IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

Discovering Video Integrity through Blockchains

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

Department of Computer Engineering, KJCOEMR, Pune, India

ABSTRACT: Video surveillance has been increasing in popularity in the recent years. This is due to the advancements in the sensor technology that has led to increased affordability of cameras and other video capturing approaches. This has led to a large number of organizations and individuals utilizing the video surveillance to deter criminals from committing the crime. This evidence can be utilized in court to facilitate the justice department effectively for investigation. As there have also been improvements in the approaches to tamper and edit the video footage effectively, there is a need to achieve video integrity to effectively prove the authenticity of the footage. For this purpose, this research article has been effective in achieving video integrity evaluation through the utilization of the distributed Blockchain framework. The presented technique utilizes Advanced Encryption System along with Blockchain framework to achieve effective and useful video integrity evaluation. The experimental outcome has been effective in demonstrating the superiority of the proposed approach.

KEYWORDS: MD5 Hashing, AES, Distributed Blockchain Framework, Video Integrity.

I. INTRODUCTION

Image capture Technologies have come a long way is the first introduction of a camera. The first useful camera was very large and you should take very low-resolution images. The cameras have improved since then and a lot of it has been moved over to digital format from the traditional film format. The digital format is highly useful for the purpose of storage and retrieval through electronic means easily. The cameras even though had become digital were highly expensive and difficult to procure.

Over the years the cameras have become cheap. This is due to the improvements in the technology which is led to a new and improved version of the camera. The digital cameras utilize light sensors to achieve an effective image of the target. The newer sensors capture more light in detail at the fraction of the cost in ownership as well as power consumption. The image sensors have improved drastically which has led to the inclusion of a camera in almost every smartphone that is available in the market. This has also lead to an increase in the number of closed-circuit television for CCTV cameras that can monitor a particular area effectively.

CCTV cameras and other surveillance equipment it is highly useful to reduce the number of attacks or intrusions at a particular establishment or their houses. These are highly useful in terms of an intrusion or theft that is performed by an individual that is captured on the CCTV cameras. This leads to the utilization of video evidence in a judicial case. The frequency of videos being utilized as evidence in a courtroom is increasing every single day.

This is due to the fact that there are a large number of techniques that are utilized for the purpose of enabling highly seamless editing of videos. These edited videos or tampered videos can lead to a wrongful conviction or can cause a lot of problems. There are tools and software that are available for the purpose of enabling effective editing on videos that can be highly difficult to detect and quantify to maintain the integrity of the image. The implementation of artificial intelligence for the creation and editing of these videos and images has been effectively useful for achieving highly realistic and extremely deceiving fake videos.

Therefore there is a need for an effective technique that can be highly useful in the detection of the integrity of the video file. There are a number of approaches that have been used to perform the detection of any manipulation on the video but most of these approaches have been inconsistent in their implementation leading to low accuracy and high computational and time complexities. Most of these approaches do not provide enough security for the video that is utilized for the purpose of video integrity evaluation.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

Thus in this research article, the proposed methodology utilizes the distributed framework of the blockchain platform for the purpose of achieving effective video integrity management. The blockchain platform is one of the most effective and useful approaches that can implement a tamper-proof mechanism for maintaining the integrity of the video. The blockchain approach utilizes hashing algorithm to determine the hash of the video block and store them in a sequence by combining the previous and the current hash key into the head.

The video files are also encrypted effectively for the purpose of safeguarding the data inside the videos from any individual or an attacker. The videos are encrypted through the utilization of the Advanced Encryption System approach which provides effective security through the implementation of distraction and diffusion cryptographic approaches. Once the encrypted data is being converted into the blockchain platform the time delay approach is utilized for the purpose of determining any tampering or manipulation of the video has been performed. This approach has been further elaborated in much detail in the upcoming sections of this research article.

Section 2 of this research paper works on past work under the name Literature review. Section 3 explains all the methodology in detail, whereas section 4 works on the evaluation of the results. Finally, Section 5 concludes this paper and leaves behind some traces of future work.

II. LITERATURE REVIEW

V. Barannik states that there has been an increase in the number of remote monitoring approaches to the utilization of video surveillance. Due to this, there has been an increase in the information that is stored in the form of video without any effective approach to utilize this information easily. Therefore doctors in this approach have proposed utilization of contour information for the purpose of achieving syntactic description of each of the frames [1]. The approach has been quantified through the utilization of extensive experimentation that has resulted in highly useful results.

G. Liu narrates that continuous and effective improvement in computer forensics has been highly useful in the terms of achieving authentication on a judicial platform. Computer forensics is a highly useful approach that effectively improves the quality of evidence that is collected. Therefore there is a need for an effective technique to determine the authenticity and integrity of a video as there has been a large number of video surveillance improvements in recent years [2]. Therefore to effectively utilize the video for the purpose of extractive integrity and authenticity the authors proposed the utilization of multiple digital watermarks through the utilization of hash algorithms.

J. Y. Yao explains that the process of assessment of video quality is one of the most important for the purpose of enabling effective communication networks and multimedia technologies. These are some of the most integral and developing approaches that have garnered public attention significantly [3]. The quality of the video is an essential concept that needs to be improved significantly to achieve improvements in the video content. Therefore the authors in this Publication have proposed their combination of visual perception and bitrate-based video quality assessment to provide the video content effectively.

M. H. Alkawaz expresses that in recent years there have been large advances in the paradigm of media especially video surveillance and editing. This leads to a lot of forgeries and video-based editing that can be highly misleading for an individual. Therefore the authors in this approach have proposed the utilization of double compression and analysis of the Metadata to detect any forgery on the video files with very high accuracy [4]. This enables the authors to effectively identify if there has been any tampering done on the video with relative ease. The main limitation noticed in this approach is the increased computational complexity that is observed.

V. Barannik elaborates on the various approaches that have been enabled through the implementation of the internet platform such as cloud storage and video streaming services for video calls. These approaches are found large scale adoption from the users as well as large organizations [5]. But these information streams can be a target of an effective attack which can render the integrity of the information system in Jeopardy. Therefore the authors have proposed the utilization of BIT errors for the purpose of detection of any cyber-attack in the information stream.

T. Song discusses the paradigm that has been facilitated a considerable leakage of information from television sets and personal computer monitors. This is due to the detection of the electromagnetic waves that can be detected using an antenna

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

for the purpose of eavesdropping. Therefore to effectively achieve are a highly useful and effective technique to counter this eavesdropping is researched upon by the researchers in this study [6]. The authors have proposed the utilization of information recovery rate and the lead digital video signal to model it as a function of SNR of the leaked video.

F. F. Kharbat introduces the concept of deep fakes or the fake videos that are generated through the implementation of artificial intelligence. These fake videos are highly problematic as they are becoming increasingly realistic and extremely convincing [7]. Therefore there is a need for the detection approach that can identify any deep fake video through the utilization of image feature detectors effectively. The authors in this research have proposed the utilization of support vector machines to fulfill the purpose of classification effectively.

D. Danko states that video evidence of any crime committed is highly useful for the purpose of enabling effective justice and resolution of any dispute. Video surveillance has increased in recent years which has led to a large number of videos that have been utilized for this purpose [8]. Therefore there is a need to measure the integrity e of the video effectively and for this purpose, the author propose is the implementation of the blockchain distributed Framework for enabling the integrity of the video.

M. Mathai narrates that there has been an increase in the accuracy of video editing software that has enabled effective and useful manipulation of videos easily. Manipulated videos are highly detrimental to society as they cause a lot of problems and differences [9]. Therefore for improving the security of the videos and reducing this type of occurrences authors have proposed the utilization of moment features and its normalized cross-correlation through localization for the purpose of video forgery detection.

V. Yatskiv explains that there is an increase in the video surveillance capabilities that are being utilized in a large collection of different fields. This video surveillance is one of the most useful security enabling features in a lot of implementations. Therefore there is a need for an effective technique that can improve the integrity of these videos and improve the security [10]. For this purpose, the authors and proposed the utilization of the blockchain framework as it is highly tamper-proof and can maintain the integrity of the video file through hash formation effectively.

R. A. Michelin expresses that there is an increased use of surveillance cameras for the purpose of monitoring and providing security for the owners of the establishment of all the government agencies. This is highly significant as it reduces the occurrence of illicit activities significantly [11]. But most of these approaches have been marred with inconsistencies and tempering. Therefore the authors in this Publication propose the utilization of the blockchain framework to enable effective security and eliminate tempering on the video files.

Q. Wan elaborate on the concept of capturing video for the purpose of providing surveillance and improved security to establishment and homeowners. This increased security is highly useful in preventing attacks and theft on the establishment of the house [12]. These video surveillance techniques are being used increasingly for enabling effective security in various different fields nowadays. With the increased use there is also a need for an effective video forensic approach that can determine the integrity of the frames effectively. Therefore the researchers in this approach have proposed the utilization of a human visual system-inspired technique for the purpose of integrity analysis of videos for forensic analysis.

A. Alimpiev discusses the widespread use and implementation of video-based surveillance and analysis. There has been increased use of various video surveillance techniques that have been effective in a varied application in recent years. The improvement, in the image capturing technology and a significant increase in the affordability of these approaches, has led to the significant involvement of the video surveillance approaches in recent years. But due to the prevalence of Different techniques that enable seamless editing of videos which leads to various tampering that needs to be detected to analyze the integrity of the video [13]. For this purpose, the authors in this approach have utilized fixed-length code through the use of a floating coding scheme to detect any structural features that are implemented through the encoding of the bitstream.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

III PROPOSED METHODOLOGY

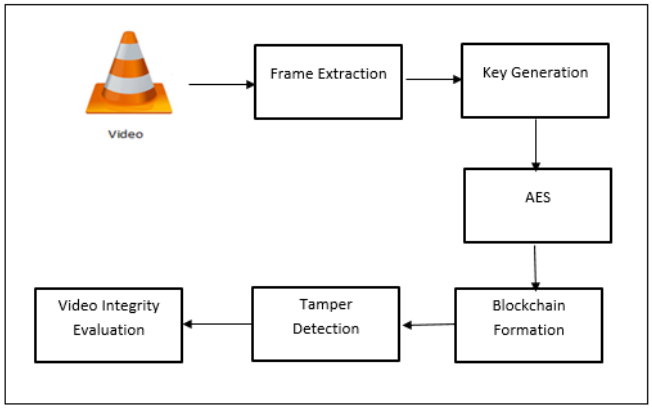

Figure 1: System overview Diagram

The presented technique for the purpose of Video Integrity evaluation through the use of distributed blockchain platform is illustrated in the fig. 1 given above. This approach has been elaborated in a stepwise manner in the section given below.

Step 1: Video Input and Frame Extraction – The proposed methodology utilizes an interactive Graphical User Interface to allow the user to provide the video as an input to the system before uploading to the third party storage. The input video is selected using the file picker and provided to the system. The java based approach utilizes Xuggler API to extract the individual frames on the said time slot from the video file. These extracted frames are temporarily stored in a folder for further processing in the subsequent modules.

Step 2: Key Generation – The extracted frames are given as an input to this module for the purpose of enabling effective key generation. For this purpose, the input frames are utilized to read the image in the form of bytes. The byte data of the frames is effectively provided for the generating the Hash keys through the use of MD5 hashing algorithm. After the generation of the hash keys, 8 random characters from the hash key are selected to generate a plain block head key. This key is utilized in the next step of the procedure for the purpose of encryption. This key generation process can be elaborated in the Algorithm 1 given below.

ALGORITHM 1: Key Generation

//Input : Frame Bytes in String F_{BS}
//Output: Key K_Y
Function: *keyGeneration*(F_{BS})
1: Start
2: jstr = " ", K_Y = ""
3: ***for*** i=0 to size of F_{BS}
4: jstr = jstr + $F_{BS\,[i]}$
5: ***end for***
6: $MD5_{HK}$=MD5(jstr)
7: REM= $MD5_{HK}$ SIZE MOD 8
8: ***for*** i=0 to K_Y Length < 8
9: i=i+(REM+1)
10: ***if*** (i< $MD5_{HK}$ length)
11: $K_Y = K_Y + MD5_{HK\,[i]}$
12: $MD5_{HK} = MD5_{HK} >> 1$

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

13: ***else***
14: i=0
15: ***end for***
16: **return** K_Y
17: Stop

Step 3: Advance Encryption System – The AES is one of the most secure and widely used implementations of cryptography for networking purposes. This module takes the key generated in the previous step as an input. The key consisting of the 8 characters is divided into two blocks. These blocks are rotated clockwise by the number of characters based on the block index. The ASCII value of the character is extracted and an addup value is added to generate a new ASCII value. This ASCII value is converted to its respective character, so that all the characters from both the blocks are being concatenated to get a single string of 8 characters of 16 bytes. This allows the effective encryption process to be completed and achieves the Block head formation of the blockchain framework.

Step 4: Blockchain Formation and Video integrity– The obtained block head key from the previous step is utilized and concatenated with the next frame's byte string. The resultant string is subjected to the key generation procedure wherein the 8 character key is generated. This key is provided to the encryption procedure for the encryption purposes which results in the creation of the blockhead for that frame. This process is repeated for the nth frame, this is the last frame of the video that provides the nth head key which is also called the Terminal Key. After this the date, time, video name and the terminal key is stored in the database and the video is uploaded to the third party storage server.

A predetermined time is selected for the execution of integrity evaluation approach. The time here refers to the time which can be set to be 3 minutes, 5 minutes, 1 day, two days etc. to any desired value. For every instance, this time threshold is reached, the system automatically downloads the video file from the third party storage and subjects it to the entire procedure once again. This procedure is performed to achieve the terminal key once again. This achieved terminal key is then compared with the one stored in the database. If the key matches then the integrity of the video is intact, if it doesn't match, then there is a lapse in the integrity indicating foul play.

IV. RESULTS AND DISCUSSIONS

The presented technique for the realization of an effective Video Integrity analysis approach has been described in this research paper. The approach has been achieved in the java programming language through the NetBeans Integrated Development Environment. The machine utilized for this purpose is equipped with an Intel i5 CPU assisted by the Windows Operating System along with 6 GB of RAM and 500 GB of storage. The database requirements have been realized through the implementation of the MySQL database server.

The proposed approach has been assessed in detail to extract its performance through the execution of the encryption and decryption of blockhead key. The experimental procedure is detailed below.

ENCRYPTION AND DECRYPTION TIME PERFORMANCE

The proposed approach utilizes the Advanced Encryption System to perform encryption and decryption. The performance of the presented technique's implementation of the AES approach needs to be quantified. This is due to the fact that the encryption and decryption is one of the most important factors in the determination of the performance of the approach.

For this purpose, the methodology has been subjected to the encryption and decryption execution on the increasing number of frames. Therefore the time elapsed for the performance of the encryption and decryption is listed in Table 1 below.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

Number of Frames	Encryption Time in Milliseconds	Decryption time in Milliseconds
10	2	2
20	14	16
30	30	31
40	45	51
50	50	52
60	62	59
70	64	66
80	75	76
90	75	74
100	95	99

Table 1: Encryption and Decryption time performance

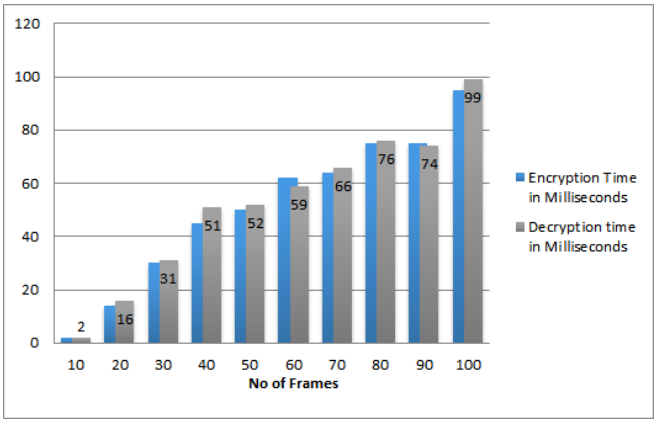

Figure 2: Encryption and Decryption Time

The figure 2 given above illustrates the time elapsed for the encryption and decryption process. It can be noticed that the encryption and decryption processes is not directly proportional to the number of frames. This outcome is depicted in the figure and table given above. This indicates that the encryption and decryption module using AES approach has been accurately implemented and achieves its goals. This outcome is acceptable due to the first time implementation of such an approach.

V.CONCLUSION AND FUTURE SCOPE

The proposed methodology for the purpose of effective video integrity evaluation has been outlined in this research article. Due to the increase in the use of effective and highly professional video editing approaches, it becomes highly difficult to achieve the authenticity of the video. Therefore, the technique presented in this approach utilizes the video input in different formats. The frames in this video have been effectively extracted in this step by java program of the proposed system. These input frames are effectively utilized for the purpose of generating the hash key through the MD5 hashing algorithm. This hash key is utilized for key generation. This key is then provided to the Advanced Encryption System for the purpose of encryption. The encrypted data of the video is to prevent any misuse of the data. This encrypted data is utilized for the purpose of enabling an effective and useful security to the data. This is achieved by creation of the Blockchain that generate a terminal key that are useful for the integrity evaluation. The integrity evaluation has been

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907013 |

performed through the use of the time delay technique effectively. The experimental results achieved have been effective in demonstrating the capability of the approach accurately.

In the future this methodology can be used to develop an open API, which can be used by many developers to achieve the same on any video repositories.

REFERENCES

[1] V. Barannik, Y. Ryabukha, and A. Krasnorutskyy, "Method of effective syntactic description of frames using the contour information to improve the integrity of the video information resource," 2015 Second International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, Ukraine, 2015, pp. 253-256, doi: 10.1109/INFOCOMMST.2015.7357328.
[2] 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, China, 2016, pp. 1223-1226, doi: 10.1109/ICInfA.2016.7832006.
[3] 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.
[4] M. H. Alkawaz, M. T. Veeran and H. Razalli, "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.
[5] 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, Armenia, 2016, pp. 1-5, doi: 10.1109/EWDTS.2016.7807752.
[6] T. Song, Y. Jeong and J. Yook, "Modeling of Leaked Digital Video Signal and Information Recovery Rate as a Function of SNR," in IEEE Transactions on Electromagnetic Compatibility, vol. 57, no. 2, pp. 164-172, April 2015, doi: 10.1109/TEMC.2014.2372039.
[7] 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.
[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] 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, USA, 2016, pp. 149-152, doi: 10.1109/SSIAI.2016.7459197.
[10] V. Yatskiv, N. Yatskiv and O. Bandrivskyi, "Proof of Video Integrity Based on Blockchain," 2019 9th International Conference on Advanced Computer Information Technologies (ACIT), Ceske Budejovice, Czech Republic, 2019, pp. 431-434, doi: 10.1109/ACITT.2019.8780097.
[11] R. A. Michelin, N. Ahmed, S. S. Kanhere, A. Seneviratne and S. Jha, "Leveraging lightweight blockchain to establish data integrity for surveillance cameras," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169429.
[12] 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.
[13] 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.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

Scan to save the contact details