A Certificate Storage Method for Confirming Video Copyright and Tracing the Source Based on Alliance Chain

Yang Yang\(^{1}\) and Dingguo Yu\(^{2*}\)

\(^{1}\) Intelligent Institute of Media, Communication University of Zhejiang, Hangzhou, Zhejiang Province, China
\(^{2}\) Department of Media Engineering, Communication University of Zhejiang, Hangzhou, Zhejiang Province, China
Email: immer@qq.com

Abstract. In recent years, with the development and update of business models and emerging technologies, there have been more and more forms of piracy and infringement of online video works. It is difficult for the department with copyright to confirm the copyright of the work and trace the source of piracy. Alliance blockchain technology can be partially decentralized, highly controllable, and data is not public by default, providing new ideas and methods for solving the above problems. The thesis proposes a multi-factor confirmation and traceability depositing method (MCTA) for video works of alliance blockchain. First, the alliance member nodes store the signature information of the person in charge in each step in the private chain during video production; second, the smart contract pre-processes the source video, implants watermarks and calculates video fingerprints, and creates a video ID for each video; Finally, double-factor authentication for the suspected infringement of pirated video to confirm the right. Carry on simulation experiment through Truffle+MiniNet+SimBlock. The results show that the method proposed in the thesis is effective and feasible for depositing video works.

1. Introduction

The consensus mechanism based on alliance nodes can ensure that the data will not be illegally modified by an organization [1-2]. The video content contains a large number of image frames [3]. In order not to affect the rate of video sending and receiving, the watermark embedding and extraction process must be efficient enough [4]. In addition, without losing the visually perceptible quality of the original signal, it is also necessary for the embedded watermark to be robust to common signal processing attacks [5]. As it can reduce storage space and improve detection efficiency, video fingerprinting has gradually become a key technology for video copy detection [6]. Video fingerprint is a feature vector that summarizes the video content [7-9]. By measuring the distance of the fingerprint code, you can determine whether the two videos are homologous [10]. Based on the above situation, the thesis is based on the alliance blockchain, with the help of digital watermarking and video fingerprinting technology, and proposes a multi-factor authentication method for the certification of the blockchain-oriented video works.
2. Related Work

2.1. Related Assumptions
(1) The unobstructed rate of the network environment is above 95%, and there is no abnormal situation such as packet loss;
(2) The member nodes of the alliance chain are directly designated, and no further application verification will be conducted;
(3) Hash encryption algorithm uses SHA256.

2.2. Related Definitions
(1) Video ID: the hash value generated by the signature of the person in charge of video production, the hash value of the video digital watermark, the hash value of the video fingerprint, and the public information of the video;
(2) Blockchain simulation: Use MiniNet to create a network that supports SDN, and use SimBlock to simulate a mirrored blockchain, which can define the network size, block generation interval, and network communication speed.

3. Problem Description
The identity of the node that proposes to log in to the alliance blockchain is authenticated, and the result of the authentication will be fed back in time. The node that passes the authentication allows the system to log in and operate. There are \( n \) steps in making a video work, you can define them as \( pro_1, pro_2, ..., pro_n \), these steps together form a set \( P \). It is stipulated that any step requires a digital signature by the responsible person, and then the hash code is calculated on the signature. This code uniquely identifies the step of the video work, which is recorded as \( H_{pro_1}, H_{pro_2}, ..., H_{pro_n} \), these codes together form the set \( HP \). As shown in equation (1):

\[ P = \{pro_1, pro_2, ..., pro_n\} \xrightarrow{Hash} HP = \{H_{pro_1}, H_{pro_2}, ..., H_{pro_n}\} \]  \hspace{1cm} (1)

\( HP \) will store the tag as a step into the private blockchain, and finally will obtain a total hash value for all the tag values of the work. This value will be stored as the video source code in the private blockchain. \( HP_{sum} \) will represent This video element participates in the subsequent traceability work as shown in equation (2).

\[ HP = \{H_{pro_1}, H_{pro_2}, ..., H_{pro_n}\} \xrightarrow{Hash} HP_{sum} \]  \hspace{1cm} (2)

Organize the public information and encrypted information of the video, calculate the exclusive video ID for the video element, and finally perform a hash operation on all the information stored in the ID to obtain a hash value, which is the video ID hash code. In the interstellar file system, select a node with a long online time and a small chance of problems, mark it as a superior performance node, distribute the Hash code of the video ID to the excellent node, and use the POA consensus algorithm to select the node that packs the block. The contract stores the Hash code into the alliance chain, and the video information certification is completed. This is called a multi-factor authentication mode, and the verification is successful. After comparing the video traceability source code, a successful infringement report is generated after success.

4. A Certificate Storage Method for Confirming Video Copyright and Tracing the Source Based on Alliance Chain

4.1. Identity Authentication of Alliance Chain Nodes
(1) All nodes that want to log in to the multi-factor confirmation and traceability certification system for the video works of the alliance blockchain need to have their own private key \( primary \) key. This private key is unique and can identify any node. The private key is also a member the unique identity authentication code of the node login alliance blockchain. The member node enters the information
verification system after successful verification. The system mainly verifies and confirms the user identity of the member node. The system compares and searches the private key entered by the member node in the node information database. If the node information does exist in the node information database, you can confirm that the node is an authentication node in the alliance blockchain, and the system will automatically update the blockchain data for it, and prompt the member node to log in successfully.

(2) If the node information does not exist in the node information database, it can be confirmed that the node is not an authentication node of the alliance blockchain, and the system automatically prompts the member node whether to register the node user.

(a) **Member nodes choose to register.** The node submits its basic information and waits for the existing member nodes to confirm in turn, and after confirmation, returns to the verification system to log in again;

(b) **Member nodes do not choose to register.** The certificate storage system will reject the access request of the member node and end the access. The detailed process is shown in figure 1.

4.2. **Video Source Tracing**

(1) The birth of each video work is proposed by the video planner. The group will issue a production plan and the signature of the person in charge of the production plan. The smart contract will target this production plan and the signature of the person in charge and integrate the two to obtain the hash code of the two as the label information of this step. This information will be first stored in the private blockchain of the video producer.

(2) The video planning team publishes its production plan to the video improvement team 1. Video perfection group 1 will give the video Id and traceability information to the video. These two pieces of information are collectively referred to as process information. The smart contract will integrate the process information with the signature of the person in charge of this step to perform a hash operation to obtain this step. The hash code is stored as tag information in the private blockchain, and then the current progress of the video work is passed to the video improvement group 2.

Repeat the above steps until the video is completely produced. After the video is fully produced, the smart contract encodes the tag information generated by all the previous steps to obtain an up-to-date hash code. This code will be stored in the private blockchain as the video source code. The detailed process is shown in figure 2.

![Figure 1](image_url)
4.3. Certificate of Video Works

(1) If the source video is a long video, the smart contract will automatically adopt an offset slicing method to divide the long video into short videos in units of 15 minutes to form a source video group. If the source video itself is a short video, it can be regarded as having only one element in the source video group.

(2) Carry out watermark embedding operation on the source video group, select the watermark algorithm to calculate and embed the watermark into each video element in the source video group, and then the watermarked video group can be generated. Perform video fingerprint calculation on the video group carrying the watermark, and use the fingerprint algorithm to calculate the fingerprint code of each video element in the video group. Establish a video ID for each video element in the video group. The ID card contains two sets of information, the first set is public information, which contains the video ID, storage location, the owner of the video, a brief introduction to the video, and the time the video was created. The second group is encrypted information, including the digital information of the video, the digital fingerprint information of the video, and the traceability source code of the video. For the video ID card, the hash code of the video ID card is obtained. This hash code is in the alliance blockchain and can be used for on-chain storage and transaction information operations on behalf of this video. The detailed process is shown in figure 3.
5. Experimental Results
In this experiment, Truffle V5.0.0 will be used, and the Solidity code will be updated to adapt it to the version above solidity0.5.0, but also to adapt to the MetaMask update, where the Nodejs version is v10.21.0, the npm version is 6.14.4, adaptation support window, and it’s shown in figure 4. Ethereum object. Extract the key attributes of the video and calculate the video ID for the video, as shown in figures 5 and 6. The attributes included in the video ID include information obtained from the video: video name, video size, video format, video duration, video frame Rate, resolution-width, resolution-height, total video frames, video creation time, video access time, video modification time, and self-added information are: signature of the person in charge (temporary computer name), signature time (stored in the database Instant system time stamp).

After the system extracts the key information of the source video, it is shown in figure 6, and the video ID Hash code for this key information is shown in figure 7. The nodes with low probability of problems and excellent performance in the interstellar file system are called superior nodes. The system...
will automatically select the superior nodes, and use the POA consensus algorithm to select the nodes of the packaged block for the video ID hash code obtained in the previous step. Hash-code the video ID card into the alliance blockchain through a smart contract. This step represents the completion of the registration of video information, as shown in figure 8.

6. Conclusion
The multi-factor confirmation method for the identification of the source of the video works of the alliance blockchain fully utilizes the Ethereum technology in the alliance blockchain, adopts the characteristics of decentralization, security and transparency, freedom from trust, collective maintenance and tamper resistance. In addition to Peer to Peer communication and smart contracts, cryptography, and distributed interstellar file system storage content, video media resource data is stored in the alliance blockchain in such a way as video ID Hash encoding. The natural defect that the blockchain cannot store large amounts of data when storing data is solved in this system by a distributed storage method such as the interstellar file system. The registration and preservation of video media resources and personal (short) video media resources have good application value.

Acknowledgments
This work was financially supported by the Key Research and Development Program of Zhejiang Province, China (Grant No.2019C03138).
References

[1] Juster H R and Ortega-Peluso C A 2019 A media campaign to increase health care provider assistance for patients who smoke cigarettes Preventing Chronic Disease 1 (16) 100-105.

[2] Luby J and Kertz S 2019 Increasing suicide rates in early adolescent girls in the united states and the equalization of sex disparity in suicide: The need to investigate the role of social media JAMA Network Open 2 (5) 23-26.

[3] Arneliwati A P 2019 The effectiveness of health education using audiovisual media on increasing family behavior in preventing dengue hemorrhagic fever (DHF) Enfermeria Clinica 1 (29) 11-21.

[4] Aplin J J and White K 2019 Growth and metabolism of non-Saccharomyces yeasts isolated from Washington state vineyards in media and high sugar grape musts Food Microbiology 10 (77) 1122-1125.

[5] Ross P and Cross R 2019 Rise of the e-Nurse: The power of social media in nursing Contemporary Nurse 1 (55) 2-3.

[6] Haiying M and Elmo X 2020 Blockchain-based mechanism for fine-grained authorization in data crowdsourcing Future Generation Computer Systems 1 (106) 104-106.

[7] Kuo T and Kim J 2020 Privacy-preserving model learning on a blockchain network-of-networks Journal of the American Medical Informatics Association: JAMIA 27 (3) 15-25.

[8] Mohammad R and Shui Y 2020 Blockchain for secure location verification Journal of Parallel and Distributed Computing 1 (136) 51-60.

[9] Yazdinejad A and Srivastava G 2020 Decentralized authentication of distributed patients in hospital networks using blockchain IEEE Journal of Biomedical and Health Informatics 1 (5) 2522-2529.

[10] Tith D and Lee J 2020 Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability Healthcare Informatics Research 26 (1) 159-165.