duration and author email, which can be added or deleted according to specific business functions.Figure 1 describes the process.

When video security needs to be verified. We first need to obtain the carrier video from IPFS, extract the secret message from the carrier video, and then perform encrypted hash operations on the secret message and the encrypted video respectively, and the result will be used as the video security message under the blockchain. Then, the metadata of the carrier video is obtained from the blockchain as video security message on the blockchain. Comparing the hash value of the carrier video under the blockchain with the hash value of the carrier video in the video metadata on the blockchain can ensure the integrity of the video. Comparing the secret message hash value obtained under the blockchain with the secret message hash value in the video metadata on the blockchain can ensure the consistency of the carrier video. Achieve the dual authentication effect of video security, effectively ensuring the security of the video.Figure 2 describes the process.

III. Experiment Result

As an implementation of this method, Fabric version 2.4 is used as a blockchain to store data, and the x265 version 2.8 encoder is used to implement the algorithm in [9] by modifying the optimal prediction mode of the 4*4 block in the frame to video Perform the embedding operation and use HM version 16.20 as the video decoder to extract the carrier video. The version description of the rest of the configuration :go version 1.20.1, Docker version 20.10.21, docker-compose version 1.25.0.Experimental environment: The cpu is Intel(R) Core(TM) i9-10900 CPU @ 2.80GHz 2.81 GHz, the gpu is NVIDIA GeForce GTX 1650, the memory is 32GB, and the operating system is Ubuntu 20.04.3 LTS.

Table I gives the experimental results, in which the total time for video metadata to be uploaded refers to the sum of the time to embed secret message into the video, the time to upload the carrier video to IPFS, and the time to store the video metadata in Fabric. The total duration of double verification refers to the sum of the time it takes to obtain the carrier video from IPFS and extract the secret message from the carrier video, and the time it takes to obtain the video metadata from Fabric and compare it with the data on the blockchain. We can see that the encoding speed of x265 is quite impressive.

When using the above-mentioned video with a resolution of 720 x 1280 and a total number of frames of 269. After embedding the secret message, the returned cid is ”Qmeiw6PbcNgPHagS3GmtWhFURDMoZXR3VmHapsuXxd nNgp”. Use the ipfs ls command to list the cid and size of the carrier video stored in blocks, as shown in Table II.

When using the above-mentioned video with a resolution of 720 x 1280 and a total number of frames of 269, the secret information is a docx document containing the text ”A Video Security Verification Method Based on Blockchain”, Obtain the carrier video through IPFS under the blockchain, and then perform an encrypted hash operation on the carrier video to obtain a hash value; extract secret message from the carrier video, and perform an encrypted hash operation on the secret message to obtain a hash value. Compare these two hash values with the hash value stored in the carrier video metadata on the blockchain. The results are shown in Table III.

TABLE I
Video metadata uploading and two-factor verification time

Resolution	**Total frames**	**Secret file size**	**Video metadata upload time**	**Two-step verification time**
1280 x 720	181	19KB	1min 35s	5.67s
720 x 1280	269	19KB	1min 50s	6.93s
960 x 544	287	19KB	2min 3s	7.52s
960 x 544	510	19KB	2min 17s	7.48s

TABLE II
Directory structure information of carrier video

Cid	**Size**
QmdAtENnz8dwaGDidZrvNbAfoaq3P3VbnqBXN2vS969rUZ	262144
QmcfcT5XGJFTBTSa1dVZAonRuoZDHtQQAkWSnpuovZsxqD	262144
Qmdj41TT7sF4yvraYvrQGzNAGXcC22coWdEeca9zChmVFT	262144
QmTaxRETH5nNryXFzi2LHwLUL8uu9wKYZ9GffLZ8rd6be5	262144
QmbFumbKw65MVmLcTgkLUybcq6JyUrgLhVwy2rmuluYunm	262144
QmzyJoYNxS7oGaxTpMuDy8yv3YeDmgyXN4Ehe4ZVLLs7Kd	262144
QmdBicpnCbADHKKbrsUVe5x73Ao8HwGHLJRQQVb2Cn4zfp	262144
Qme1owWmeAnn649mmaanpt3tmcgB23ir3n25K4pRHqmEh5	262144
Qmettuv3xHSn7tCEu1zHXoqH6zDLqVPnvsKrvk3KbtU6HH	262144
QmZ4RuVfSMoSCejqpbhaQ7oYypPR5yyzUvhSQsePmizEiT	262144
QmZBs6hzSwxv4YxknBNPATy6VgpCb38LwyRpRwB1UepEzh	262144
QmdyLAZaG1c41L6ZrQhdskiAC4TKsvejLuGpg3qKEatUnc	262144
QmXZgnUQqzU5wAfzVK5gxZftJhhmJrFtj899dsX27SVjHe	262144
QmPZ2sKWD3pBdPtbyS6xCtnTCkNu5HpbGxjPDMma9MKsc2	262144
QmUK9iigtT6aSbF6WN5hmR1QPt5V97EuukqVC6XXmc1Gyg	80707

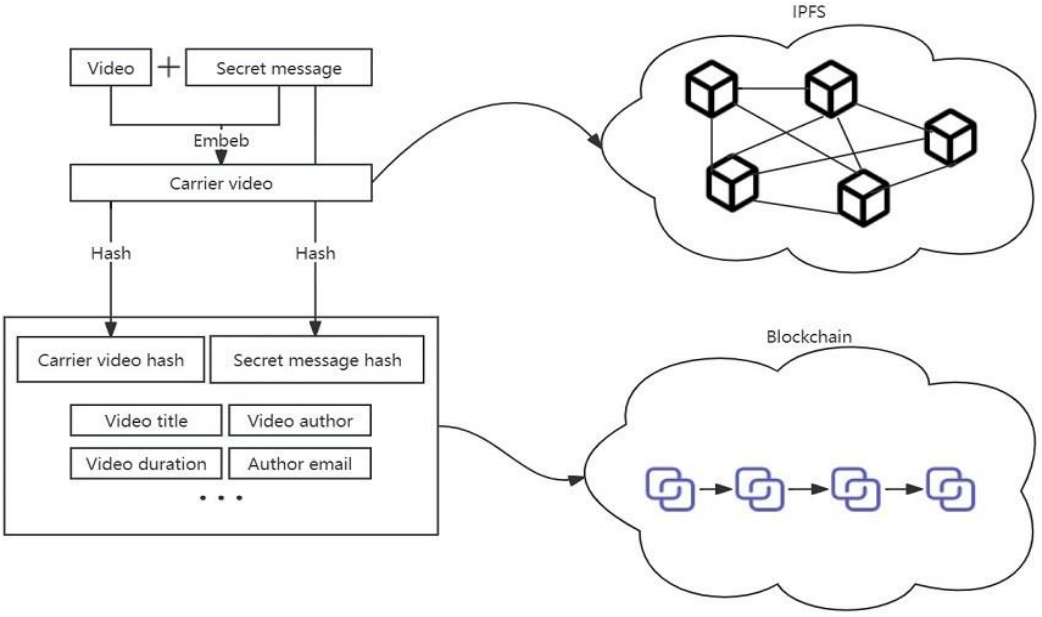

Fig. 1. Video metadata to blockchain.

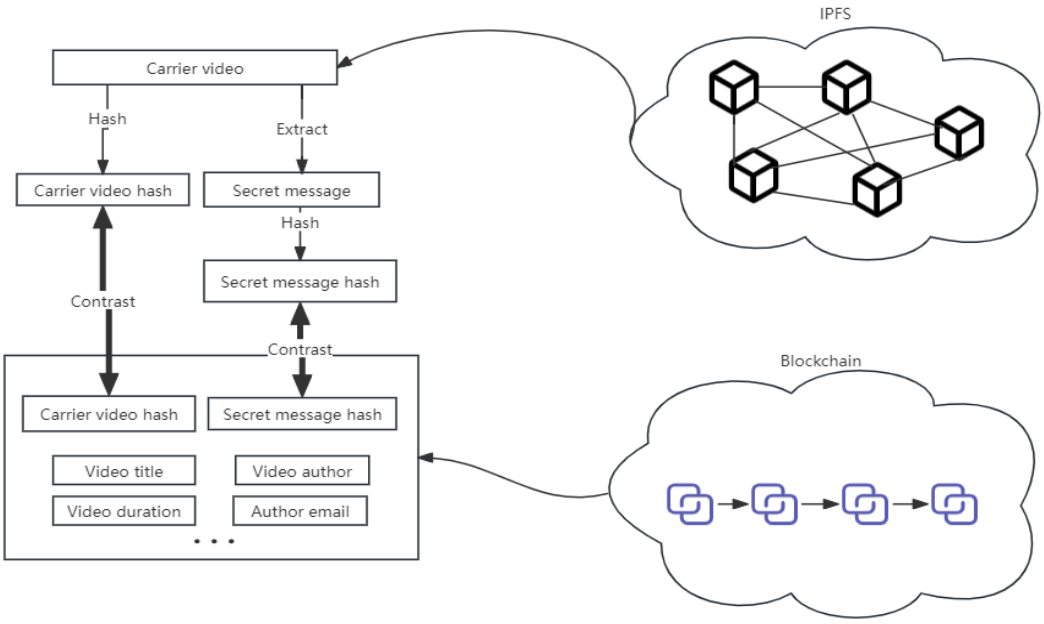

Fig. 2. Video metadata two-factor verification.

TABLE III
HASH VALUE COMPARISON RESULTS

Certification	Off-blockchain data	blockchain data
Carrier video hash value	20366167ee5f9e87128275b58025024aa3d2ed767a520e0e2281cd2ab94ec67c	20366167ee5f9e87128275b58025024aa3d2ed767a520e0e2281cd2ab94ec67c
Secret message hash value	b2dc22656762ea33c4348f475ee307c6ed825d14ed2f51e00ffd88e103646c29	b2dc22656762ea33c4348f475ee307c6ed825d14ed2f51e00ffd88e103646c29

IV. CONCLUSION

This paper combines blockchain technology and video steganography technology to achieve double verification of video security.Utilize the video metadata uploading rules under the blockchain to improve the security performance of video steganography that cannot be tampered with or forged. Furthermore, by utilizing the call execution of off-blockchain video steganography, blockchain and off-blockchain collaborative operations improve the security protection of secret information by video steganography and the application scope of existing blockchain technology. Compared with existing video steganography methods and blockchain technology, it has better video security verification effects. It can provide a way to implement video integrity verification scenarios such as video copyright protection, traceability tracking, and verification of whether the video has been changed.

ACKNOWLEDGMENT

We thank the anonymous reviewers for their helpful comments.This research was supported and funded by Henan Big Data Development Innovation Laboratory of Security and Privacy, Henan International Joint Laboratory of Blockchain and Audio/Video Security, and Zhengzhou Key Laboratory of Blockchain and CyberSecurity.

REFERENCES

[1] Y. Qi, J. Liu, F. Dong, P. Dong, Y. Dai, and L. Jiang,"Short Video Copyright Protection Based on Blockchain Technology," in 2021 2nd Asia Conference on Computers and Communications (ACCC), Singapore: IEEE, Sep. 2021, pp. 106–110.

[2] S. S. Siddique and N. S. Fatima, "Smart Verification System for Media File Using Blockchain," 2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2022, pp. 1417-1424.

[3] N. A. A. Moneim and M. T. Gaata, "Video Data Authentication Using a Smart Contract Published on the Blockchain," 2022 Fifth College of Science International Conference of Recent Trends in Information Technology (CSCTIT), Baghdad, Iraq, 2022, pp. 93-99.

[4] Q. Feng, J. Chang and Z. Wu, "Research on the Application of Blockchain in Media Communication Copyright Management," 2023 IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), Beijing, China, 2023, pp. 1-6.

[5] Liu Y, Liu S, Wang Y, et al. Video steganography: A review[J]. Neurocomputing, 2019, 335: 238-250.

[6] Liu S, Liu Y X, Feng C, et al. Blockchain privacy data protection method based on HEVC video steganography[C]. 2020 3rd International Conference on Smart BlockChain (SmartBlock), Zhengzhou, China. IEEE, 2020: 1-6.

[7] Anitha G , Maria K . Probing Image and Video Steganography based On Discrete Wavelet and Discrete Cosine Transform[C]. 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India. IEEE, 2019:21-24.

[8] Liu Y X, Liu S, Zhao H G, et al. A new data hiding method for H. 265/HEVC video streams without intra-frame distortion drift[J]. Multimedia Tools and Applications, 2019, 78(6): 6459-6486.

[9] W. Jia, R. Ding, and W. Li, et al., "A HEVC Video Information Hiding Algorithm Based on Intra-Frame Prediction Modes," Optoelectronics and Laser Technology, vol. 25, no. 8, pp. 1578-1585, 2014.

[10] M. Ghasempour and M. Ghanbari, "A Low Complexity System for Multiple Data Embedding Into H.264 Coded Video Bit-Stream," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 30, no. 11, pp. 4009-4019, Nov. 2020.

[11] D. Xu, "Data hiding in partially encrypted HEVC video," ETRI Journal, vol. 42, no. 3, pp. 446–458, Jun. 2020.

[12] O. S. Faragallah, A. I. Sallam, M. Alajmi, and H. S. El-sayed, "Efficient selective chaotic video stream cipher for SHVC bitstream," Multimed Tools Appl, vol. 82, no. 20, pp. 30689–30708, Aug. 2023.

[13] Velazquez-Garcia, L., Cedillo-Hernandez, A., Cedillo-Hernandez, M., Nakano-Miyatake, M., Perez-Meana, H. (2022). Imperceptible–visible watermarking for copyright protection of digital videos based on temporal codes. Signal Processing: Image Communication, 102, 116593.

[14] Jambhale, T., Gaffar, H. A. (2022). A deep learning approach to invisible watermarking for copyright protection. In Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021 (pp. 493-503). Springer Singapore.

[15] Trautwein D, Raman A, Tyson G, et al. Design and evaluation of IPFS: a storage layer for the decentralized web[C]//Proceedings of the ACM SIGCOMM 2022 Conference. 2022: 739-752.