International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

A Thorough Study on Video Integrity using Blockchain

Nikhil Bhusari[1], Tejaswini Kshirsagar[1], Akash Chandlekar[1], Apurva Borude[1], Kiran Gaikwad[1], Anuja Palhade[2]

[1]Student, [2]Professor,

[1,2]Department of Information Technology, Dhole Patil College of Engineering, Pune, Maharashtra, India

ABSTRACT

There has been an increase in the surveillance of public as well as private areas due to the immense increase in crime. This increase in crime rates has been instrumental in the development of CCTV cameras and other imaging devices for monitoring purposes. This has provided an increased convenience and ease of mind for the businesses as well as residences. The surveillance also provides an effective deterrence against the criminals and their activities. The surveillance footage can be utilized as incriminating evidence against the perpetrator. But the problem with this approach is maintaining the integrity of the video against tampering and other effects. Some techniques and tools can alter a video and change the integrity of the video, while the result is imperceptible to the naked eye. Therefore, the maintenance of the integrity of the video is an extremely necessary component of surveillance devices at cloud or personal storages. The analysis of the related work has been instrumental in achieving our methodology that is based on RSA encryption and Blockchain Platform.

KEYWORD: *Blockchain, Distributed Systems, RSA Asymmetric Encryption*

How to cite this paper: Nikhil Bhusari | Tejaswini Kshirsagar | Akash Chandlekar | Apurva Borude | Kiran Gaikwad | Anuja Palhade "A Thorough Study on Video Integrity using Blockchain" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.796-798, URL: www.ijtsrd.com/papers/ijtsrd38066.pdf

IJTSRD38066

I. INTRODUCTION

In recent years there has been an enormous increase in technological improvements which has led to a similar increase in the number of electronic devices. These electronic devices have been getting increasingly affordable. This has led to an increased number of individuals that are equipped with electronic devices. This has led to an increased amount of research being performed to achieve better electronic devices that can be cheaper and better suited for mass production. The improvements in sensors and other electronic devices have led to the availability of cheap and high-quality equipment.

The advancements have been also focused on imaging approaches and techniques which have been getting better over the years. Smartphones have been one of the most effective in improving imaging techniques and image sensors. The improvements in the imaging sensors and the reduction in their prices have been instrumental in the increased usage of image sensors or cameras for surveillance. These approaches have

Allowed effective and secure implementations of security for the majority of the individuals. There are CCTV cameras that are used for constant surveillance. These applications are useful for enabling effective monitoring of the surroundings.

The CCTV cameras are extremely useful in situations that allow police to spot any illegal activities that are captured in the footage. This captured footage can be utilized as evidence for the criminal activity in the court of law which can turn into incriminating evidence against the criminal effectively. These videos have been used extensively to catch the perpetrator red-handed in the criminal act. This has reduced the number of crimes in areas that have been covered with security cameras.

The most important hurdle when presenting the video in court is that the integrity of the video must be intact for the presentation. The integrity of the video would mean that the video must not be tampered with or edited. This also states the fact that the video is the same as the video captured by the CCTV cameras. This is one of the most crucial aspects as there are techniques that have been developed that can effectively perform editing on a video that can be made with such an accuracy that it is imperceptible to the human eyes. This can be used to effectively tamper with the video and cause a false incident to discredit the perpetrators.

Therefore, the maintenance of integrity is one of the most essential components that validate the video feed of a CCTV camera. For achieving these goals, this research article analyzes previous researches and related works to understand the approaches and their limitations effectively. These researches have been outlined in this paper which has helped us formulate our approach effectively. The future editions of this research will illustrate the methodology in further detail.

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

F. Kharbat [1] narrates that by using artificial intelligence fake videos are created which is becoming more and stronger in recent years. Human faces in a video are replaced with another face by using Generative Adversary Networks (GANs). Many tools are available on the internet to do this kind of video integrity. In the proposed paper Support Vector Machine (SVM) regression is used to detect deepfake videos. Feature-point detectors such as HOG, ORB, BRISK, KAZE, SURF, and FAST algorithms are used to extract features for the SVM classifier. Thus in the proposed paper SVM can be effectively used to detect false videos by using feature-detector-descriptors.

Q. Wan explains a serious effort has been made to develop video forensic technology because digital videos have been extensively used for security purposes. Forensic video analysis faces two problems such as finding evidence present in a video and the second one is to authenticate the original video source. [2] To evaluate video altering and tampering an automatic jump-cut detection system is used and Human Visual System is used when the human eye may not be able to detect the video altering and tampering but this system does. The main aim is of the proposed paper to detect whether information has been maliciously modified or erased from the original video.

G. Liu states in recent years there has been continuous development in the field of computer forensics and judicial authentication technology. In recent times the monitoring system is quite popular almost everywhere there are camera video is collected. [3] Video forensics is becoming a key research topic but it faces many challenges such as computing power and high compression factor so there is a lot of improvement to be made in the field of video forensics. It requires technology such as authenticity identification and integrity evaluation. In the proposed system they have used a hash algorithm and multiple digital watermarking methods to verify the integrity of the video file.

R. Michelin explains to support criminal investigations the video footage produced by surveillance cameras is important evidence. The video can be collected from the public as well as private surveillance systems. Surveillance cameras are mostly used for safety, security, and traffic monitoring, and law enforcement. This camera can be located in different places such as shops, malls, and offices purposes. Information collected from the untrusted video sources may raise the issue regarding integrity.[4] Thus the proposed paper implements allow an authorized person to validate whether video footage has tampered with or not. The researcher used lightweight blockchain technology to store the video metadata as blockchain transactions can help in validation of video integrity.

J. Yao describes in multimedia, network, and communication technologies video quality assessment (VQA) plays a very important role. [5] Three main categories of VQA Full-Reference (FR), Reduced-Reference (RR), and No-Reference (NR) quality assessment. In the proposed paper they have implemented the NR VQA metric based on the bitrate, video contents. They have tested the system on 150 distorted videos from the LIVE video database. NR VQA methodology focuses on the video distortion issued by transmission and rarely consider the video contents. To serve better video transmission real-time guides the parameter setting, and optimizes the algorithms is used. A good VQA metric evaluates their qualities automatically and accurately,

Y. Ye focuses on detecting object alteration in video sequences that carrying crucial semantic information. Authenticity and integrity of the video sequence are the points required for the application. The proposed paper implements the tampered objects in video sequences with a moving camera for capturing the moving background.[6] Thus global motion estimation and alignment used video frame feature points extraction algorithm, video frame alignment and grouping algorithm, video frame feature points matching algorithm, video frame global motion estimation algorithm for better results.

M. Alkawaz explains the integrity of digital media has been questioned in many ways. The integrity of digital video can be disturbed in many ways this integrity videos cannot be seen with naked eyes. The double Compression method is used to determine whether a video has tampered with or not. To check any frame insertion digital Video can be analyzed frame by frame. [7] The input video is converted into a grey-scale to improve the efficiency of processing each frame. Each frame will be compared with one before and after frame to check the tampering occurs in the video. The double compression method is used and it shows effective result

D. Danko states video plays a very important material to interrogate a crime and to solve a case. In recent times blockchain technology has drawn attention in various fields. Thus the proposed paper implements blockchain technology to verify the authenticity of a video captured by using IoT devices. Thus the hashing techniques use to observe the tampering of the video. Video forgery techniques are used in the proposed paper. [8] To tamper video Advanced video editing tool is used which can easily tamper the video. Thus by generating the hash values for individual frames before it is sent to the cloud. To evaluate performance the system has been tested on a Raspberry Pi with different quality videos.

V. Barannik aims to analyze information security. There are a lot of problems in the information security of video information resources in aerial surveillance systems. To ensuring speed of transfer of multimedia data statistical coding codes of variable length is applied based on data processing. [9] The acceptable quality of image recovery the coding provides a high extent of compression. A dynamic redundancy existence results in structural coding technology. Thus by using encoding technology for the structural code formation the threat of data integrity reduces.

M. Mathai explores several forensic related issues arise for many security concerns. There is an increase in the number of sophisticated forgery tools manipulating a video has become an easy task nowadays. For different media content, many forgery detection algorithms have been developed. [10]The unsupervised video forgery detection and localization technique implemented in this paper ensure the

use of the statistical moment features and normalized cross-correlation factor. The features from the prediction-error array of each image are calculated for each frame-block. The technique localizes the duplication not only at frame level but also at region-level.

A. Alimpiev narrates in the recent time and coming days there is a huge gain in wide application transfer multimedia files in the one-direction video monitoring systems and two-way transmission in video conferencing systems. In modern imaging methods, some disadvantages were observed. [11]In the proposed paper the researcher developed the concept of integrity with the redistribution of statistical codes. Thus the proposed paper applies the code generation feature for stream synchronization that makes sure localization of error propagation within the transforms due to this there is an increase in integrity.

Y. Jin defines a video surveillance system combination of computers, networks, and communications. [12]Video surveillance systems are widely used in many fields such as education, transportation, and industry due to distributed architecture, parallel image processing, and ease of installation and expansion. It faces many challenges such as low quality, big delay of video data transmission which can cause data integrity. To overcome this kind of problem the author develops an Unmanned Aerial Vehicle (UAV) cluster. In Unmanned Aerial Vehicle (UAV) cluster series of optimization algorithms and scheduling, strategies are developed.

III. CONCLUSION

The paradigm of video integrity is one of the most essential needs of the hour. The increase in surveillance and other video monitoring approaches have been devised to achieve effective security in malls, shops, and other public places. The videos offer an effective solution for remotely monitoring an area effectively. The video is also an effective source of evidence in various scenarios and can also be utilized in different fields for monitoring purposes. The paradigm of video editing is also gaining traction wherein the videos can be tampered with and doctored with very high accuracy. Some tools are effective in achieving imperceptible tampering of the video that can be deceiving and can be used to wrongfully convict an innocent person. Therefore, an effective technique for evaluating the integrity of the video is being formulated Blockchain and RSA asymmetric encryption. The formulated idea will be reflected in our future researches.

REFERENCES

[1] F. F. Kharbat, T. Elamsy, A. Mahmoud and R. Abdullah, "Image Feature Detectors for Deepfake Video Detection," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1-4, DOI: 10.1109/AICCSA47632.2019.9035360.

[2] Q. Wan, K. Panetta, and S. Agaian, "A video forensic technique for detecting frame integrity using human visual system-inspired measure," 2017 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, 2017, pp. 1-6, DOI: 10.1109/THS.2017.7943466.

[3] G. Liu, L. Wang, S. Xu, D. Zhao, and S. Yang, "Video forensics research based on authenticity and integrity," 2016 IEEE International Conference on Information and Automation (ICIA), Ningbo, 2016, pp. 1223-1226, DOI: 10.1109/ICInfA.2016.7832006.

[4] G. Liu, L. Wang, S. Xu, D. Zhao, and S. Yang, "Video forensics research based on authenticity and integrity," 2016 IEEE International Conference on Information and Automation (ICIA), Ningbo, 2016, pp. 1223-1226, DOI: 10.1109/ICInfA.2016.7832006.

[5] J. Y. Yao and G. Liu, "Bitrate-Based No-Reference Video Quality Assessment Combining the Visual Perception of Video Contents," in IEEE Transactions on Broadcasting, vol. 65, no. 3, pp. 546-557, Sept. 2019, DOI: 10.1109/TBC.2018.2878360.

[6] Y. Yao, Y. Cheng, and X. Li, "Video Objects Removal Forgery Detection and Localization," 2016 Nicograph International (NicoInt), Hanzhou, 2016, pp. 137-137, DOI: 10.1109/NicoInt.2016.30.

[7] M. H. Alkawaz, M. T. Veeran, and H. Razali, "Video Forgery Detection based on Metadata Analysis and Double Compression," 2019 IEEE 7th Conference on Systems, Process, and Control (ICSPC), Melaka, Malaysia, 2019, pp. 190-193, DOI: 10.1109/ICSPC47137.2019.9067977.

[8] D. Danko, S. Mercan, M. Cebe, and K. 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), Monterey, CA, USA, 2019, pp. 48-52, DOI: 10.1109/MASSW.2019.00016.

[9] V. Barannik, S. Podlesny, A. Krasnorutskyi, A. Musienko, and V. Himenko, "The ensuring the integrity of information streams under the cyberattacks action," 2016 IEEE East-West Design & Test Symposium (EWDTS), Yerevan, 2016, pp. 1-5, DOI: 10.1109/EWDTS.2016.7807752

[10] M. Mathai, D. Rajan, and S. Emmanuel, "Video forgery detection and localization using normalized cross-correlation of moment features," 2016 IEEE Southwest Symposium on Image Analysis and Interpretation (SSIAI), Santa Fe, NM, 2016, pp. 149-152, DOI: 10.1109/SSIAI.2016.7459197.

[11] A. Alimpiev, V. Barannik, S. Podlesny, O. Suprun, and A. Bekirov, "The video information resources integrity concept by using binomial slots," 2017 XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), Lviv, 2017, pp. 193-196, DOI: 10.1109/MEMSTECH.2017.7937564

[12] Y. Jin, Z. Qian and W. Yang, "UAV Cluster-Based Video Surveillance System Optimization in Heterogeneous Communication of Smart Cities," in IEEE Access, vol. 8, pp. 55654-55664, 2020, DOI: 10.1109/ACCESS.2020.2981647.