

# Video Integrity Verification using Blockchain

Domain : Blockchain  
Guide: Dr. Sabitha S

**Febin Baiju**  
**LTVE17MCA062**  
**Roll No : 59**

**MCA S6**

# Overview

- ◆ Introduction
- ◆ Literature Review
- ◆ Problem Definition
- ◆ Motivation
- ◆ Objectives
- ◆ Existing System
- ◆ Proposed System
- ◆ Experimental Evaluation
- ◆ Screen shots
- ◆ Result
- ◆ Future Scope
- ◆ Conclusion

# Introduction

- *The video recorded by CCTV or ADR systems can provide important visual information and also can act as a witness in the court of law.*
- *It plays a major role in providing evidence in crime investigations or during disputes involved in a motor accident*
- However, the openness of the network makes it easier for the videos to be shared around the world.

# Introduction

- *The openness of the network however comes with a big disadvantage. The videos can be duplicated or tampered when it gets passed on to different people.*
- *Even though some of the video tampering can be identified using human eyes, the advancements in the video editing softwares has made it difficult these days to identify most of them.*

# Introduction

- *Since surveillance videos are crucial part of evidence, tampering can might even change the judgement in the judicial court.*
- *Therefore, we implement a new method to check the video integrity by combining **HMAC** and **elliptic curve cryptography** with **blockchain**.*

# Literature Review

AUTHOR	PAPER TITLE	YEAR OF PUBLISHING	METHODOLOGY
L. Yu et al	Exposing frame deletion by detecting abrupt changes in video streams, ScienceDirect	2016	Video forensics, Anomaly detection, Frame deletion detection, Video stream analysis
Hareesh Ravi, A.V. Subramanyam, Gaurav Gupta, B. Avinash Kumar	Compression noise based video forgery detection, IEEE International Conference	2014	Forgery, Transform coding, Image coding, Markov processes
Sangwook Lee, Ji Eun Song, Wan Yeon Lee, Young Woong Ko	Integrity Verification Scheme of Video Contents in Surveillance Cameras for Digital Forensic Investigations, IEICE Transactions	2015	digital forensics, integrity, surveillance camera

# Problem Definition

- CCTV footages are prone to tampering due to advancement of video editing softwares and the openness of the internet which allows to distribute the video file to large number of audience easily.

# Motivation

- In this digital era, CCTV footages are likely to be tampered due to the easy access to the 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 ideal way is to use Blockchain.



# Objectives

- To build a video surveillance system that can be used to verify the integrity of the video footage by using hashes.
- To secure the hash of file with unique key for each footage.
- Use of Blockchain, to detect and prevent modification of the hash stored

# Existing System

The conventional method of surveillance systems include following methods:

- No security protocols are used in surveillance systems
- Video Watermarking is used for proving the authenticity of video

# Existing System

The conventional method of surveillance systems include following methods:

- Verification systems use md5 algorithm for hashing purposes
- Uses flat file based database

# Drawbacks

Conventional methods drawbacks include:

- **Lack of security protocols** will make it possible for video footage to be easily shared and tampered.
- **Video Watermarking** is not particularly safe, because a good graphic designer can recreate new watermark in the tampered video just like new.

# Drawbacks

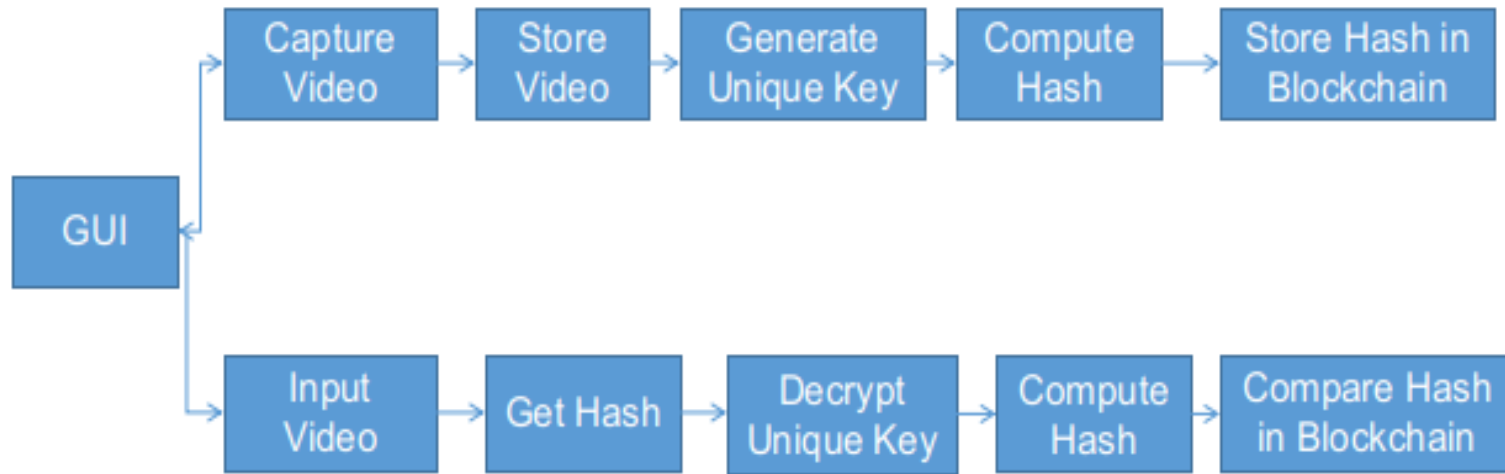
Conventional methods drawbacks include:

- **Verification using MD5 algorithm** is not safe comparing to other hashing algorithms. It is prone to collisions.
- **Flat file based database** is easily accessible to modify the data.

# Proposed System

- The proposed system uses Blockchain technology to store the HMAC SHA256 hash of the video, which is much more secure than MD5 algorithm
- With Blockchain, the data is stored in a decentralised architecture
- The key used in HMAC SHA256 is uniquely generated which provides more security from decryption by third party.

# Design



# Methodology

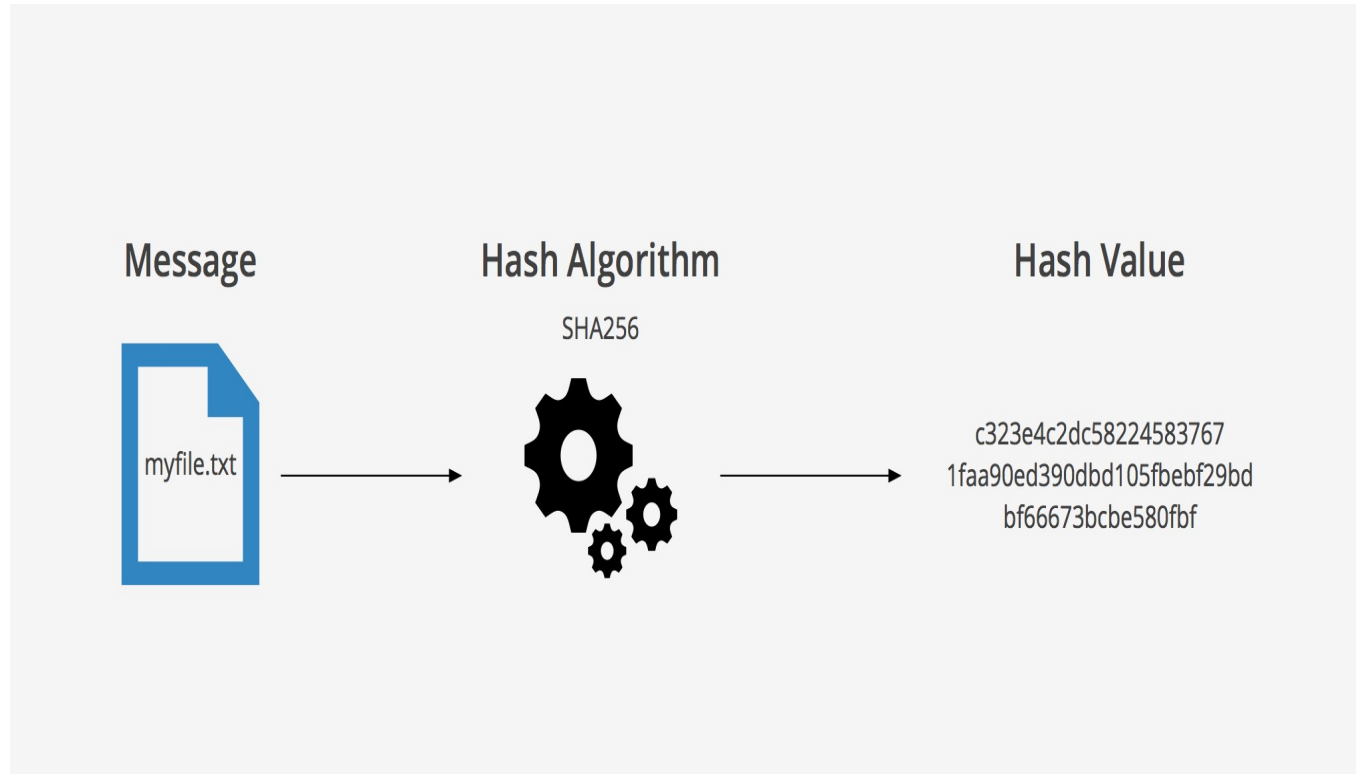
There are five phases in the system:

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

## **I. Video Hash Generation**

The HMAC-SHA256 of the video data is generated using an unique key, and the value is stored in the blockchain





SHA256 is combined with HMAC to provide more security for the encryption

## **II. Key Encryption**

- 1) 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.
- 2) The encryption of the key will provide more security

### **III. Block Generation**

The hash of the video along with its unique key's public key is stored in the blockchain.

Here the video footage is submitted to Blockchain, and now the checking phase begins.

### **IV. Key Decryption**

The unique key is decrypted using the shared key from Elliptic Curve Diffie–Hellman Key Exchange method.

### **V. 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.

## **VI. Result**

- **PyQT5 Framework**

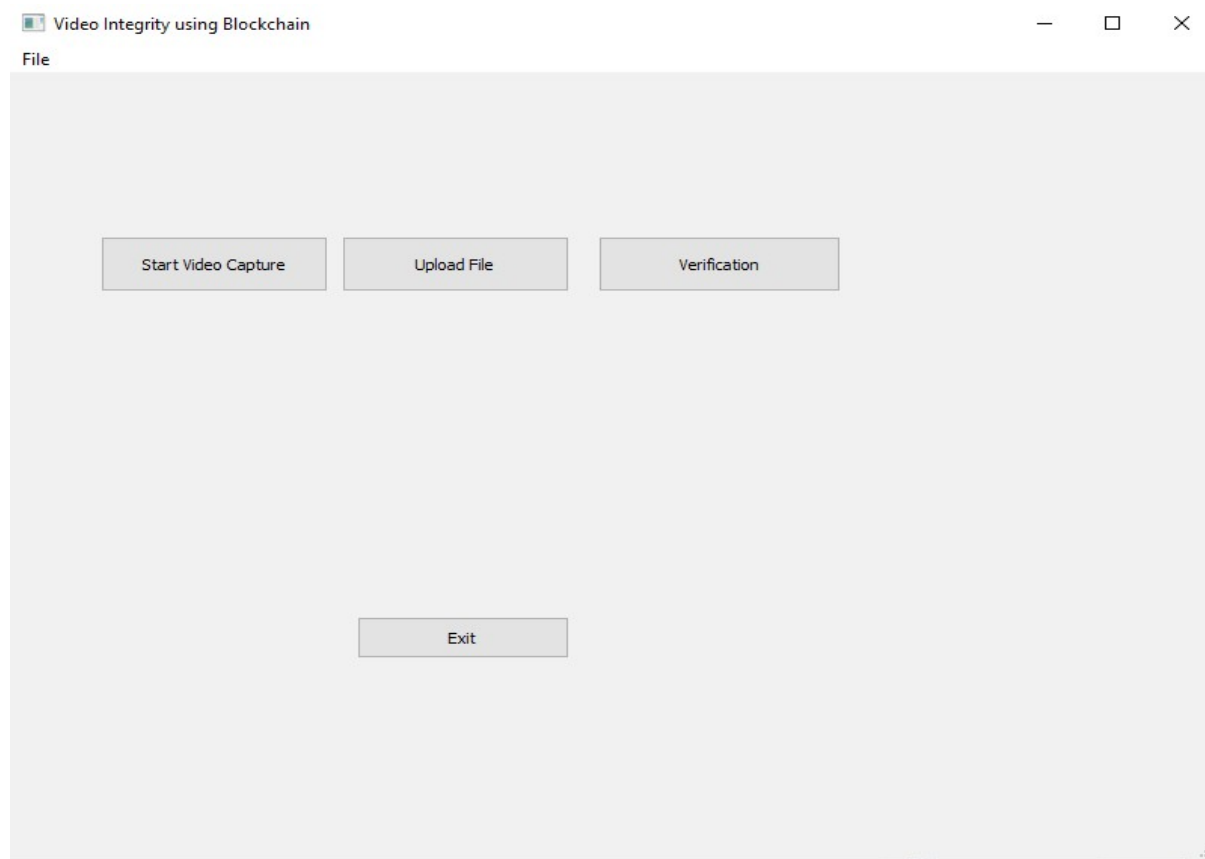
- 1) PyQt5 is a lightweight python GUI framework that is used to display the user interface.

# Experimental Evaluation

- Done testing with the developed system and it works successfully.
- Few difficulties were encountered due to lack of resources.
- Identified issues with delay in creation of blockchain node due to limited system resources.
- PyQt5 framework used to develop GUI takes more memory and with current configuration of the system it takes time to load the initial window.

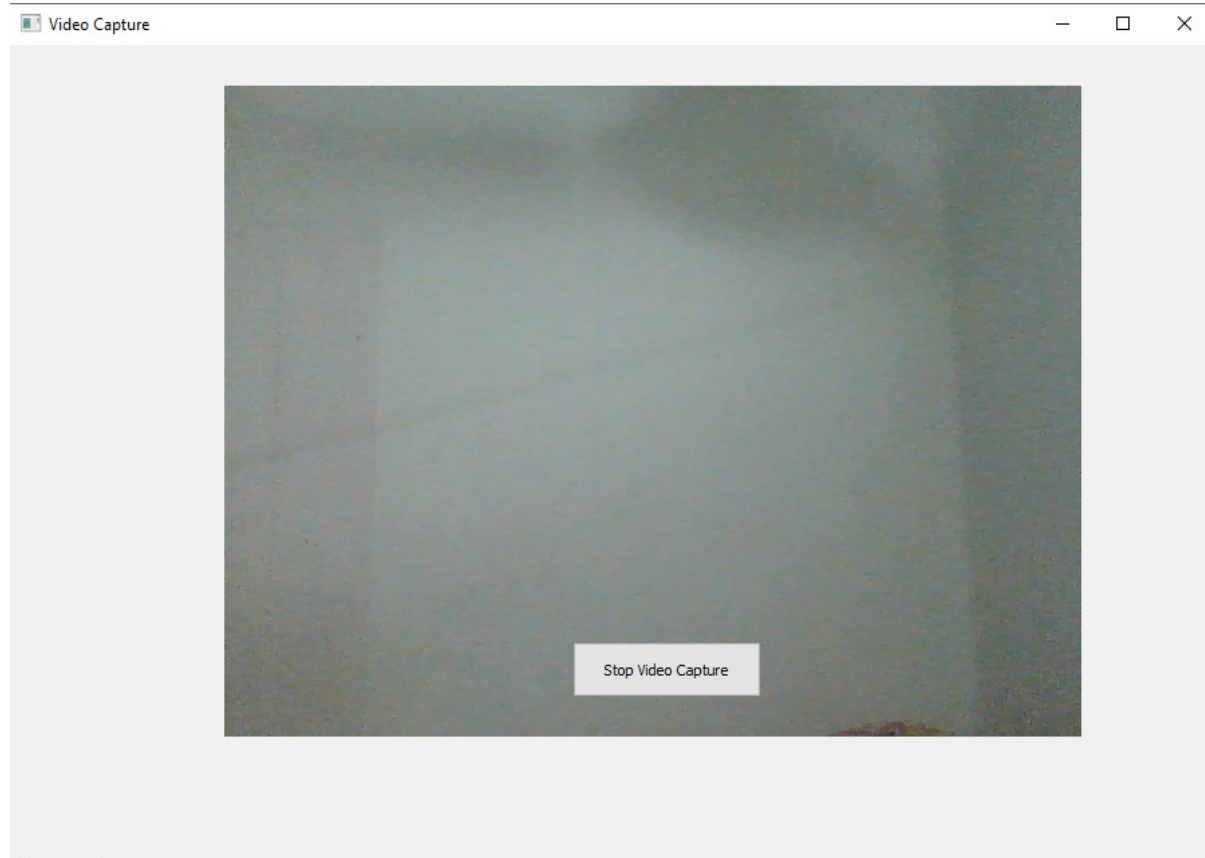
# Screenshots

## Main form




# Screenshots

## Capture Video from Webcam



# Screenshots

## Blockchain Transactions

Ganache

ACCOUNTS

BLOCKS

TRANSACTIONS

CONTRACTS

EVENTS

LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK  
23

GAS PRICE  
20000000000

GAS LIMIT  
6721975

HARDFORK  
MUIRGLACIER


NETWORK ID  
5777

RPC SERVER  
HTTP://127.0.0.1:7545

MINING STATUS  
AUTOMINING

WORKSPACE  
ORGANIC-BRAKE

SWITCH

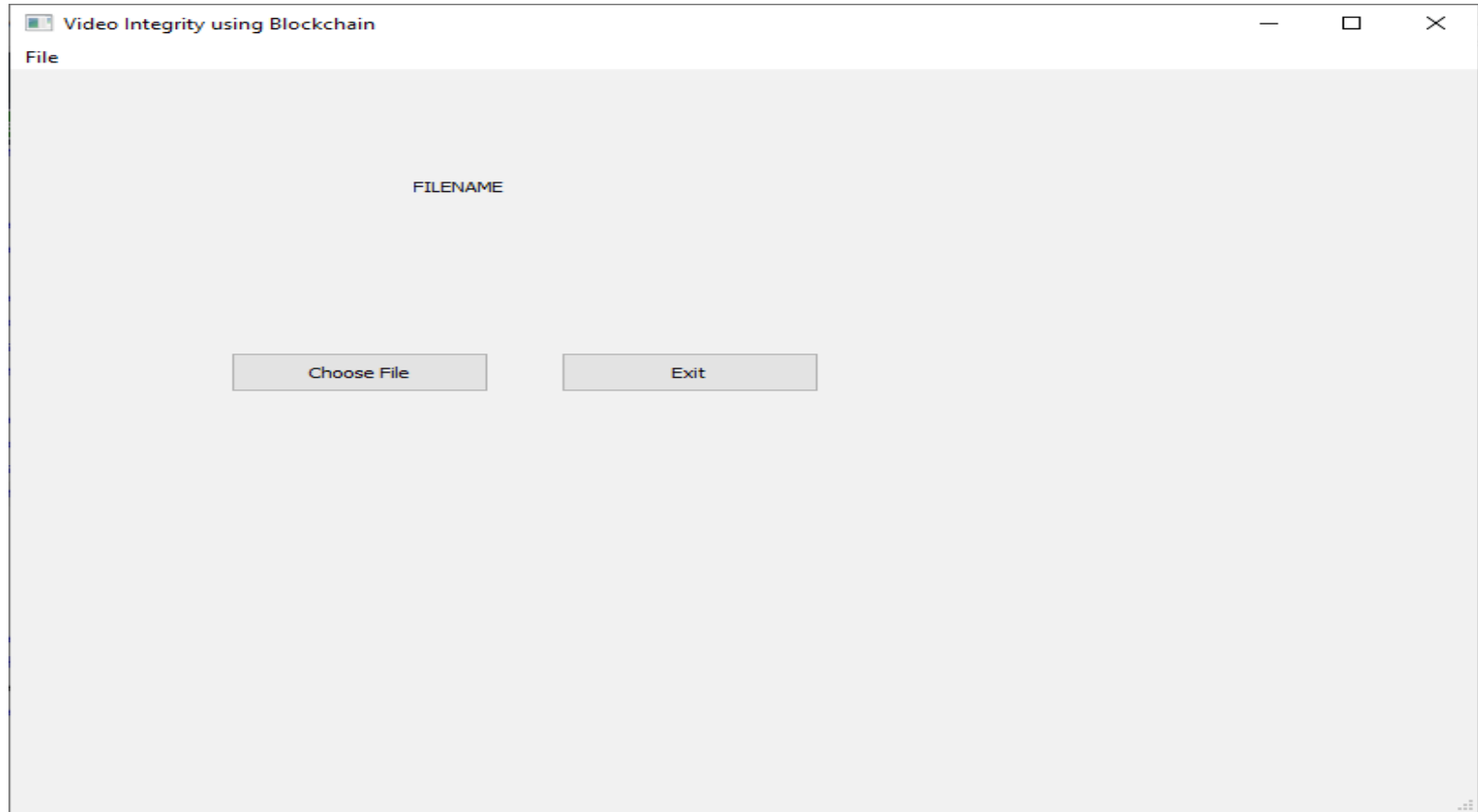


TX HASH <b>0x1051883bc64bd91f5ae0d98b05f8c1ee5a636500ddccb9533ec7ebc912946338</b>	<div>CONTRACT CALL</div>		
FROM ADDRESS 0x8E7eA024AF926d9B41E39346D65EA3d7d3874850	TO CONTRACT ADDRESS 0x6e0d73dff772ad017E3AEa1cfb53E87E3FCb54a0	GAS USED 587186	VALUE 0
TX HASH <b>0x70f78adab2c1591934b711f1a38a050fd494e2d3be0c55018602e581bc9b4a06</b>	<div>CONTRACT CALL</div>		
FROM ADDRESS 0x8E7eA024AF926d9B41E39346D65EA3d7d3874850	TO CONTRACT ADDRESS 0x6e0d73dff772ad017E3AEa1cfb53E87E3FCb54a0	GAS USED 557197	VALUE 0
TX HASH <b>0x2c93357f7f6f141e25432fd5a3c2da2bd3d881e0ffdc3bfd8f55e4f702d415a</b>	<div>CONTRACT CALL</div>		
FROM ADDRESS 0x8E7eA024AF926d9B41E39346D65EA3d7d3874850	TO CONTRACT ADDRESS 0x6e0d73dff772ad017E3AEa1cfb53E87E3FCb54a0	GAS USED 527207	VALUE 0
TX HASH <b>0xa57df64fc308289c10d522c7ca1d170e9853e0b9682fda3da20065ff1ebbf39e</b>	<div>CONTRACT CALL</div>		
FROM ADDRESS 0x8E7eA024AF926d9B41E39346D65EA3d7d3874850	TO CONTRACT ADDRESS 0x6e0d73dff772ad017E3AEa1cfb53E87E3FCb54a0	GAS USED 497218	VALUE 0



# Screenshots

## Video Verification Form



The screenshot shows a software window titled "Video Integrity using Blockchain". The window has a standard Windows-style title bar with minimize, maximize, and close buttons. Below the title bar is a menu bar with the option "File". The main area of the window is light gray and contains a text input field labeled "FILENAME". Below the input field are two buttons: "Choose File" and "Exit".

Video Integrity using Blockchain

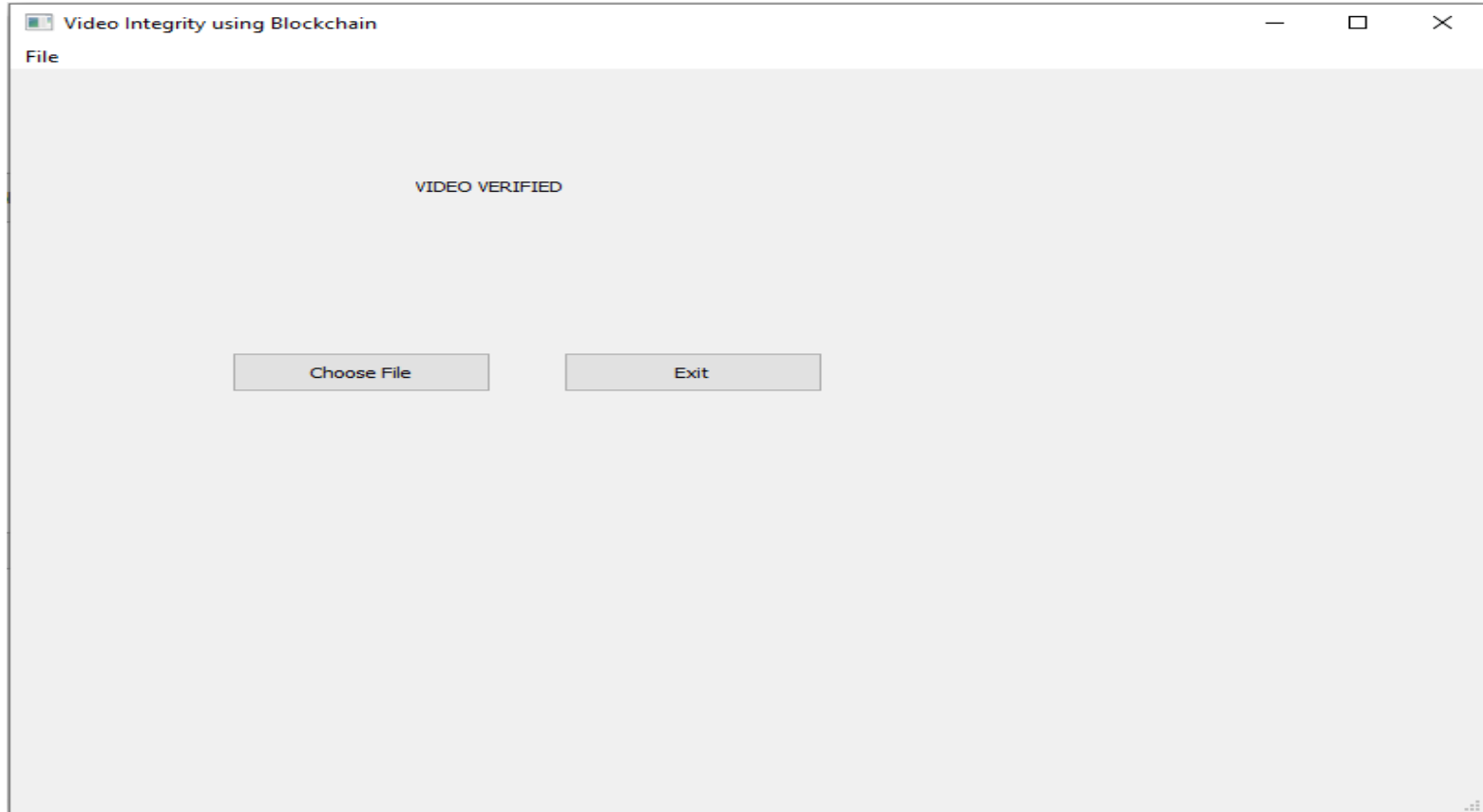
File

FILENAME

Choose File Exit

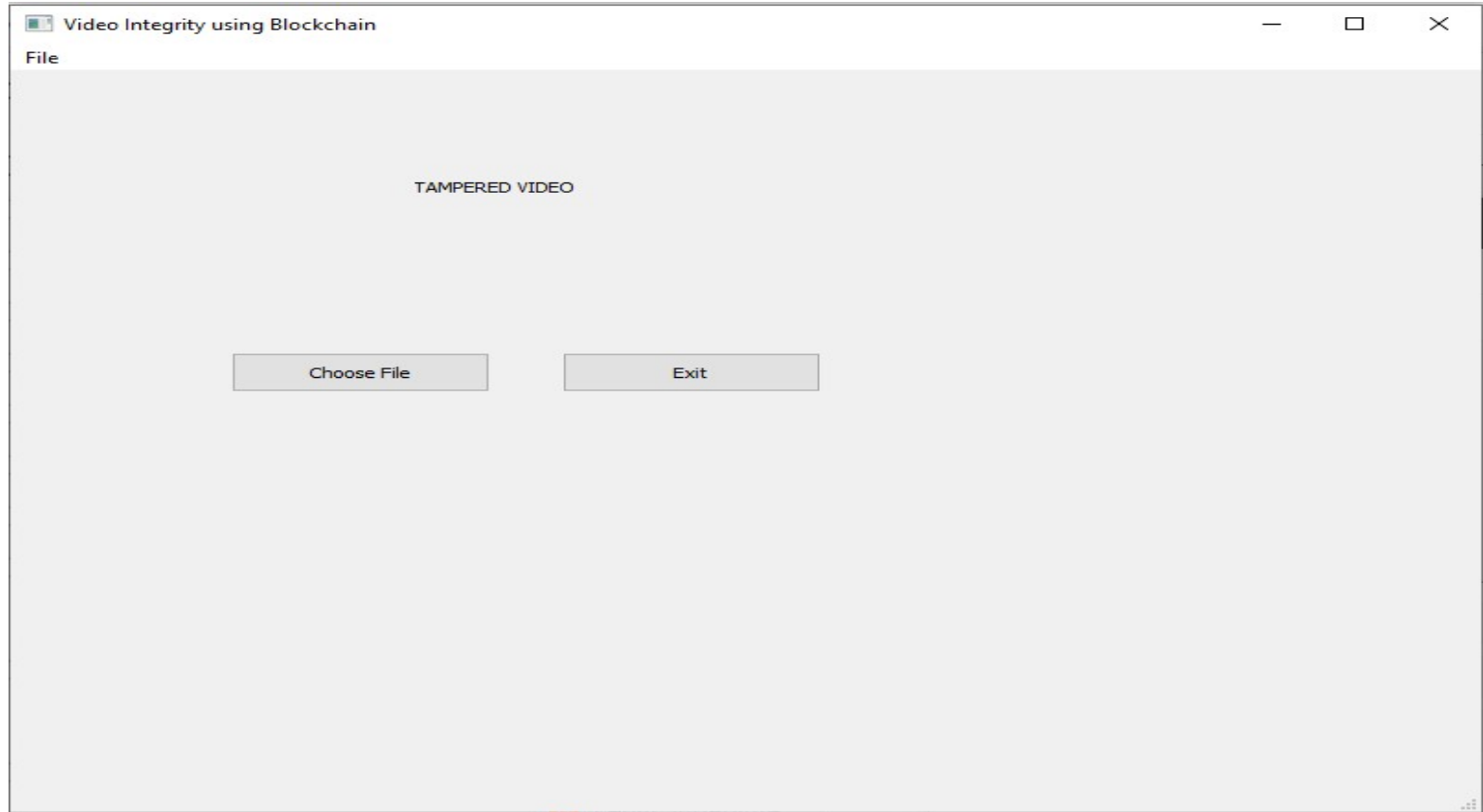
# Screenshots

## Video Verification - Success



# Screenshots

## Video Verification – Tampered Video Identification



# Result

- The main feature of the project has been met.
- It is able to verify the integrity of the video with 100% accuracy.
- Detection of any tampering is detected by powering the combined use of cryptography and blockchain technologies.

# Future Scope

- Segmentation of videos for better complexity.
- Making the raw video footage available in the Blockchain for public access.
- Apply the method for other types of files like audio, images and documents.

# Conclusion

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