Efficient Model for Video Integrity through blockchain

1. Nikhil Bhusari, Department of IT, Dhole Patil College of Engineering, Pune
2. Tejaswini Kshirsagar, Department of IT, Dhole Patil College of Engineering, Pune
3. Akash Chandlekar, Department of IT, Dhole Patil College of Engineering, Pune
4. Apurva Borude, Department of IT, Dhole Patil College of Engineering, Pune
5. Kiran Gaikwad, Department of IT, Dhole Patil College of Engineering, Pune
6. Prof. Anuja Palhade, Department of IT, Dhole Patil of Engineering, Pune

***Abstract* – Video and the maintenance of his integrity is one of the most essential concepts that require effective understanding of the process of video generation and storage. Videos are highly integral as they are useful in providing effective realization of audio and video of a particular scenario that can be revisited again through visual and auditory means. The videos are highly useful to such an extent as they are being used as undeniable evidence in the court of law. But due to the large prominence of various tools and techniques that are being used to make forgeries and achieve manipulations on video realistically this utilization of videos as evidence becomes highly problematic and less straight forward. Therefore, there is a need for an effective approach that can be designed to achieve highly accurate and useful realization of video integrity and its evaluation. For this purpose, the proposed methodology effectively, implements the RSA an encryption along with key generation and block chain formation to achieve effective video integrity evaluation.**

Keywords: *RSA Encryption, Key Generation, Blockchain Framework*

I. INTRODUCTION

Videos are a highly useful and an integral part of life nowadays. People can talk document their most memorable memories and take videos of memorable sites that the can we visit again later just by watching those images and listening to the sounds creating a nostalgic environment. This is largely been possible due to the increase in the number of smart phones and other devices that are equipped with cameras and imaging devices that are highly capable of taking a clear video. These are effectively useful and highly engaging and due to the effective reduction in the price of these image sensors they have become highly economical to own a camera and take a video. This is the reason why there are increasing number of videos that are available and not just photos which was the norm several decades ago.

In this day and age of information the videos contain lot of valuable information that can be extremely useful in a variety of different scenarios. This information it is so useful that it can be used effectively e in a court of law or as an evidence which can be highly completing and can change the course of an investigation. Therefore, the videos for an integral part of the evidence that needs to be investigated and taken into consideration for effective analysis. This means a great importance is being paid to the videos which are no doubt equality evidence against the criminal law for the criminal for effectively providing the tools for providing justice.

But there is on the other hand a significant increase in the number of video editing tools and devices that are being used extensively for manipulating a lot of videos. These tools and other approaches for editing the videos have been around for long time but they have been getting extremely better over the years. This has led to significant manipulation such as deep fake videos which are being used to achieve effective and highly realistic forgeries. And as the video is an extremely useful tool for the purpose of providing justice in the form of evidence, this becomes highly problematic scenario as the judges can be fooled into incriminating wrong person for what led Go criminal effectively.

Therefore, this demands the need for an effective video integrity maintenance approach that can be utilized for the purpose of enabling the analysis of the video integrity to determine if there have been any manipulations of forgeries that have been attempted. They have been a number of approaches that have been realized for the purpose of achieving the integrity evaluation accurately but most of these approaches are either highly constraint due to their computational requirements for are usually time intensive which can be highly problematic for a real-life implementation.

This research article effectively e elaborates on a video integrity evaluation system that utilizes RSA encryption, along with the implementation of the blockchain distributed framework. The RSA encryption is one of the most useful and highly effective encryption tools that are being used in the recent years for a large number of security implementation. This encryption approach is an asymmetric encryption technique that is utilized for the purpose of achieving highly e accurate and secure generation of cipher text which is very difficult to crack. The complexity achieved in the RSA implementation is due to the implementation of co-prime and prime numbers. The RSA encryption is highly apt for this implementation due to the effective security e and the robustness offered by the RSA approach easily.

This research paper dedicates section 2 for analysis of past work as a literature survey, section 3 deeply elaborates the proposed technique and whereas section 4 evaluates the performance of the system, and finally section 5 concludes the paper with traces of future enhancement.

II LITERATURE SURVEY

F. Kharbat explains that the problem with detection of fake videos has been due to the fact that there have been multiple video editing approaches that has been effective in achieving a real like result that can fool a lot of individuals. This is a problem that has been related to the increase the reliability of the forensic approaches that are used to identify any changes or tampering that is being performed on the video [1]. Any type of tampering can result in the decrease in the security of the video significantly. The authors have been utilizing the image features for the detection of deep fake alteration ben performed.

Q. Wan expresses that there has been a wide use of video-based surveillance for the purpose of enabling an effective and useful improvement in the security of a particular location [2]. This is highly useful as it allows for remote surveillance along with reducing the reliance on human based interference in the determination of the safety conditions of an area. But there has been an increase in the number of editing tools that can perform effective editing of the videos which can be a problem for the forensic analysis. Therefore, an effective technique for the detection of the frame integrity has been elaborated in this research article.

G. Liu elaborates on the effective utilization of the video paradigm for the purpose of achieving effective surveillance and authentication [3]. This is a highly effective paradigm that allows the increase in the security of the platform through the implementation of the video-based surveillance. There are some inconsistencies that have been making the approach highly problematic to achieve the proper implementations. Therefore, the authors have proposed the use of hash computation for the purpose of achieving the digital watermarking.

R. Michelin discusses on the topic of achieving useful implementation of the video surveillance for the purpose of protection and safeguarding a particular location [4]. The video surveillance has been effective in realization of the safety from large distances that has been highly problematic for the purpose of achieving an effective and useful scenario without any malpractice by individuals with malicious intent. Therefore, to improve the integrity of the video the researchers have implemented a blockchain in a lightweight manner and have achieved effective improvement in the surveillance cameras.

J. Yao introduces the concept of determination of the video quality and its assessment through the use of different characteristics. This is highly useful as it allows for an effective understanding of the visual perception of quality that can be extremely useful for various implementations [5]. The determination of the video quality is extremely beneficial to utilize the VQA scores for the assumption of the video contents and the bitrate. The researchers in this research article have devised a novel implementation of a no reference-based assessment measure for the video quality through the use of visual perception.

Y. Yao Narrates that there has been increase in the number of techniques for the forgery of videos highly effectively. These forgeries have been extremely accurate and can effectively fool a number of individuals easily [6]. This is a problematic scenario as most of these videos are highly useful forms of evidence in the court of law and can be used to incarcerate a person. The effort to reduce this occurrence and improve the localization and forgery detection approach in videos the authors has proposed a unique implementation in this research article. The approach utilizes the effective identification of objects and detects forgeries accurately.

M. H. Alkawaz states that the paradigm of video surveillance is one of the most effective forms of security in the day and age of information nowadays. This is highly problematic as there are also various techniques and tools that can imperceptibly forge the videos to look like the real deal which can be highly dangerous in various scenarios [7]. This is an undesirable circumstance that needs to be effectively eliminated to maintain the video integrity and provide effective and useful surveillance at the same time. Therefore, for this purpose the authors in this approach have proposed the utilization of an effective approach that can detect the forgery in the videos through the utilization of double compression and analysis of the metadata.

D. Danko introduces the concept of maintenance of video integrity which is a highly important task to effectively integrate or resolve a crime. This is due to the fact that video evidence is considered highly valuable evidence in the court of law which can be problematic if the video is forged or has any dispute [8]. These kinds of problems require the maintenance of video integrity effectively to achieve important realizations and investigate the crime accurately. Therefore, for this purpose the authors in this approach have proposed utilization of blockchain platform to effectively maintain the video integrity on videos captured by internet of things devices.

A. Alimpiev discusses the paradigm of utilizing the resources and information from videos for the purpose of effectively analyzing this information that can be useful for determining the integrity of the videos. A lot of videos along with the captured image have a lot of other data that can be successfully analyzed to achieve effective understanding of the integrity of the image and the video easily [9]. Therefore, to achieve effective extraction of these information resources the authors in this approach have proposed the utilization of binomial slotting which can be developed for the purpose of extracting the integrity.

M. Mathai expresses that there has been a significant increase in the rise of manipulated videos that have been spreading mission formation among the masses every day. These manipulated videos are highly difficult to analyze and effectively understand due to the fact that these videos are highly problematic to understand if they are actually real or manipulated [10]. This is a very big problem as the videos can be used to spread misinformation which can be highly dangerous is for a lot of different reasons. Therefore, there is a need for an effective technique that can analyze the video to maintain the integrity and detect any forgery that are being performed on the video. To solve this problem the others in this approach have proposed the utilization of moment features along with normalization of cross correlation and location for forgery detection in the videos.

Y. Jin explain the concept of utilizing video surveillance as an effective approach that is being used for the purpose of engaging security and safety of a particular area. The purpose of achieving video surveillance requires extensive realization of communications along with networks and utilization of computers to achieve effective video surveillance [11]. This process is highly complicated and requires extensive and effective implementation to achieve the goals. The video surveillance is a important part of a smart City therefore and effective approach for the purpose of achieving heterogeneous communication through the use of system optimization in a cluster based unmanned aerial vehicle video surveillance system has been effectively elaborated in this research article.

IV PROPOSED METHODOLOGY

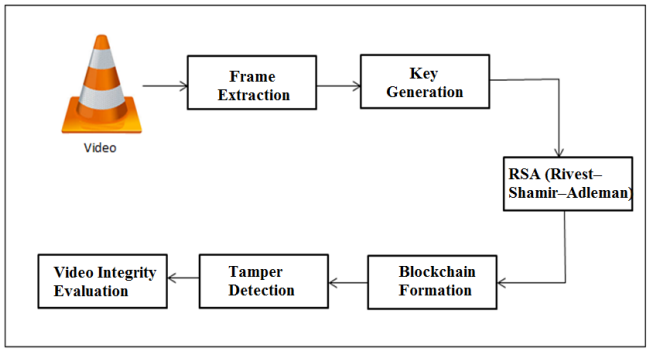


Figure 1: Video integrity Evaluation System Overview

The proposed methodology for the purpose of enabling a video integrity evaluation system has been depicted in the system overview given in the figure 1 above. The detailed steps utilized for this purpose

Step 1: Video Input and Frame Extraction – The system requires a video input for initialization of the methodology. For this purpose, a graphical user interface has been developed that takes the video input which is provided to the system. The swings framework is utilized to enable a file picker that provides the system with the path of the video. The selected path is then used by the Xuggler API to interface with the video and achieve the extraction of the frames. The frames are extracted according to a predetermined time interval and provided to the next step of the system for the purpose of further processing.

Step 2: Key Generation – The output from the previous step, consisting of the video frames is being taken as an input in this step of the procedure. These frames are used for the purpose of performing key generation procedure that is implemented through the use of the MD5 hashing algorithm. The frames provided as an input are read in the form of images which are converted into bytes for effective processing. The extracted byte data of the frames is provided as an input to the key generation module which implements the MD5 for the purpose of hash key generation.

The process of key generation initiates through the use of the bytes data of the frames to achieve a single string through the concatenation of the contents. This achieved string is provided to the MD5 hashing approach for the hash key generation. The resultant hash key is calculated through the implementation of the modulus operations and the achieved values are further processed.

The achieved values are processed through the use of an iteration which starts from 0 and terminates at a key length of 8. This iteration is also utilized to create more confusion in the key generation procedure through the addition of the value of I to the value, 1+remainder. Another condition is checked in this iteration, wherein the value of I is compared to the key generated by the MD5 hashing approach, if the value is less than the key, the i^{th} character is extracted and the key is rotated by one element. Once this entire procedure is completed, this module gives the output as a hash key.

The achieved hash key is then reduced by selection of 8 random characters, which results in a plain block head key. The resultant key is useful in the next step of the procedure for the purpose of achieving an effective encryption. The procedure for key generation has been has been illustrated in the algorithm 1 given below.

ALGORITHM 1: Block head Generation

```
//Input : Frame Bytes in String F_BS
//Output: Key K_Y
Function: blockHeadGeneration(F_BS)
1: Start
2: kstr = " ", BH_KEY = ""
3:   for  i=0 to size of F_BS
4:        kstr = kstr + F_BS [i]
5:  end for
6:        MD5_HK= MD5(kstr)
7:        MOD_VAL= MD5_HK SIZE MOD 8
8:    for i=0 to BH_KEY Length < 8
9:          i=i+( MOD_VAL +1)
10:          if ( i< MD5_HK length)
11:          BH_KEY = BH_KEY + MD5_HK [i]
12:          MD5_HK = MD5_HK >> 1
13:          else
14:          i=0
15:  end for
16:   return  BH_KEY
17: Stop
```

Step 3: RSA Encryption – The key generated in the previous step is utilized as an input in this step of the procedure. The encryption approach is achieved through the use of effective realization of the Rivest-Shamir Adleman or the RSA approach. This encryption standard utilizes an asymmetric approach that allows for an effective and secure encryption. The key generated in the previous step is provided to the RSA module to achieve effective encryption of the input frame data.

This input key is then effectively divided into the two different forms of keys, namely, public key and private key. The public key is used to achieve the encryption of the data, whereas the private key is used to decrypt the encrypted data to get the original data back. The public key is estimated using an effective combination of co-primes and prime numbers, which derive the two important elements of the key, N and E.

The private key pri(N,D) is achieved through the MOD operation.

These two keys are derived using the equations given below. The equation 1 is used to achieve the public key, whereas the equation 2 is used to determine the private key.

$C_D = P^E \text{ MOD } N$ _____(1)

$D_D = C_D^D \text{MOD } N$ _____(2)

Where
C_D - Cipher Data, P- Plain data D_D-Decrypted Data

Step 4: Blockchain Formation – The head keys generated in the previous step form an important aspect of this step of the module. The blockchain approach is an integral part of the approach where the effective integrity of the videos given as an input is maintained. The block head key is combined with the byte string of the subsequent frame. The string achieved through this process is then put through the key generation procedure to achieve an 8-character key. This key is then encrypted using the RSA module which results in the block head for that particular frame. This procedure is constantly performed for all the frames in the video. Once the last frame or the nth frame is reached the entire process for key generation is performed and the resultant key is referred to as the terminal key. Once the terminal key is reached, it is effectively stored in the third-party database along with the attributes of the video, such as the video name, time and date.

Step 5: Tiled Bitmap Algorithm – This is step where the integrity of the video is maintained and evaluated. The tile here refers to the time, wherein a specific time interval, such as 2 minutes, 3 minutes etc. is being utilized for the purpose of evaluation. Once the time threshold is reached, the system downloads the file from the third-party server and utilizes it as an input to the system to perform all of the steps again. This leads to the system achieving a terminal key. Once the terminal key is achieved, it is effectively compared with the terminal key for the same video stored in the database previously. If both the keys are same and the obtained key matches the key stored in the database, then the integrity of the video is maintained. Whereas if the keys do not match, this indicates some tampering or forgery being performed on the video.

V. RESULTS AND DISCUSSIONS

The proposed methodology for the purpose of enabling an effective approach for the determination of video integrity and its analysis has been elaborated in this research article. The technique has been achieved through the use of the java programming language on the NetBeans IDE. For the development purposes, a machine with the configuration consisting of an Intel Core i5 processor along with 600GB of storage and 4 GB of RAM is used. The responsibilities for database storage have been satisfied through the use of the MySQL Database server.

The proposed methodology has been evaluated for its performance through the use of extensive experimentation which has been depicted in detail in the section given below.

Encryption and Decryption Time performance

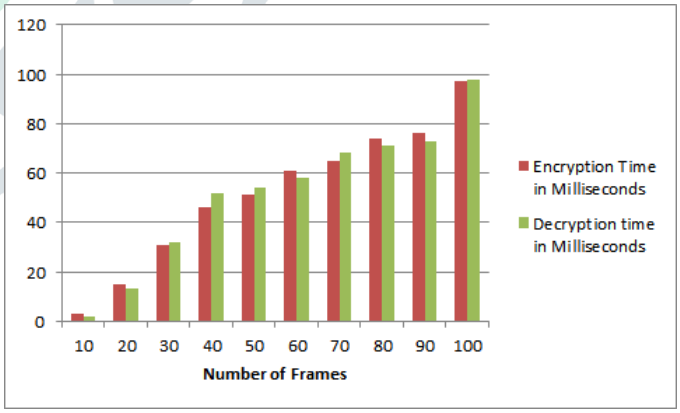
The presented technique has been effectively assessed for its performance of the encryption approach. The encryption in this methodology has been provided through the use of the RSA encryption. The reason for the selection of this experimental approach is due to the fact that the encryption is one of the most integral aspects of the prescribed approach. Also, the performance improvement in this module can provide effective realization of the performance of the entire system.

The experimental setup aims to determine the time taken for the encryption and decryption for an increasing number of frames. The encryption module is effectively assed for its performance the resultant outcomes are recorded in the table 1 given below.

Number of Frames	Encryption Time in Milliseconds	Decryption time in Milliseconds
10	3	2
20	15	13
30	31	32
40	46	52
50	51	54
60	61	58
70	65	68
80	74	71
90	76	73
100	97	98

Table 1: Encryption and Decryption time performance

Figure 2: Encryption and Decryption Time



The values obtained as the resultant outcomes have been utilized to achieve an effective graph in the figure 2 above. As it can be understood from the values achieved in the experimental evaluation, the process of encryption and decryption is not directly proportional to the number of frames given as an input. This indicates that the process of encryption and decryption achieve through the RSA approach has been implemented accurately. The results indicate an effective and useful implementation of the approach which is a highly promising outcome for the first-time implementation of such a system.

VI. CONCLUSION AND FUTURE SCOPE

The methodology for an effective approach for the purpose of integrity evaluation has been outlined in detail in this research article. Videos are highly useful and have been an effective part of everyday human life in the recent years. While most of the smartphones are effectively equipped with the state-of-the-art camera sensors that can effectively capture a video, most of the videos that are captured are in the form of video surveillance. Videos are so important that they are used as evidence in the court of law to achieve effective and useful incrimination against the criminal. But due to a lot of different techniques that are we designed to achieve video forgeries and manipulation there have been and effect active need for an evaluation system for the integrity of the videos. For this purpose, the system takes the video as an input which is effectively utilized for the frame extraction. Once the frames of the video are extracted these frames are effectively encrypted through the use of RSA encryption system. These encrypted frames are transferred to the next module which is the key generation module. This module effectively generates the keys of the encrypted frames which are then utilized the successfully to build a blockchain platform. This effectively secures each and every frame from the video in the form of a blockchain and if any manipulation is done on even a single frame which would lead to a large avalanche effect which should be indicated of loss of integrity.

For the purpose of future research directions this approach can be effectively formulated as an API for easier integration and evaluation.

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), 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), 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), 2016, pp. 1223-1226, doi: 10.1109/ICInfA.2016.7832006.

[4] 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), 2020, pp. 1-3, doi: 10.1109/ICBC48266.2020.9169429.

[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. 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.

[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] 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

[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] 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.