Video Integrity Verification Using Blockchain

A PROJECT REPORT

submitted by

FEBIN BAIJU
LTVE17MCA062

to

the APJ Abdul Kalam Technological University
in partial fullfilment of the requirements for the award of the degree

of

Master of Computer Applications

Department of Computer Applications
College of Engineering Trivandrum
Trivandrum-695016

JULY 2020

DECLARATION

I undersigned hereby declare that the project report Video Integrity Verification Using Blockchain, submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Dr. Sabitha S. This submission represents my ideas in my words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity as directed in the guidelines of Institutional ethics committee of the college and have not misrepresented or fabricated any data or idea or fact or source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title.

Place : Trivandrum
Date : 26/07/2020 Febin Baiju

DEPARTMENT OF COMPUTER APPLICATIONS

COLLEGE OF ENGINEERING TRIVANDRUM

CERTIFICATE

This is to certify that the report entitled **Video Integrity Verification Using Blockchain** submitted by **Febin Baiju** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications is a bonafide record of the project work carried out by him under my guidance and supervision. This report in any form has not been submitted to any University or Institute for any purpose.

Internal Supervisor External Supervisor

Head of the Dept

ACKNOWLEDGEMENT

If words are considered as symbols of approval and tokens of acknowledgement, then let words play the heralding role of expressing my gratitude.

First of all, I would like to thank God almighty for bestowing me with wisdom,courage and perseverance which had helped me to complete this project ***Video Integrity Verification Using Blockchain***. This project has been a reality as a result of the help given by a large number of personalities.

I am extremely thankful to **Dr Jiji C V**, Principal, College of Engineering Trivandrum for providing me with the best facilities and atmosphere which was necessary for the successful completion of this project.

I would like to remember with gratitude **Dr. Sabitha S**, Head Of Department Department of Computer Applications, College of Engineering, Trivandrum for the encouragement and guidance rendered.

I express my sincere thanks to **Dr. Sabitha S**, Associate Professor, Department of Computer Applications, College of Engineering Trivandrum for her valuable guidance, support and advice that aided in the successful completion of my project.

Finally, I wish to express my sincere gratitude to all my friends, who directly or indirectly contributed in this venture.

Febin Baiju

ABSTRACT

The proof of crime or road accidents is based on video recordings taken from the security camera. But the video footage is prone to many video tampering attacks. Although visual proof is needed for integrity testing, for human vision it is not easy to recognize video forgery or distortion. A video integrity verification system is developed with the help of blockchain. The blockchain system works by using HMAC and Elliptic curve Cryptography. The video data from the surveillance footage is hashed and stored in the blockchain real-time. The verification process generates a hash for the input video and compares it with the hash stored in the Blockchain. This method is implemented in surveillance camera and accident data recorder systems.

.

Contents

List of Figures

Chapter 1

Introduction

The purpose of this project is to develop a new method to verify video integrity of monitoring cameras. The technical advance resulted in the use of monitoring cameras like CCTV or ADR systems on a large scale. The CCTV or ADR footage can provide valuable visual details and can be a witness. This plays an significant part in presenting evidence in accidents or car accident conflicts. However, the network's transparency enables the global exchange of videos. This however has a major disadvantage. When sent to various individuals, the videos can be duplicated or manipulated. Although some video manipulation can be detected by human eyes, advancements in software for video editing have made identifying the majority of them hard these days. Since videos from surveillance are an essential component of evidence, interfering can also alter court decisions. I therefore use a new method to monitor video integrity in a blockchain model, which combines HMAC and elliptical curve cryptography.

Generally, active and passive approaches are used for verifying the integrity and authenticity of video. Digital signatures, fingerprints and watermarking that requires information in the form of signatures or hash values as a proof is used in active approach. The passive approach does not have any instance to original contents, but, it is based on noise residue and compression artifacts in the tampered video. Most of the video cameras and monitoring systems use algorithms of compression incorporated in the device. Yet the saved videos can be manipulated by decompressing the file, modifying it and recompress the file again.

Here i introduce a new method that can detect video tampering by using blockchain which can ensure the integrity of the video. The proposed method is active apporach therefore, a value is generated for every video footage which can be used to validate the integrity of the video. Therefore, noisy residues and inconsistent periodic artifacts are not required to find in the proposed method. This leads to a better verification method for video integrity. The Hash of video footage is stored in the blockchain. Then, the hash is generated and compared to the blockchain node during the verification process.

1.0.1 Motivation

One of the key reasons CCTV cameras play a major role in businesses is that they help to prevent as well as deter crime. Most thieves and robbers target industrial buildings and places of work if they see no safety staff. However if there is a CCTV installed outside the premises they may just drop the plan of theft . In fact, the video and images will be registered even if someone unauthorized tries to come into the workplace. This can help catch the thieves or burglars, thus providing justice.

In this digital era, CCTV footages are likely to be tampered due to the easy access to internet and video editing softwares. It can make the right judgement challenging, because the evidence can potentially be distorted by someone before they hit the court. It is important to store them safely in order to serve the correct justice and the best way to do this is by using Blockchain technology.

1.0.2 Problem Definition

CCTV or ADR systems are capable of delivering video and may also be a witness to the essential visual details at Court of Justice. This is an important part of evidence in criminal investigation or during road crash cases. The network's openness enables the videos to be shared all over the globe. However, the accessibility of the network comes with a big disadvantage. It is possible to replicate or tamper the videos as it is distributed to various people. Although some of the video manipulation can be detected by Human vision, advance methods of video editing made it difficult to find them these days. We must verify the integrity of the video recordings in order to address these problems.

Video Integrity check using Blockchain is required because the existing systems are not efficient enough for the real world applications. The video footage is decentralized in this architecture and implements new security protocols to make it secure. The other systems are storing the datas about the video in flat file based database which is easier to access and modify. Blockchain technology in the proposed sytem assures that no data is accessible to modify by a third party.

1.0.3 Objectives

The main objective of this project is to develop a Blockchain and Cryptography based video surveillance system that can be used to verify the integrity of the video footage. Blockchain assures the integrity of the data and cryptography ensures the safe key exchange and the hashing schemes. Then it is required to secure the hash of file with unique key for each footage. Use of Blockchain, to detect and prevent modification of the hash stored is necessary. Elliptic Curve Diffie-Hellman Key Exchange algorithm is used for the key exchange of the video datas. Blockchain was implemented using Ethereum Blockchain with Web3.Py in Python Programming language. Elliptic Curve Diffie-Hellman Key Exchange algorithm for key exchanging was implemented in Python. The GUI of the project is developed using PyQT5 framework in Python.

1.0.4 Report Organization

Chapter 2: This chapter covers all the details of literature review. That is the comprehensive summary of some previous research on the proposed topic.

Chapter 3: Purpose and description of the project is explained here along with the tools used for the development

Chapter 4: This chapter deals with methodologies used in the proposed system. It includes System design and data flow diagrams design.

Chapter 5: Results and Discussions of the work is explained with the help of screenshots of the application.

Chapter 6: Conclusion and Future scope of the application are explained.

Chapter 7: The previous reports which helped in the project are listed.

Chapter 2

Literature Survey

This section presents related literature concerning various video integrity verification methods.

2.1 Frame Change Detection

This method is used for detecting changes in frames of video footages by means of periodic artifacts. Frame removal and alteration are detected by this system to detect any video tampering. Variations in residual and intra-macro block variations are measured in this process. Based on the characteristics produced, a fusion index is created based on abnormal shift in video streams. A dataset is composed of six sub-sets and measures the video and Group of images (GOP). The downside is that it needs high computing power to check the frame deletion, therefore it is inefficient.

2.2 Slack Space Video Frames

This approach tests the quality of video content in legacy camera surveillance systems lacking integrated integrity protection. This method is used to verify integrity for automotive blackboxes of AVI or MP4 formatted video content. When a video is tampered the changed contents of the video are overwritten over the original video contents. But the slack space of the storage media will have the original video contents since the size of the tampered video will always be larger than the original video. This method checks the size difference between the slack space video frames and the the allocated storage for the video. If they are not the same it will mean that the video is tampered. This method is used only with legacy systems which does not have any form of integrity verification and this method can be easily spoofed by accessing slack space.

2.3 Double Quantization

Double quantization occurs when a tampered video is compressed twice. This method implements a forgery detection algorithm based on pixel estimates and double statistics of compression for videos from static cameras. When a video is tampered, it gets double compressed. This method checks the difference of the noise added when the video is double compressed and single compressed. The difference can tell whether the video was tampered or not. But this algorithm can detect only if the bitrate of double compressed video is higher than that of original video.

Chapter 3

Requirement Analysis

3.1 Purpose

Modern video editing softwares are easily capable of tampering surveillance camera videos, which can defeat it's purpose to be used in the judicial court. Therefore, here i introduce a technique to detect tampering in surveillance videos by using blockchain with elliptic curve cryptography and HMAC.

3.2 Overall Description

The proof of crime or road accidents is based on video recordings taken from the security camera. But the video footage is prone to many video tampering attacks. Although visual proof is needed for integrity testing, for human vision it is not easy to recognize video forgery or distortion. Video files need to be protected from video forgery so that it is presented before the court in it's original form. If video files are tampered, it can cause the guilty to escape. Hence it is very important to protect the video file from tampering.

3.3 Operating Environment:

The operating environment required are:

3.3.1 Hardware Requirements

- Intel Quad Core or equivalent processor
- Intel Quad Core or equivalent processor
- 2 GB or more RAM
- 1.6 GHz or more CPU Speed
- 300 GB or more hard disk space

3.3.2 Software Requirements

- Linux/Windows
- MetaMask
- Ganache
- Solidity
- Python

3.4 Functional requirements

Functional requirements represent the intended behavior of the system. This behavior may be expressed as services, tasks or functions that the specified system is required to perform. The following functional requirements have been identified for this project.

The main functional requirements are;

- Capture video from the external/internal camera
- Calculate the video Hash from the captured video.
- Store it in the Blockchain and make it available for verifying the integrity of the footage using hashes.
- A GUI for allowing the authorised person to check the integrity of the video.

3.5 Non Functional requirements

Non-Functional requirements define the general qualities of the software product. Non-functional requirement is in effect a constraint placed on the system or the development process. They are usually associated with the product descriptions such as maintainability, usability, portability, etc. It mainly limits the solutions for the problem. The solution should be good enough to meet the non-functional requirements.

3.6 Performance Requirements

- **Accuracy:** The program should preserve consistency in the working and the essence of the usability.
- **Speed:** The system needs to be fast and responsive for the users.

3.7 Quality Requirements

- **Transparency:** The program provides all participants with accurate data.
- **Scalability:** All practical specifications will be met by the program.
- **Maintainability:** The system should be maintainable. It must maintain safeguards to prevent failures in the network and regularly record its activities.
- **Reliability:** The acceptable threshold for the downtime should be as long as possible. If the system has been disabled, it should take the least minimal time to restore the system. .

Chapter 4

Design And Implementation

4.1 Overall Design

Our system is a video integrity verification system. It can record video footage like a surveillance camera and also provides an interface to upload video to check the integrity of the video footage. One of the main aims while designing the system was to abstract as much lower level details of the system as possible from the user. This system provides a desktop interface for its users. The interface is developed using Python's PyQT5 framework. The only technology available today that could handle all these problems and provide us with immutable, verifiable and trustworthy certificates is 'Blockchain'. The proposed system uses the public blockchain technology called Ethereum blockchain. Here the focus is on checking the integrity of videos with blockchain and providing security and transparency to the data using elliptic curve cryptography and HMAC. Following figure shows the block diagram of the system:

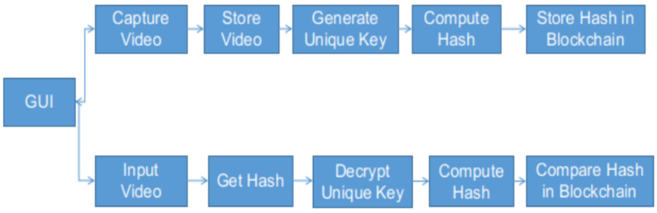


Figure 4.1: Block diagram of the proposed system

4.2 Module Description

- **Capturing Video and Storing in Blockchain** The system captures the video and stores their Hash in Blockchain
- **Verify Video Integrity:** The authorised personel is allowed to access the GUI Interface to check the video presented before him/her. The input video hash is verified by the personal through this interface.

4.3 Data Flow Diagrams for the System

A data flow diagram (DFD) is a graphical portrayal of the ”flow” of information through a data framework, displaying its procedure perspectives. A DFD is frequently utilized as a fundamental advance to make a diagram of the framework without going into incredible detail, which can later be expounded. DFDs can likewise be utilized for the perception of information handling (organized structure).

Context Diagram (Level 0)

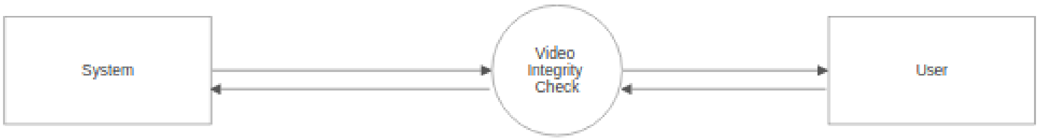


Figure 4.2: Level 0 DFD

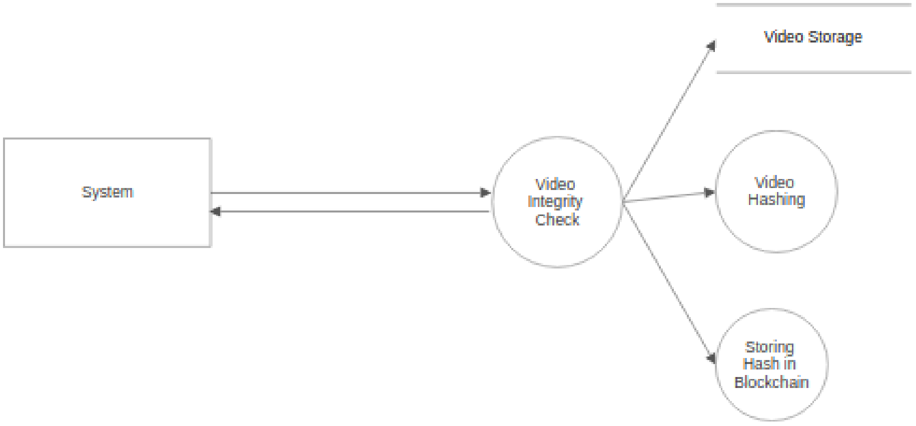


Figure 4.3: Level 1.1 DFD

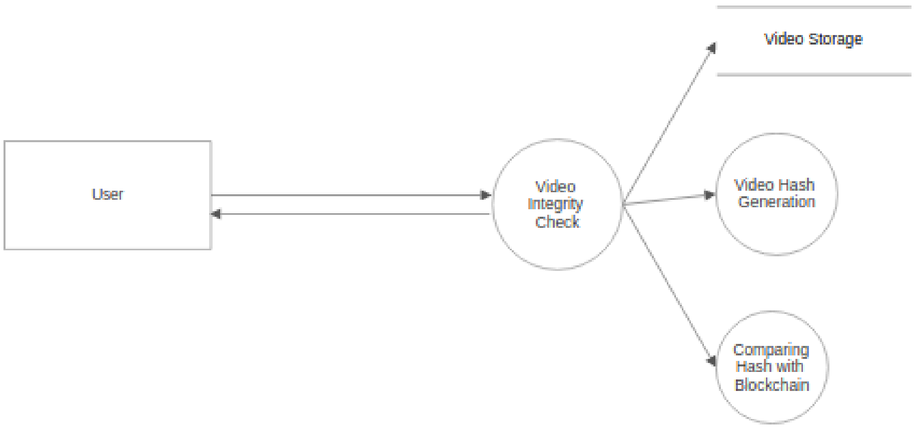


Figure 4.4: Level 1.2 DFD

Chapter 5

Results And Discussion

The Video Integrity check using Blockchain system contains mainly 5 phases. They are:

- **Video Hash Generation**
- **Key Encryption**
- **Block Generation**
- **Key Decryption and Comparison**
- **Results**

5.1 Video Hash Generation

The video capturing device captures the real time footage and stores them chronologically in the device. Then the HMAC-SHA256 of the video data is generated using an unique key, and the value is then stored in the Blockchain.

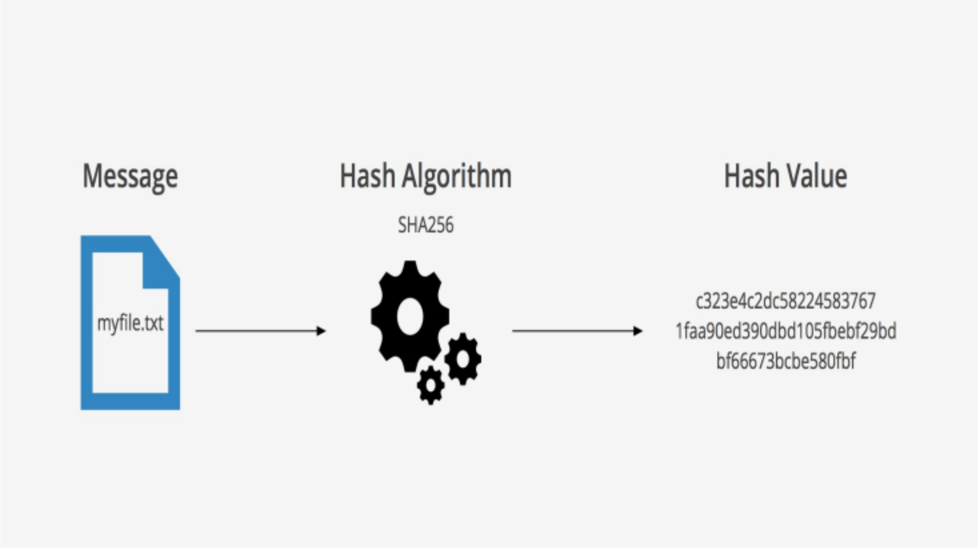


Figure 5.1: Hashing of File

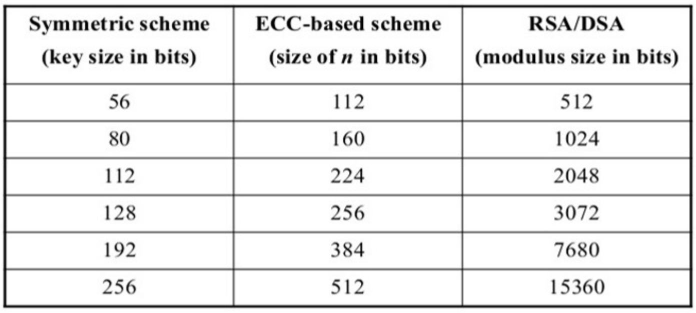
5.2 Key Encryption

The unique key used for hashing the video is encrypted using Elliptic Curve Cryptography and the key is exchanged using Elliptic Curve Diffie–Hellman Key Exchange technique. The encryption of the key will provide more security.

5.2.1 Elliptic Curve Crytography

Elliptical Curve Cryptography (ECC) is a type of public-key cryptography. It calculates elliptic curve arithmetic instead of using integer of polynomial arithmetic. In contrast with RSA, ECC offers similarly good protection but uses smaller key sizes. major advantages of ECC:

- **Uses smaller keys, signatures and ciphertexts**
- **ECC helps to generate key very quickly**
- **ECC scores over RSA due to its much faster encryption and decryption**
- **ECC computations uses less CPU cycles and less memory compared to RSA, therefore it is suited for securing mobile and handheld devices.**



Symmetric scheme (key size in bits)	ECC-based scheme (size of *n* in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Figure 5.2: key sizes of other security methods

An elliptical curve is characterized by an equation of two coefficient variables. The elliptic curve cryptography uses the elliptical curves in which all variables and coefficients are limited to finite field elements. ECC over real numbers are the set of points (x , y) that satisfy y2 = x3 + ax + b, where x, y, and b are real numbers. A different set of values for a and b results in an elliptical curve that is distinctive.

For example a = -5 and b = 0.48 gives the elliptic curve with equation y2 = x3 - 5x + 0.48. If the cubic polynomial x3+ax+b has no repeated roots, we say the elliptic curve is non-singular. A necessary and sufficient condition for the cubic polynomial x3+ax+b to have distinct roots is $5a^3 + 27b^2$ not equal to 0.

5.2.1.1 Elliptic Curves over finite fields

Instead of selecting the field of real numbers, we can create elliptical curves over other areas. Let a and b be elements of Zp for p prime, p>3. An elliptic curve E over Zp is the set of points (x,y) with x and y in Zp which satisfy the equation

$$y^2 + (modp) = x^3 + ax + b(mod\ \ p) \tag{5.1}$$

To get a non-singular elliptic curve, we'll need $5a^3 + 27b^2$ (mod p) $\neq$ 0 (mod p). The elliptical curves over Zp are a finite set of points. As in the actual case, addition of points can be set for prime p>3 on the elliptical curve E over Zp. It is essentially done in the same way as the actual situation, with the necessary modifications.

5.2.2 Diffie-Hellman Key Exchange – ECC

Two parties John and Alex need to exchange a secret key.
1. Both John and Alex agree upon starting point P point on elliptic curve publicly defined as y2 = x3 - 5x + 0.48
2. John selects his private key X and computes XP shares this with Alex
3. Alex selects his private key 'B' and computes BP. Then, shares with John.
4. John receives BP and computes BPX by multiplying with his private key.
5. Alex receives XP and computes XPB by multiplying with his private key.
6. It is evident that BPX = XPB , hence both John and Alex have same key which can be used as a private key for encryption and decryption.

5.3 Block Generation

The hash of the video along with it's unique key's public key is stored in the blockchain. The unique key is stored in the Blockchain because as mentioned in the above component the filename also has to be preserved. Then the video footage's hash is submitted to Blockchain.

5.4 Key Decryption and Comparison

The hash generated by the input video footage is then compared with the hash value in the Blockchain. If a match is found, the video footage is genuine else it is tampered. The unique key is decrypted using the shared key from Elliptic Curve Diffie–Hellman Key Exchange method.

5.5 Results

5.5.1 Screenshots

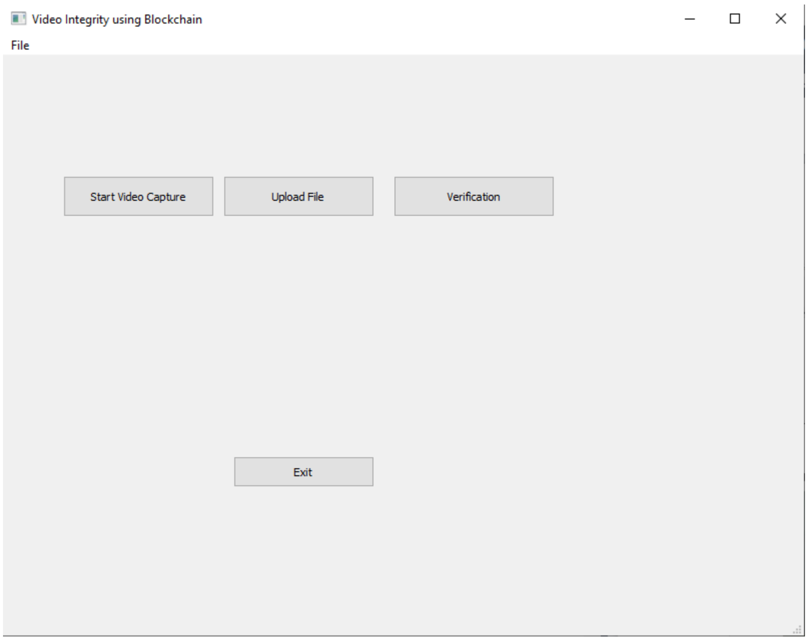


Figure 5.3: Main Interface

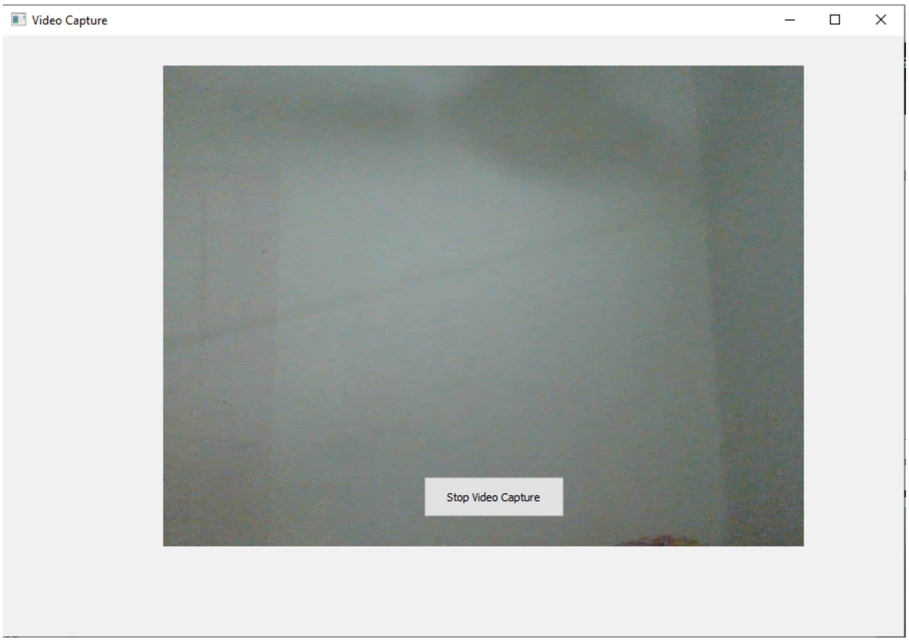


Figure 5.4: Capture Video

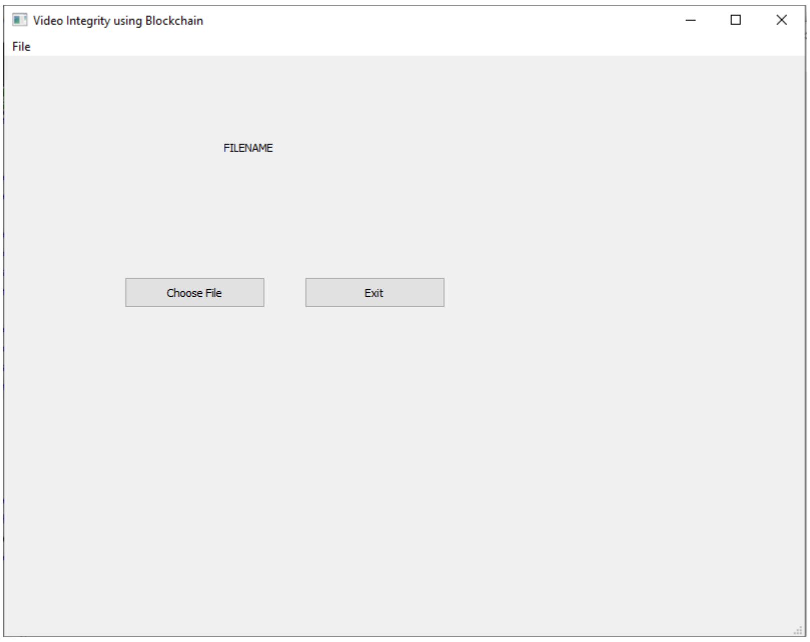


Figure 5.5: Video Verification

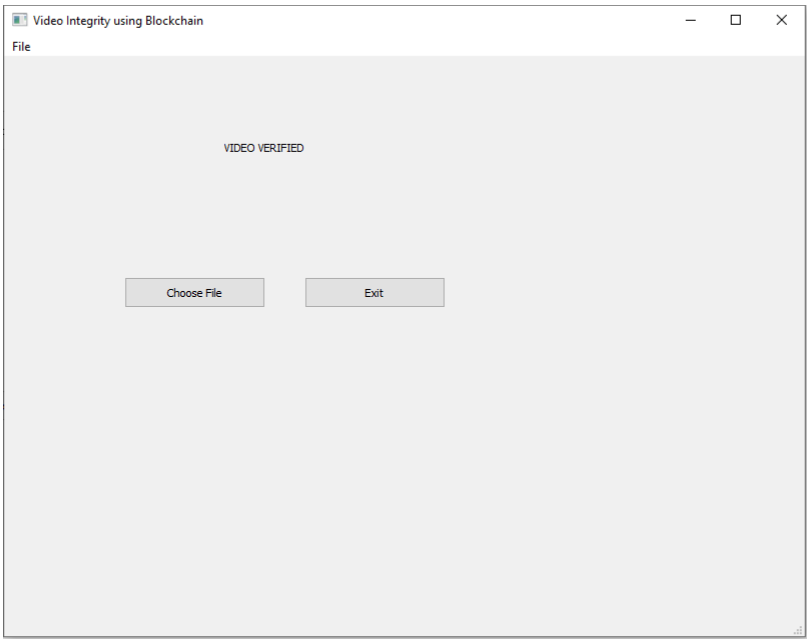


Figure 5.6: Video Verification Result

Chapter 6

Conclusion And Future Work

An efficient Blockchain based Video Integrity System is developed that can record real time video footages. This system uses various crytography methods and the Blockchain technology for operations. Blockchain method ensures the immutability and integrity of the sytem. Cryptographic algorithms used are Elliptic Curve Diffie-Hellman for the Key Exchange and HMAC for the key encryption. These keys ensures that the hash is safe and not available for someone else to reproduce the same data.

In the future work, this system can be further improved to add various types of files like documents,images and other media files. The availability of the video data itself instead of the hash to the general open network and segmentation of videos to improve the system.

Bibliography

[1] Sarala Ghimire, Jae Young Choi and Bumshik Lee *"Using Blockchain for Improved Video Integrity Verification"*, 2016

[2] C. Lee, J. Lee, Y. Pyo, and H. Lee *"Broken Integrity Detection of Video Files in Video Event Data Recorders"*, 2016s.

[3] H. Krawczyk, M. Bellare, and R. Canetti *'HMAC: Keyed-Hashing for Message Authentication'*, 1997

[4] Gemalto *'Benefits of Elliptic Curve Cryptography'*. 2019

[5] "SHA-1 Broken - Schneier on Security *'https://www.schneier.com/blog/archives/2005/02/sha1'*, 2005

[6] D. Hankerson, A. Menezes, and S. V. Springer *""Guide to Elliptic Curve Cryptography'*, 2017