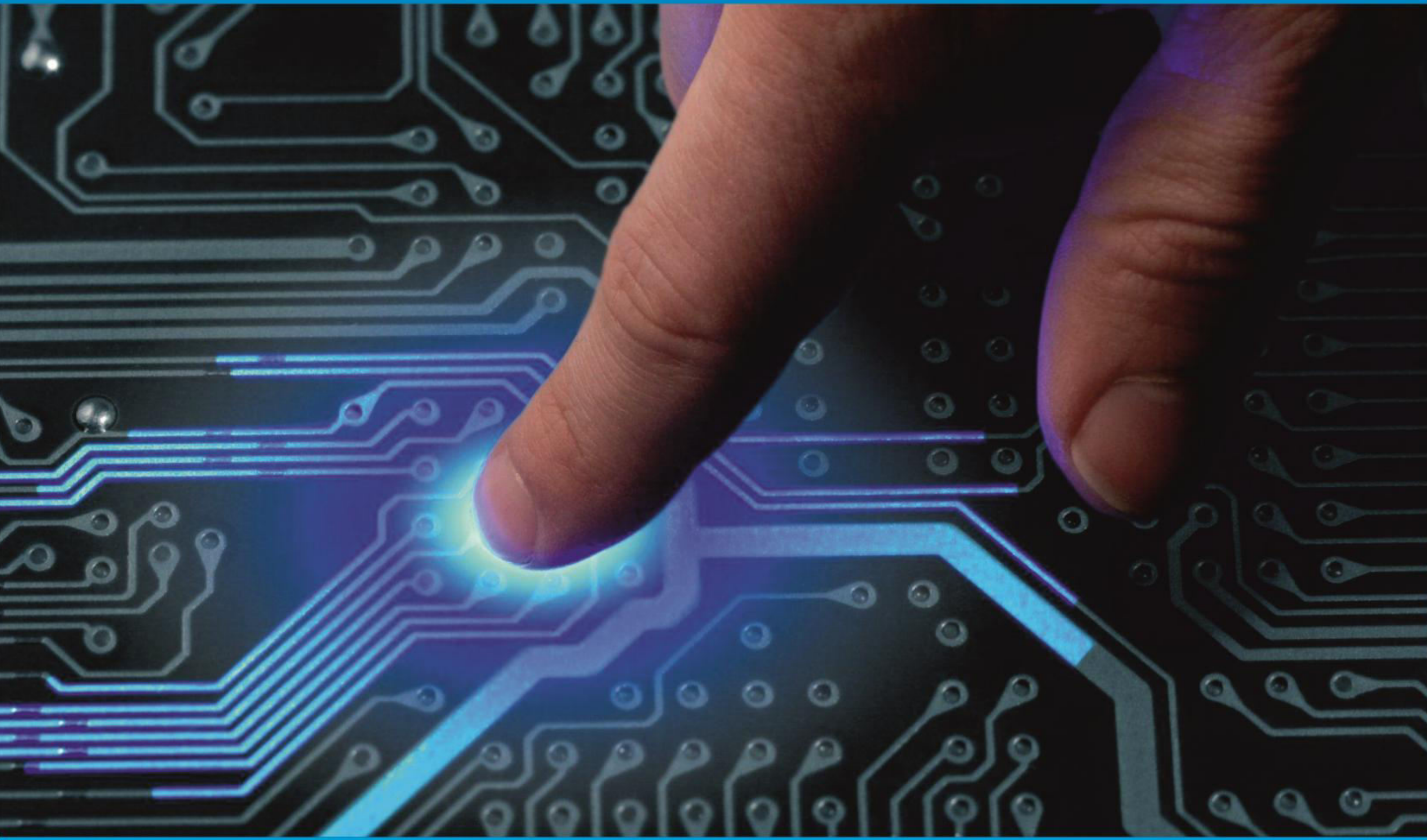
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.488 |

|| Volume 9, Issue 4, April 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0904136 |

A Review on Video Integrity Maintenance Systems

Mahima Gaikwad, Gauri Suryawanshi, Sayali Jadhav, Prof. Vikas Maral

Department Computer Engineering, KJCOEMR, Pune, Maharashtra, India

ABSTRACT: Videos of become highly prevalent due to the increase in the number and the affordability of camera sensors across the world. The main reasons for utilization of cameras is through the use of surveillance purposes. The cameras can effectively record the video of a particular area that can be effectively utilized for the purpose of providing surveillance to that particular area. The surveillance videos are highly useful in the case of a mishap such as a theft or robbery and can be used to identify the criminals easily. These videos are highly useful for the purpose of enabling effective justice in the form of evidence that can be incriminating for the perpetrators. But due to the increase in the number of tools and other software's that are utilized for enabling and effective tampering of forgery of the videos there is a need of an effective approach for maintaining the integrity of the videos. Therefore a number of researches on the video integrity paradigm were analyzed this approach to achieve our methodology based on AES encryption and the Distributed Blockchain Framework which will be discussed in detail in the upcoming editions of this research.

KEYWORDS: Blockchain, Bilinear Pairing, and Advanced Encryption Standard.

I. INTRODUCTION

The increase in the video surveillance across the world has been attributed to the fact that the video capturing approach has been significantly improved in the past few years. There has been considerable improvement in the capturing technologies which has been significant in the overall development of image and video based implementations. There are increasing number of camera based smartphones that have been proliferating in the common public. All the smartphone that have been manufactured in the past decade are equipped with an image and video capture sensor. This leads to a large market for image and video capturing sensors across the world.

The increase in the number of users, leads to an increased demand in that particular commodity. This has led to the industry corresponding to the increase in demand by ramping up the supply effectively. The increase in the supply allows the manufacturing to mass produce these sensors which leads to increased margins and the significant reduction in the price which leads to increased consumption. The reduction in the prices due to the mass production of these sensors led to the increase in the researches being performed on this paradigm. The increased researches have been considerable in the overall improvement in the methodology and the effective realization of a cost effective approach.

The improvement in the affordability of such devices led to the increased usage of cameras in home monitoring devices, Closed Circuit Television Systems, On-board Dashcams etc. The widespread use of such devices being used for constant surveillance has been effective in reducing the incidences of mishaps such as break-ins and other malicious activities. The presence of any type of monitoring deters any future attacks or intrusions effectively. This also allows the law enforcement agencies to effectively counteract any criminal activity and provide surveillance to the city and improve the security effectively. The car or vehicle Dashcams can allow for the effective monitoring of the driving conditions and provide insight to any mishaps that take place on the vehicle.

The video footage is highly useful as it can be considered as an evidence in the court of law. These videos provide incriminating evidence that can cause inconceivable evidence against the perpetrators performing the criminal activity. This makes it a highly useful and indispensable technique for effective security and privacy that can be implemented in an extremely cost effective manner. This kind of security is also a form of passive security that ensures that the presence of the camera would suppress the thief or the robber and reduce the incidence of these problematic scenarios significantly.

But due to extensive research into image processing and video editing, this has led to an increased number of tools and software that has been utilized for the purpose of forging videos and images. These techniques are highly accurate as they can effectively and very accurately provide realistic forgeries that can fool even a trained eye. These tools are highly proliferated and are available for a large number of people. This leads to a lot of forced videos that can be problematic to deal with. This undermines the video as an effective tool for providing justice. Therefore an approach for an effective technique that utilizes the videos and effectively maintains integrity of the videos against forgeries is the need of the hour. for this purpose a collection of researchers have been effectively outline in this research article which has been useful for achieving our approach for video integrity maintenance through the use of the distributed blockchain platform which will be elaborated in the upcoming editions of this research.

This literature survey paper dedicates section 2 for analysis of past work as a literature survey, and finally, section 3 concludes the paper with traces of future enhancement.

II. RELATED WORKS

Rong Wang et. al. [1] proposed a video surveillance system dependent on the approved blockchain (BC) and edge computing. The system consists of three parts: the physical layer, the data service layer, and the application layer. The physical layer is a data acquisition layer that provides a local area network for gathering all sorts of data through the self-organization of different wireless sensor nodes and cameras. A data storage layer comprising BC and edge computing is the data service layer. It is used to gather data and to provide those who do not have computing power. The Data Application Layer consists of an IPFS and a monitoring center for storing and querying files. The files are uploaded via the agent gateway from the physical level to the monitoring center cache. The storage layer is in charge of the storage of various cache data and the continuous collection of BC data. The framework uses valid blockchain, edge editing, IPFS technology, and CNN. The blockchain approved characteristics such as no tampering, security encryption, and fault tolerance, ensure system robustness and reliability. Huge video data storage is done by utilizing the IPFS storage service. The CNN is utilizing to track in real-time.

Mohammed Hazim Alkawaz et. al. uses a double compression method to test the integrity of a video. During checking of a video that is tampered with and not tampered with, it shows a different significant result. Several tests were performed during this research. This technique was tested with data collected from other sources, as well as white noise. By using this technique, authors can guarantee the integrity of digital video which plays such an important role as evidence or proof in a particular situation [2]. The system is tested using black noise that passes through an online source. Black noise is a change that professionals have already made. The system also attempted a white noise generated by the developer to analyze the results with black and white noise. Advanced systems are used to detect tampering by either inserting frames, deleting frames, or simply deleting.

Ge Ge et. al. recommends a key framework of video surveillance that depends on identity cryptography algorithms. In the presented scheme the SM9 identification cryptographic algorithm is the asymmetric cryptographic algorithm for identity verification, the synchronization cryptographic algorithm for data encryption is the SM4 algorithm, and the data integrity algorithm [3]. The SM4 is encrypted and transmitted by a balance encryption algorithm. It is difficult to properly decode the ciphertext data and recover the video information if the intruder intercepts the video data and even if there is no symmetric key. Furthermore, video surveillance data include real-time performance and a huge amount of data, which in turn helps to analyze and ensure the relevant rules of ciphertext data. Therefore, it is difficult to carry out attacks like replay and hijacking. The system's key recipient identity and a public key is encrypted and then transferred, and the steps of key creation, storage, and decryption is carried out on the hardware and modified accordingly. The key is safe until the attacker receives the decryption algorithm and the private key.

Aditya Dhiran et. al. briefly explains how cryptography and blockchain technology can be utilized to detect video fraud and discusses a possible way to implement it. Despite advancements in technology, the problems associated with video fraud persist and there is no specific solution to this problem. So, this research attempted to solve this major problem by using blockchain technology and provided a prototype model. To be more effective, this can be applied on a big scale. A blend of cryptography and blockchain is the suggested prototype platform. For protection and video hash generation[4], many algorithms, such as MD5 and AES, are used. Each node contains a video hash, as well as the previous node's hash that functions as a blockchain.

Guangqi Liu et. al. introduced a method of video forensics that depends on hashtagging and sources of integrity using hash computing and multiple digital watermarks[5]. The studies contain two components: the hashing algorithm design and the development of numerous techniques of digital watermarking, the second components is the decision reliability and honesty of video sources. To ensure the authenticity of video data hash consistency and numerous watermarking methods are utilized to check the video file quality.

Swadhin Thakkar et. al. introduced a novel technique of implementing a highly secure communication layer by utilizing a powerful combination of steganography and cryptography. The presented framework encrypts a secret message using secure encryption algorithms and distributes it over a wide bandwidth utilizing spread spectrum techniques. Then, it is combined into the coverage without affecting the precision of perception, since the amount of information encoded is smaller than the perception threshold and is considered noise. The original video is accessible for the recipient to successfully retrieve the secret message[6]. This document achieves an additional layer of data authentication and integrity validation security by adding a hash-based message authentication code (HMAC) module to the message. Next, the authors analyze the effectiveness of the presented technique against various detection, modification, and destruction attacks. The proposed combination of methods demonstrates better immunity to these attacks while maintaining a private and confidential connection.

Dominik Danko et. al. suggested ways to exploit the idea of blockchain to boost video credibility and detect drone-captured tampered images. This idea can be embodied by storing a video frame on the blockchain. This makes the video frame irreplaceable. It cannot be changed by anyone and can be utilized as evidence for theological purposes. The video frame is, however, too wide to be put on the blockchain, so the video frame hash was placed on the blockchain[7]. These hashes are unchanged and can be used later to validate a video. To avoid adjustments during data transmission, it is sent straight from the IoT device to the blockchain. The framework presented was implemented using Hyperledger as the blockchain technology in a real setup. Experimental studies have shown that, once the required video resolution is chosen, the concept is promising and functional.

Yena Jeong et. al. suggested a blockchain-based framework to reasonably show if the video management system is well-organized. Besides, it limits leakage and unauthorized viewing by the internal administrator. Videos recorded from IP cameras are stored in IPFS by a private blockchain network of encrypted and trusted administrators[8]. The video decryption key is not stored in the block but is stored in a database of specific nodes with the option to verify the collection so that internal managers cannot verify the decryption key. Besides, when a person who wants to watch a video receives approval from the blockchain network or the internal manager monitors the video on the screen, the internal manager executes the chain code to export the video. In the string code API, the license is generated using the decryption key, reading period, and browse number. In the proposed blockchain framework, the video surveillance system can securely manage videos from outsiders and internal administrators. Also, if the video export is handled well, it is possible to manage the recording of the purpose.

Seyed Yahya Nikouei et. al. proposed a new way to exchange indexing and feature data between nodes in an intelligent monitoring system that takes advantage of the edge fog cloud computing simulation. Features take out from the edge video frames are forward to the fog node through a secure channel in this classification architecture and features are added to the index table with background for quicker and more focused queries[9]. The communication amongst the nodes located at the edge, fog, and cloud surface is protected by smart contracts that take benefit of the hash values of the index table to develop the next block in the blockchain network. A hybrid RSA-AES encryption method was utilized to protect the extracted properties of objects interested in the transfer of fog from the edge nodes before the new block is extracted. Once the new block mine is created, the entire network will be synchronized with the new information. Using a web service, the cloud can safely access the index table and query information from one of the nodes. Experimental findings confirm that the approach proposed is very head-to-head, making it a promising and feasible solution for video query applications for real-time surveillance.

Sarala Ghimire et. al. proposed a new video IVM approach based on the blockchain of centralized video data. The blockchain contains HMAC and ECC algorithms in the proposed system for hashing and encrypting video parts and keys, respectively. Moreover, the VICs created by the encrypted output-input are stored in a chained time-series manner. Video segment validation is checked when the saved integrity code is compared with the newly generated video code during validation[10]. Experimental findings indicate that the identification of the PC environment and embedded systems are more robust than other traditional methods.

Regio A. Michelin et. al. provide a framework to ensure the data integrity of stored videos and allow authorities to verify that video content has not been tampered with. The proposed framework follows the three-tiered architecture. Surveillance cameras are considered reliable and are provided with a detection layer. Gateways are also trusted and are deployed in the transport layer and responsible for running the video, maintaining the blockchain-based video integrity. After all, the authors have incredible third-party storage tires where they can use any suitable storage system[11]. To do this, they use the Interplanetary File System Network (IPFS) to store surveillance videos. The presented scheme uses simple blockchain technology to help store video metadata as a blockchain transaction and verify video integrity. The assessment shows that the overhead caused by using blockchain to generate transactions causes a slight delay of a few milliseconds.

Pengpeng Yang et. al. introduced an effective method for analyzing video file containers, which allows to characterize the identified manipulation and provide a description of the result. The proposed method is based on decision trees, an irregular learning method used for classification problems in many areas of signal processing. Their key feature is the ability to break a complex decision process into a set of simple decisions. The authors have enriched the tool with a reliability reporting framework designed to automatically swap up the container elements that only contribute to the intrinsic variability of the source. Compared to the state of the art, the proposed method, now simply called EVA, offers new legal opportunities, including manipulation software identification, provides additional information related to the history of the source material, such as the original device operating system[12]. The presented framework is very effective because the decision can be made by examining the presence of a small number of features regardless of the length of the video.

III. CONCLUSION AND FUTURE SCOPE

The methodology for effective maintenance of integrity of the videos has been achieved in this approach through the analysis of previous works on this topic. Videos are an integral part of life nowadays as every smart phone as an integrated camera in it. But most of the video files are captured from CCTV cameras that are utilized by various establishment owners and law enforcement agencies to monitor the city as well as the areas around it. This provides an effective security in the form of difference where in a person would not commit a crime in full view of a CCTV camera. But due to the rise in various tools and services that provide effective utilization of editing of the videos to produce forgeries. Therefore the need of video integrity maintenance is very high which has led to the creation of the proposed methodology that utilizes AES encryption and Blockchain Framework which will be discussed in detail in the upcoming editions of this research article.

REFERENCES

[1] Rong Wang, Wei-Tek Tsai, Juan He, Can Liu, Qi Li and Enyan Deng, "A Video Surveillance System Based on Permissioned Blockchains and Edge Computing", 2019 IEEE International Conference on Big Data and Smart Computing (BigComp), 04 April 2019.

[2] Mohammed Hazim Alkawaz, Maran Tamil Veeran, and Husniza Razalli, "Video Forgery Detection based on Metadata Analysis and Double Compression", 2019 IEEE 7th Conference on Systems, Process and Control (ICSPC), 16 April 2020.

[3] Ge Ge, Huamin Feng, Biao Liu, and Junwei Zhang, "Research on Video Surveillance Key Management Scheme Based on Identification Password", 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 27 January 2020.

[4] Aditya Dhiran, Dinesh Kumar, Abhishek, and Anshul Arora, "Video Fraud Detection using Blockchain", 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 01 September 2020.

[5] Guangqi Liu, Lianhai Wang, Shujiang Xu, Dawei Zhao, and Shumian Yang, "Video Forensics Research based on Authenticity and Integrity", 2016 IEEE International Conference on Information and Automation (ICIA), 02 February 2017.

[6] Swadhin Thakkar, Kaustubh Shivdikar and Chirag Warty, "Video Steganography using Encrypted Payload for Satellite Communication", 2017 IEEE Aerospace Conference, 08 June 2017.

[7] Dominik Danko, Suat Mercan, Mumin Cebe, and Kemal Akkaya, "Assuring the Integrity of Videos from Wireless-Based IoT Devices using Blockchain", 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW), 09 April 2020.

[8] Yena Jeong, DongYeop Hwang, and Ki-Hyung Kim, " Blockchain-Based Management of Video Surveillance Systems", 2019 International Conference on Information Networking (ICOIN), 20 May 2019.

[9] Seyed Yahya Nikouei, Ronghua Xu, Deeraj Nagothu, Yu Chen, Alexander Aved and Erik Blasch, "Real-Time Index Authentication for Event-Oriented Surveillance Video Query using Blockchain", 2018 IEEE International Smart Cities Conference (ISC2), 04 March 2019.

[10] Sarala Ghimire, Jae Young Choi, and Bumshik Lee, "Using Blockchain for Improved Video Integrity Verification", 2017 IEEE World Congress on Services (SERVICES), 14 September 2017.

[11] Regio A. Michelin, Nadeem Ahmed, Salil S. Kanhere, Aruna Seneviratne and Sanjay Jha, "Leveraging lightweight blockchain to establish data integrity for surveillance cameras", 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 17 August 2020.

[12] Pengpeng Yang, Daniele Baracchi, Massimo Iuliani, Dasara Shullani, Rongrong Ni, Yao Zhao, and Alessandro Piva, "Efficient Video Integrity Analysis Through Container Characterization", IEEE Journal of Selected Topics in Signal Processing (Volume: 14, Issue: 5, Aug. 2020), 08 July 2020.

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details