REVERSIBLE DATA HIDING IN ENCRYPTED VIDEOS BY REVERSIBLE IMAGE TRANSFORMATION

A PROJECT PRELIMINARY REPORT

by

ASHWIN JOSHY (VJC18CS033)
BIMAL S KUMAR (VJC18CS043)
KARTHIK RAMESH (VJC18CS070)
RUBIN SABU (VJC18CS098)

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
VISWAJYOTHI COLLEGE OF ENGINEERING AND TECHNOLOGY, VAZHAKULAM
NOVEMBER 2021

REVERSIBLE DATA HIDING IN ENCRYPTED VIDEOS BY REVERSIBLE IMAGE TRANSFORMATION

A PROJECT PRELIMINARY REPORT

by

ASHWIN JOSHY (VJC18CS033)
BIMAL S KUMAR (VJC18CS043)
KARTHIK RAMESH (VJC18CS070)
RUBIN SABU (VJC18CS098)

in partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

under the guidance

of

Mrs. Mili Els JOSE

Assistant Professor, CSE Dept.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
VISWAJYOTHI COLLEGE OF ENGINEERING AND TECHNOLOGY, VAZHAKULAM

NOVEMBER 2021

VISWAJYOTHI COLLEGE OF ENGINEERING AND TECHNOLOGY, VAZHAKULAM

Department of Computer Science and Engineering

Vision

Moulding socially responsible and professionally competent Computer Engineers to adapt to the dynamic technological landscape

Mission

1. Foster the principles and practices of computer science to empower life-long learning and build careers in software and hardware development.

2. Impart value education to elevate students to be successful, ethical and effective problem-solvers to serve the needs of the industry, government, society and the scientific community.

3. Promote industry interaction to pursue new technologies in Computer Science and provide excellent infrastructure to engage faculty and students in scholarly research activities.

Program Educational Objectives

Our Graduates

1. Shall have creative aid critical reasoning skills to solve technical problems ethically and responsibly to serve the society.

2. Shall have competency to collaborate as a team member and team leader to address social, technical and engineering challenges.

3. Shall have ability to contribute to the development of the next generation of information technology either through innovative research or through practice in a corporate setting

4. Shall have potential to build start-up companies with the foundations, knowledge and experience they acquired from undergraduate education

Program Outcomes

1. **Engineering knowledge**:Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

2. **Problem analysis**:Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences

3. **Design / development of solutions**:Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

4. **Conduct investigations of complex problems**:Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

5. **Modern tool usage**:Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.

6. **The engineer and society:**Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

7. **Environment and sustainability:**Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

8. **Ethics:**Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice

9. **Individual and team work:**Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings

10. **Communication:**Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

11. **Project management and finance**: Demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and unread in a team, to manage projects and in multidisciplinary environments.

12. **Life-long learning**:Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

Program Specific Outcomes

1. Ability to integrate theory and practice to construct software systems of varying complexity
2. Able to Apply Computer Science skills, tools and mathematical techniques to analyse, design and model complex systems
3. Ability to design and manage small-scale projects to develop a career in a related industry.

VISWAJYOTHI COLLEGE OF ENGINEERING AND TECHNOLOGY, VAZHAKULAM

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

Certified that project work entitled **" Reversible Data Hiding In Encrypted Videos By Reversible Image Transformation "** is a bonafide work done by **Mr. Ashwin Joshy** University Register No.**VJC18CS033**, **Mr. Bimal S Kumar** University Register No.**VJC18CS043**, **Mr. Karthik Ramesh** University Register No.**VJC18CS070**, **Mr. Rubin Sabu** University Register No.**VJC18CS098** in partial fulfillment of the award of the Degree of Bachelor of Technology in Computer Science & Engineering from APJ Abdul Kalam Technological University, Thiruvananthapuram, Kerala during the academic year 2021-2022

Internal Supervisor **External Supervisor**

Mrs. Mili Els Jose
Project Coordinator
Asst. Professor
Dept. of CSE, VJCET

Mr. Amel Austine
Head of Department
Asst. Professor
Dept. of CSE, VJCET

ACKNOWLEDGEMENT

First and foremost, we thank **God Almighty** for His divine grace and blessings in making all these possible. May He continue to lead us in the years. It is our privilege to render our heartfelt thanks to our most beloved Manager **Msgr. Dr. Pius Malekandathil** ,our director **Rev. Fr. Paul Nedumpurath** and our Principal **Dr. K K Rajan** for providing us the opportunity to do this project during the Fourth year (2022) of our B.Tech degree course. We are deeply thankful to our Head of the Department, **Mr. Amel Austine** for his support and encouragement. We would like to express our sincere gratitude and heartfelt thanks to our Project Guide **Mrs. Mili Els Jose**, Assistant Professor, Department of Computer Science and Engineering for his motivation, assistance and help for the project. We also express sincere thanks to our Project Coordinator **Mrs. Mili Els Jose**, Assistant Professor, Department of Computer Science and Engineering for their guidance and support. We also thank all the staff members of the Computer Science Department for providing their assistance and support. Last, but not the least, we thank all our friends and family for their valuable feedback from time to time as well as their help and encouragement.

DECLARATION

We undersigned hereby declare that the project report "Reversible Data Hiding In Encrypted Videos By Reversible Image Transformation", submitted for partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology of the APJ Abdul Kalam Technological University is a bonafide work done by us under the supervision of Mrs. Sindhu Jose. This submission represents ideas in our own words and where ideas or words of others have been included, We have adequately and accurately cited and referenced the original sources. We also declare that We have adhered to the ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We 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 formed the basis for the award of any degree, diploma or similar title of any other University.

Place : Vazhakulam

Date : .....

Ashwin Joshy

Bimal S Kumar

Karthik Ramesh

Rubin Sabu

ABSTRACT

In recent years, due to the steady increase in the popularity of outsourcing data to the cloud, it is crucial to preserve and protect the privacy of data and allow the cloud server to easily manage the data at the same time. Under these demands, our proposed system implements Reversible Data Hiding in encrypted videos. Reversible Image Transformation is also used which encrypts the original image to form the target image. The RIT-based framework allows the user to transform the content of the original image into the content of another target image of the same size. The transformed image, which looks like the target image, is used as the "encrypted image", and is outsourced to the cloud. The proposed system has the added advantage of encrypting videos uploaded by users onto the cloud thus securing its content. We also use multi-MSB (most significant bit) prediction and Huffman coding as an encryption strategy in the proposed system.

Key Words :– RDH (Reversible Data Hiding), MSB-Prediction, Huffman Coding, RIT (Reversible Image Transformation), CIT (Class Index Table), Encryption, Decryption

Contents

List of Figures

List of Abbreviations

RDH	Reversible Data Hiding
RIT	Reversible Image Transformations
CIT	Class Index Table
AI	Accessorial Information

Chapter 1

INTRODUCTION

The cloud is an emergent technology that is widely used.It can be used to store user data.The security of data being transmitted via cloud has become very important especially in situations that handle sensitive information such as military applications.Here arises a need to protect the privacy of data being transferred.There can be different reasons for encrypting videos.For instance,if a user wants to hide a confidential video in the cloud.So, an efficient system is proposed that implements Reversible Data Hiding (RDH) in encrypted images.In RDH, Original image is extracted by removing data/message that was embedded into it.Reversible Image Transformation (RIT) is also a technique that is implemented with regard to encrypted images/videos. In RIT,the content of an image is transformed to another image of same size.

1.1 Problem Definition

The existing cloud services do not provide much secure encryption on all types of confidential data that are stored in the cloud. The current system offers lack of concealment when encrypting video data that is sent by users to receiver via the cloud.

1.2 Objective

To allow users to upload videos on to cloud in a more encrypted form thus providing more security and confidentiality.It deals with the hiding of original video in another video and then encrypt and embed it with additional secret data.

1.3 Scope

As discussed in the problem definition, the conventional methods provide less encryption .The proposed system helps implement secure video transmission through cloud by Reversible Data Hiding and Reversible Image Transformation.It applies to military applications wherein highly sensitive data can be securely stored and transmitted.In the medical field, confidential video data of patients needs to be protected in case the storage is hacked.In Law Forensics, the data collected for investigation purpose should be stored securely to prevent illegal access.So, our proposed video encryption system can satisfy many such applications.

Chapter 2

LITERATURE SURVEY

2.1 Reversible Data Hiding in Encrypted Images by Reversible Image Transformation

These days outsourced storage by the cloud turns into an important service, particularly for media records, for example, images or recordings, which need huge extra room. To deal with the re-appropriated images, the cloud server might implant a few extra information into the images, like picture classification and documentation data, and utilize such information to distinguish the ownership or verify the integrity of images. In this IEEE paper we are able to find an efficient data hiding method in encrypted images using Reversible Image Transformation.

This system finds an efficient data hiding method in encrypted images using RDH. Initially the original image and a target image is selected. The target image will have equal or greater size with the original image. Then both the images are divided into N blocks that are non-overlapping. After the division they take the mean and standard deviation(SD) for each block in both original image and target images. Then these blocks are sorted in the ascending order of the SD for both original and target images. From the sorted data blocks are classified into 2 classes. Class 0 for smaller values of SD and class 1 for higher values of SD.

After classification, each block in the original image is paired with the corresponding target image block which has the same class and same block number. Then they calculated the mean difference of the blocks in each pair and it is added to each pixel of the original block. Now a transformed block is generated. To make further similarity between the target image and transformed image, we rotate the transformed image in θ(0/90/180/270) degree. Thus the final transformed image is formed.

The mean difference and θ of each block are compressed with the CIT of I and then encrypted with AES using key K. This is then embedded with the transformed image to form the final encrypted image. Decryption is the reverse process of encryption.

2.1.1 Advantages

- We can transform the original image to an arbitrary selected target image with the same size for better encryption.
- We can restore the original image from the encrypted image in a lossless way.
- The cloud server can easily embed data into the “encrypted image”.

2.1.2 Disadvantages

- Only applicable to images.
- Limited amount of data is applicable for embedding.

2.2 Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models

This IEEE paper deals with data hiding in encrypted 3D mesh models.First step is to map decimals belonging to vertex coordinates to integers in order to execute bit-stream encryption. Many least-significant bits are operated to embed the data with the help of data-hiding key. Content of mesh can only be roughly created with the aid of encryption key. Only with the help of spatial correlation in the natural mesh models original mesh and the secret data which is embedded can be extracted and recovered.

2.2.1 Advantages

- Can be used to encrypt 3D meshes.
- Both encryption and data hiding key is needed to recover the mesh perfectly.
- This method has a high data-embedding payload.
- This maintains high values of the decrypted meshes and has a low computational complexity.

2.2.2 Disadvantages

- Can only be used for encrypting 3D meshes.
- This method is mainly aimed at non-separable RDH schemes but not separable RDH schemes.

2.3 Encrypted signal-based reversible data hiding with public key Cryptosystem

This system uses an encrypted signal based RDH with public key cryptosystem. Here Paillier homomorphic encryption is also used. Here the user generates encrypted signal and hider does another encryption and also emedding. Hider performs all of this with receivers public key. Advantage obtained here is increased payload and high and better signal quality.

2.3.1 Advantages

- Has more payload than other EIRDH schemes.
- Higher signal quality than other EIRDH schemes.
- ESRDH scheme allows multiple signal providers and data hiders since they know the receiver's public key unlike C—EIRDH which has specific providers and hold shared keys.
- ESRDH scheme is based on public key encryption, and thus the encrypted signal or that with the embedded message can be delivered directly. (secure channel not necessary).

2.3.2 Disadvantages

- Limited amount data for embedding.

2.4 An Improved Reversible Data Hiding in Encrypted Images Using Side Match

This system uses a side match technique for RDH in encrypted images.This paper adopts a better scheme for measuring the smoothness of blocks (as compared to another method called Zhang's RDH method in encrypted images).In the paper,an encrypted image is partitioned into blocks,each block carries a single bit by flipping three LSBs of a set of pre-characterized pixels.Here a side match technique implementation is used to additionally reduce error rate of recovered bits. The entity that owns the data/content needs to cipher it before sending it for data embedding process.A randomly generated sequence r is used to encrypt cover image. XOR operation is performed on bits of I and r to get a new equation consisting of I'(encrypted image). For embedding, I' is partitioned into uncorrelated blocks with each block able to accomodate a single bit.The perfection/smoothness of a picture block is assessed by performing modulus of difference between adjacent/neighboring pixels. Greater the modulus value, more complex is the picture block.The block smoothness is determined here by adding the modulus value of vertical and horizontal differences of the image block pixels.The side match strategy helps to connect the boundaries of the recuperated blocks to the unrecuperated blocks and then implement smoothness evaluation.

2.4.1 Advantages

- Enhanced Data Extraction.
- Improved Image Recovery Strategy (as compared to Zhang's work).
- EA new algorithm to better estimate the smoothness of image blocks is used.
- Reduce error rate.

2.4.2 Disadvantages

- For large sized blocks, results are not as accurate as smaller sized blocks.

2.5 Secure Reversible Data Hiding video Trans- formation using cloud storage

This paper propses a secure video transformation system in cloud storage. Cloud is an eminent technology.The data stored in cloud needs to be preserved and protected.Cloud offers various services such as SaaS, PaaS, IaaS.Cloud is less costly, reliable, flexible. Cloud is also polpular for storing multimedia files that usually take up a lot of storage space.To protect the transferred images from the sender, some data is embedded to the images to verify the owner.RDH is used to obtain the original image by removing the embedded message.RIT moves initial image I content to related representation(semantic) of another image j of similar size as I.In this system, RIT is

implemented in videos where a video can be embedded into a target image.Here video frames are produced and each frame is encrypted and hiding is performed using target image (target image has greater size than frame). Later, after sending the frame along with target image to cloud, the receiver receives the video from CSP. This system proposes video hiding in another image.For maintaining security, the video frames produced are encypted and (each frame) hid to another image. Then a new video is produced containing only the target image (i.e. video with target image stream).Corresponding to each frame in the video, target image is repeatedly chosen.An authentication mechanism (based on ID) is used for user authentication.This newly produced video is sent to cloud.Target image is also sent along with it.Ownership details are present in the image. First, a user selects a video that is needed to be outsourced to cloud.Video frames are produced and each of them is encypted and hiding (LSB hiding) is done.A target image that needs to be hidden is selected (repeatedly chosen).After hiding, a new video that has only target image as frames is produced and sent to cloud(along with target image).A key is produced that is used for encryption and the same for decryption too. Details like ownership and watermarking is embedded into the target image. According to a user request, the CSP provides the video stored in cloud.It is additionally managable to unscramble and get the first video utilizing the common key.

2.5.1 Advantages

- The user can outsource the data to the cloud in a secured manner.
- This work improves the security of the data and provide authentication.

2.5.2 Disadvantages

- Complex process for image transformation.

2.6 Double Faced Data Hiding in Images and Videos using RIT Approach

This paper proposes a Double faced data hiding technique in images and videos , the system outsources the original image to cloud and it encrypts the original image to encrypted video. Just like all the other RDH methods , here the original image is reproduced losslessly after extracting the embeded data. In case of Image hiding, first the Image is given as input then a target image of equisize is selected from database. After that the data to be hidden is encrypted using AES and then it gets embedded to the final image. After the above process, the encrypted image is forwarded to cloud.

2.6.1 Advantages

- User can decide what to embed and how to encrypt through cloud.
- Increased Embedding capacity.

2.6.2 Disadvantages

- Strong network connection is needed since majority of operation is through cloud.

Chapter 3

PROPOSED SYSTEM

The proposed system provides a much more secure way for videos to be sent via the cloud. This system implements more efficient encryption and a protected cloud storage mechanism where videos can be stored more securely. It also has a higher data embedding capacity.

3.1 Architecture Diagrams

Figure 3.1: Architecture Diagram

Figure 3.2: Usecase Diagram

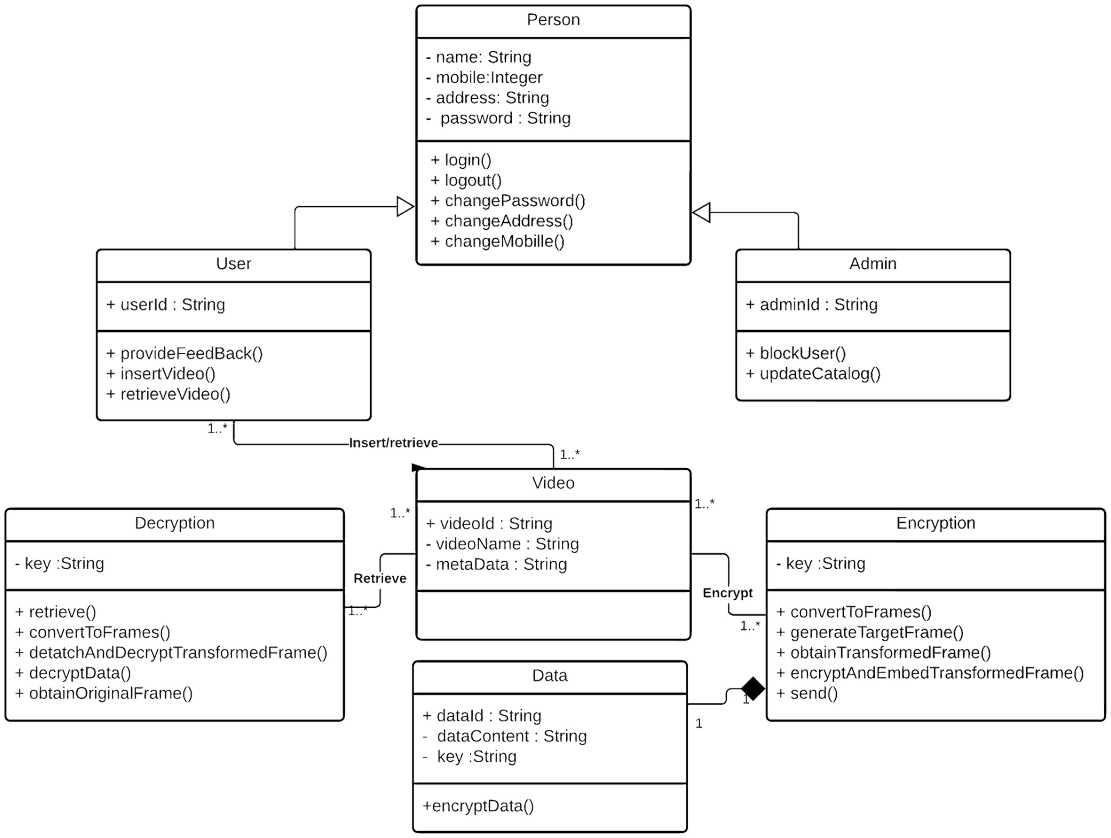


Figure 3.3: Class Diagram

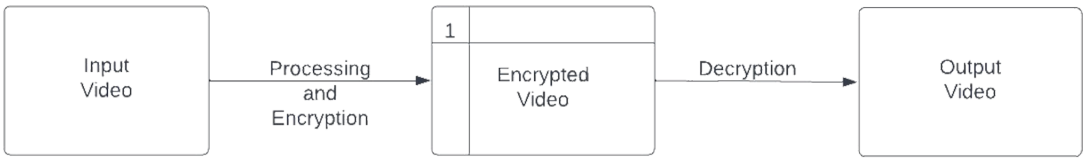


Figure 3.4: DFD Level 0 Diagram

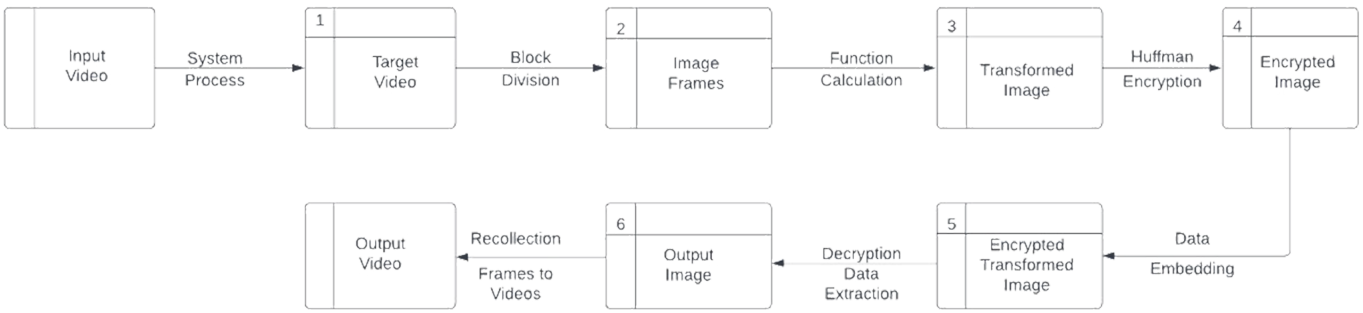


Figure 3.5: DFD Level 1 Diagram

3.2 System Requirements

The basic requirements for the proposed systems is the hardware for capturing the ‘image and software for its processing and producing the required output.

3.2.1 Hardware Requirements

The hardware requirements consist of a laptop with a quadcore processor with 4GB RAM or more for running the MATLAB, Python and processing the image. Along with this, a preferable GPU is required for faster image processing and producing faster output results.

3.2.2 Software Requirements

The softwares are generally for coding and execution of algorithms. The software platforms used in this system are MATLAB and IDE for running Python.

3.2.3 MATLAB

The MATLAB has been used for processing the image like conversion of color image into binary image, Hole filling, Border clearing and deleting the small objects in the image.

3.3 Implementation Details

The primary aim of this project is to give more protection for the videos that are uploaded to cloud storage. From the research of the related papers we had, a more secure data embedding system is created.

In our proposed system, we give the original video as the initial input. Also, a target video with the same size as the original video is taken. As we are using the RIT-based technique, we need to divide both the videos into frames with, both original and target video frames having the same size. Considering each frame pair (I, J), RIT is performed on them.

In RIT, we initially divide the original video frame and the target video frame into N blocks which are non-overlapping. For each block, the mean and standard deviation(SD) is calculated. By considering the SD of each block for the original and targeted frame, we classify the blocks into two classes. Smaller values of SD will be in class 0 and higher values of SD will be in class 1. Then each original frame-block is paired with its corresponding target frame-block. That is, the jth block of ith class in the original frame is paired with the jth block of ith class in the target frame.

Now we have block pairs as (B, T) [2], where B is the original frame block and T is the target frame-block. The mean difference for B and T is calculated. To get the transformed block we add the mean difference to the original frame-block. To maintain the similarity of the transformed image with the target image, we rotate the transformed block into a θ degree (θ = 0/90/180/270). Then each target block is replaced by the transformed block to form the transformed image T'.

In the proposed framework, we find out label map of the first picture initially and install it onto encrypted picture [1].For this, think about initial image I of size m x n, we work out the predicted worth(value) per pixel (px) with the help of a Median Edge Detector. The approach in MED considers the 3 neighbouring pixels(left, top and diagonally left) around current pixel x(i,j). Next, we need to convert current pixel values(x) and predicted pixel values(px) into a 8-digit paired grouping.

Then we compare these $x^k(i,j)$ and $px^k(i,j)$ bit wise sequentially from MSB to LSB and stop when a particular digit/bit is dissimilar and present pixel label equals length of their same bits.Now since there are 8 bits in converted binary sequence, there are 9 cases for the label of the pixel(0 to 8).We also take into account certain values called tag values that range from 0 to 8.Consider t as tag value for the present pixel location.This indicates that it can place (t+1) bits.n.Next is the image encryption phase where individual pixels from initial image is encrypted wth the help of Ke. Here Ke is the encryption key.An arbitrary random matrix r is created with similar size as initial image i.e.m x n.Now we convert current value for the pixel x(i,j) and corresponding r(i,j) into 8-bit sequence.This sequence is then encrypted. In this way , encrypted image is obtained.The mean difference and the of every block is taken and embedded in the image can be obtained from original image label map (needs to be changed into a binary sequence as additional data).

There are 9 types of labels for pixels in a natural image, so we use 9 binary codes to represent all the various labels.Since the number of each label differs, the label map is recorded through Huffman coding.Huffman coding compresses auxiliary information thus increasing image payload. So, we predefine 9 types of Huffman codes to represent 9 types of labels, as 00, 01, 100,101, 1100, 1101, 1110, 11110, 11111.Sort the 9 label types by the number of pixels.Label with a greater number of pixels is represented using shorter code and label with a lesser number of pixels is represented using larger code. For the 9 Huffman codes, "00" is used in the place of a label having largest pixel count, and "11111" represents the label with the least pixel count(number of pixels).To create more storage facility in the encrypted image, there arises a need to embed label map.In encrypted image Ie, first convert the label map into a binary sequence by Huffman cod- ing. Then take the Huffman coding rule, the binary sequence, and the length of the binary sequence as auxiliary information.

The next stage is embedding of Label map, here in order to create more space to increase embedding capacity we use label map and embed it in image. Using Huffman coding we need to form a binary sequence by converting the label map. Then we take Huffman coding rule, binary sequence and it's length as information to embed.Next, first row and column of reference pixel is used to store Partial Aux information. It's because aux information acquired from previous pixel is used to determine label of current pixel. At last, multi-MSB substitution is used to embed auxiliary info and reference pixels replaced.

Then for Data hiding, the label map and Huffman coding rule are extracted from the encrypted image before hiding data. First, extract the partial auxiliary info in the reference pixel to obtain the Huffman coding rule and length of auxiliary information. Then, as per the existing Huffman coding rule and aux info, the 't' tag value of the present pixel is attained, and bits of (t+1) aux info are taken out. We restore the label map formed on the Huffman coding rule after obtaining aux info. The additional data is finally integrated in the remaining pixels, which contain space reserved for embedding the in the encrypted image, in accordance with Multi MSB Eqn. As a result,the encrypted image which is marked with add-on data is produced.Before embedding, we encrypt it using the key which is used to hide data to increase its security.The receiver can take out the label map and Huffman code rule from encrypted image which was marked, for extracting data and recovery of image. Then, the additional encrypted data and reference pixel are taken out using label map in a similar manner. Then reference pixels are placed to first row and column as before.Based on key receiver owns:

1. The embedded data can be accessed by directly decrypting extracted encrypted additional data if the receiver has the key which was used to hide data.
2. The original picture can be retrieved if receiver possesses the Img encryption key.

At first, the image obtained is decrypted using the pseudo-random matrix "r" produced with image encryption key, we get decrypted image . In the decrypted image, the (t+1) front bits in each of the pixels differ from the original pixels except the reference. Next, scan all pixels in the image from left to right and top to bottom except reference pixel. The MED predictor is used to calculate the current pixel's predicted value, px(i,j). After that the original pixel x(i,j) is then reconstructed as per the 't' tag value and the predicted value px(i,j). Therefore, in order to extract the add-on data and recreate the original image, both the data concealment key and the image encryption key are required.

Chapter 4

RESULTS

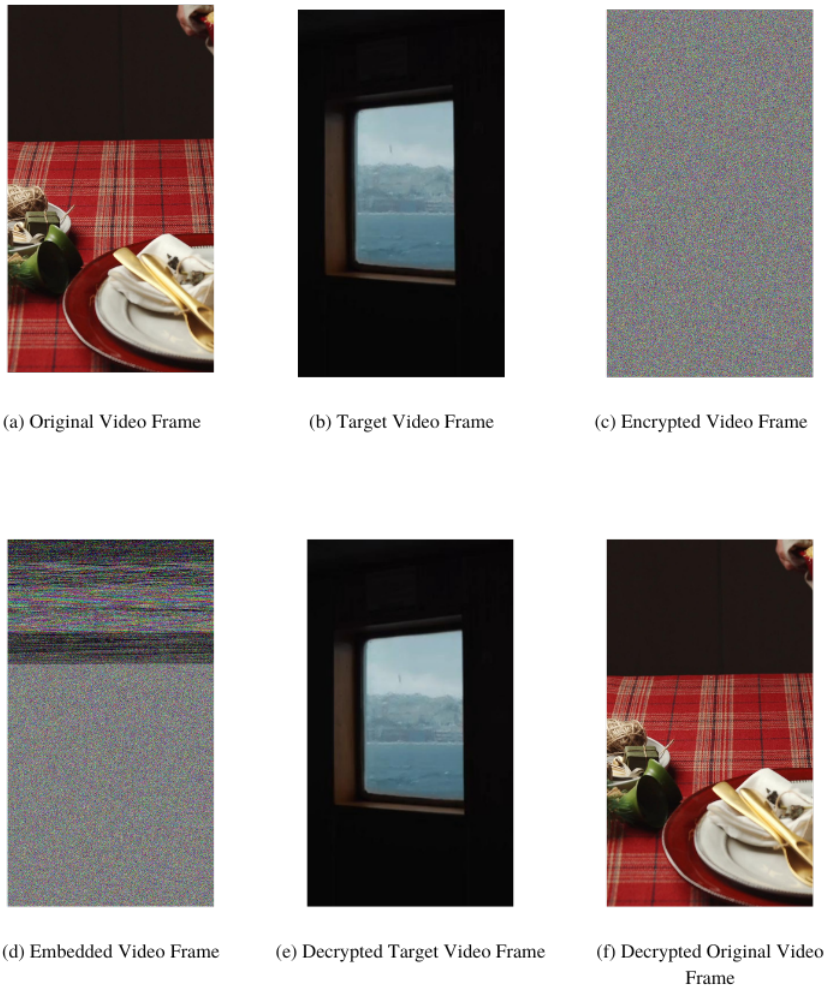
The proposed system was tested with a system having the following specifications:

- Ram - 8GB
- processor - Ryzen 5
- OS - Windows 11

The user interface works by taking the key and data from the user and the frame (as well as the data) is encrypted. Later,on decryption, the decrypted data is saved onto a text file and the decrypted frame is saved in MP4 file format.

Table 4.1: Observation

Resolution	***Capacity in Bits***
256*144	427530
852*480	5249072
1280*720	12319695
1920*1080	29785518
4096*2060	137414248



(a) Original Video Frame

(b) Target Video Frame

(c) Encrypted Video Frame

(d) Embedded Video Frame

(e) Decrypted Target Video Frame

(f) Decrypted Original Video Frame

Figure 4.1: Proposed System Result

Chapter 5

CONCLUSIONS

As cloud computing is gaining more and more attraction, the need for secure storage of data is increasing in demand. As in existing systems, the encryption of different types of data is limited and less secure. Through our proposed system, we have introduced a more secure way to encrypt videos and embed data inside them. In this system, we use Separable Reversible Data Hiding method in order to encrypt video and data. Hence the security is increased. In our proposed work we use Reversible Data Hiding technique to hide data and separate video into frames and then apply Reversible Image Transformation using the frames of a target video and then encrypt the image and data using Multi- MSB Prediction and Huffman coding. This provides high data embedding capacity and enhanced encryption. An improvement to our proposed system would be to encrypt the audio factor of the video.

References

[1] Weiming Zhang; Hui Wang; Dongdong Hou; Nenghai Yu, “Reversible Data Hiding in Encrypted Images by Reversible Image Transformation” IEEE Transactions on Multimedia (Volume: 18, Issue: 8, Aug. 2016), DOI: 10.1109/TMM.2016.2569497.

[2] Ruiqi Jiang; Hang Zhou; Weiming Zhang; Nenghai Yu, “Reversible Data Hiding in Encrypted Three-Dimensional Mesh Models” IEEE Transactions on Multimedia (Volume: 20, Issue: 1, Jan. 2018).,DOI: 10.1109/TMM.2017.2723244

[3] Yu-Chi Chen; Chih-Wei Shiu; Gwoboa Horng, “Encrypted signal-based reversible data hiding with public key cryptosystem” Journal of Visual Communication and Image Representation Volume 25, Issue 5, July 2014, Pages 1164-1170,DOI:10.1016/j.jvcir.2014.04.00

[4] Wien Hong; Tung-Shou Chen; Han-Yan Wu, “An Improved Reversible Data Hiding in Encrypted Images Using Side Match” IEEE Signal Processing Letters (Volume: 19, Issue: 4, April 2012), DOI: 10.1109/LSP.2012.2187334

[5] Amrutha OC, Rabina P, "Secure Reversible Data Hiding video Transformation using cloud storage"

[6] Santosh Dinkar Kale, Dr. Neeta Deshpande, "Double Faced Data Hiding in Images and Videos using RIT Approach"

Appendix A

Reversible Image Transformation

```
function RI=Extract_Secret_From_Transformed_Image(app,Mosaic,Key)
    %Input:The transformed image to be extracted to original image
    %Output:Recovered image
    %This function converts transformed image back to org IMG
    try
    n=4;
    [M,N,ch]=size(Mosaic);
    numberOfblocks=M*N/n^2;
    Mosaic=double(Mosaic(:));
    len_ld=Mosaic(end);
    for i=len_ld:-1:1
       ld(i)=num2str(Mosaic(end-i));
    end
    ld=str2double(ld);
    dat=rem(Mosaic,4);
    dat=dat(1:ld);
    dat=de2bi(dat,2);
    data=dat(:);
    dec=bi2de(reshape(data,length(data)/8,8))';%Converting back to decimal
    %Retrieving auxilary data from transformed image
    muR1=dec(1:numberOfblocks);
    muG1=dec(numberOfblocks+1:2*numberOfblocks);
    muB1=dec(2*numberOfblocks+1:3*numberOfblocks);
    muR=dec(3*numberOfblocks+1:4*numberOfblocks);
    muG=dec(4*numberOfblocks+1:5*numberOfblocks);
    muB=dec(5*numberOfblocks+1:6*numberOfblocks);
    avgstd=dec(6*numberOfblocks+1:7*numberOfblocks);
    avgstd1=dec(7*numberOfblocks+1:8*numberOfblocks);
    [val1,tileindx]=sort(avgstd);
    [val2,targetindx]=sort(avgstd1);
    Mosaic=reshape(Mosaic,[M,N,3]);
    k=1;
    for i=1:n:M
        for j=1:n:N
            ntile{k}=Mosaic(i:i+n-1,j:j+n-1,:);
            k=k+1;
```

```
        end
    end
    %Secret Image Extraction
    ntile=ntile(targetindx);
    for k=1:numberOfblocks
        ci=ntile{k};
        nci(:,:,1)=(ci(:,:,1)-muR1(k))+muR(k);
        nci(:,:,2)=(ci(:,:,2)-muG1(k))+muG(k);
        nci(:,:,3)=(ci(:,:,3)-muB1(k))+muB(k);
        ntile3{k}=nci;
    end
    ntile3(tileindx)=ntile3;
    k=1;
    for i=1:n:M
        for j=1:n:N
           RI(i:i+n-1,j:j+n-1,:)=ntile3{k};
            k=k+1;
        end
    end
    RI=(uint8(RI));
    str = sprintf(['Error: Either the key is invalid or the
          video is not suitable\n']);
     uialert(app.UIFigure, str, 'Try adding another Key/Video');
    end
end
```

Appendix B

Huffman Coding

```
function [Code,Code_Bin] = Huffman_Code(app,num_Map_origin_I)
    % Function description: use variable-length encoding (multi-bit 0/1 encoding)
    to represent the marker category of pixel values
    % Input: num_Map_origin_I (statistics of pixel value marker categories)
    % Output: Code (mapping relationship), Code_Bin (binary
    representation of Code)
    % Remarks: Use the 9 codes of {00, 01, 100, 101, 1100, 1101,
    1110, 11110, 11111} to represent 9 types of markers
    % Rule: The more pixels in the marked category, the
    shorter the encoding length used to represent its category
    %{00,01,100,101,1100,1101,1110,11110,11111}?{0,1,4,5,12,13,14,30,31}
    %% Find its mapping encoding relationship
    Code = [-1,0;-1,1;-1,4;-1,5;-1,12;-1,13;-1,14;-1,30;-1,31];
    for i=1:9
        drder=1;
        for j=1:9
            if num_Map_origin_I(i,2) < num_Map_origin_I(j,2)
                drder = drder + 1;
            end
        end
        while Code(drder) ~= -1 % prevent the number of pixels in the
                                two marker classes from being equal
            drder = drder + 1;
        end
        Code(drder,1) = num_Map_origin_I(i,1);
    end
    %% Represent the Map mapping relationship as a binary bit stream
    Code_Bin = zeros();
    t = 0; % count
    for i=0:8
        for j=1:9
            if Code(j,1) == i
                value = Code(j,2);
            end
        end
        if value == 0
```

```
            Code_Bin(t+1) = 0;
            Code_Bin(t+2) = 0;
            t = t+2;
        elseif value == 1
            Code_Bin(t+1) = 0;
            Code_Bin(t+2) = 1;
            t = t+2;
        else
            add = ceil(log2(value+1)); % indicates the length of
                  the marker encoding
            Code_Bin(t+1:t+add) = dec2bin(value)-'0';
            % Convert value to binary array
            t = t + add;
        end
    end
    end
```

Appendix C

Screenshots

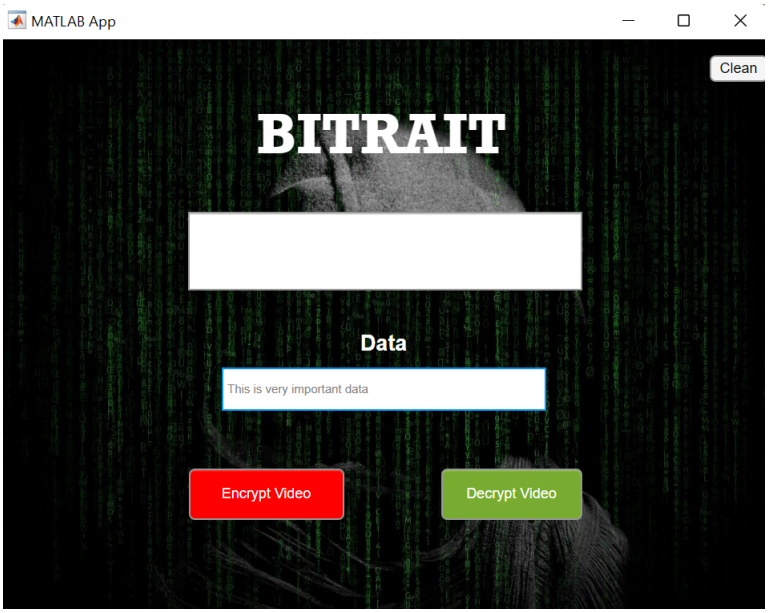


Figure C.1: UI containing data to hide

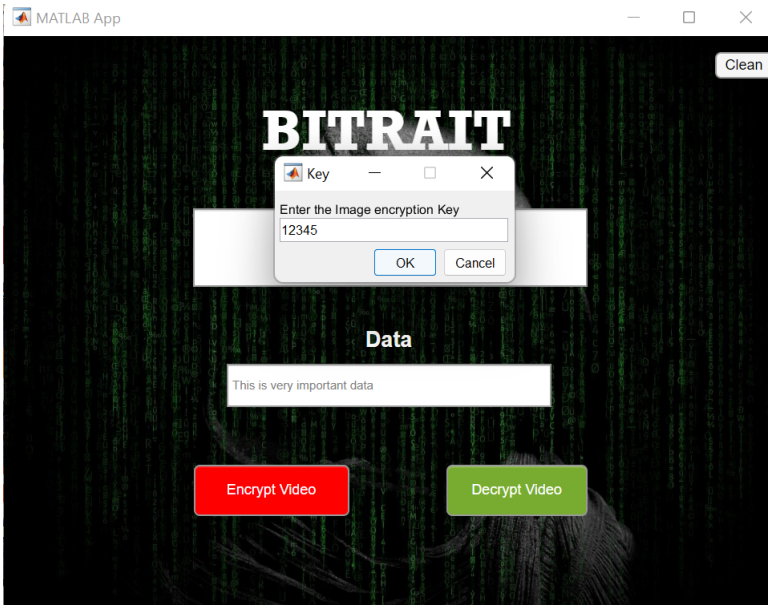


Figure C.2: Key for image encryption

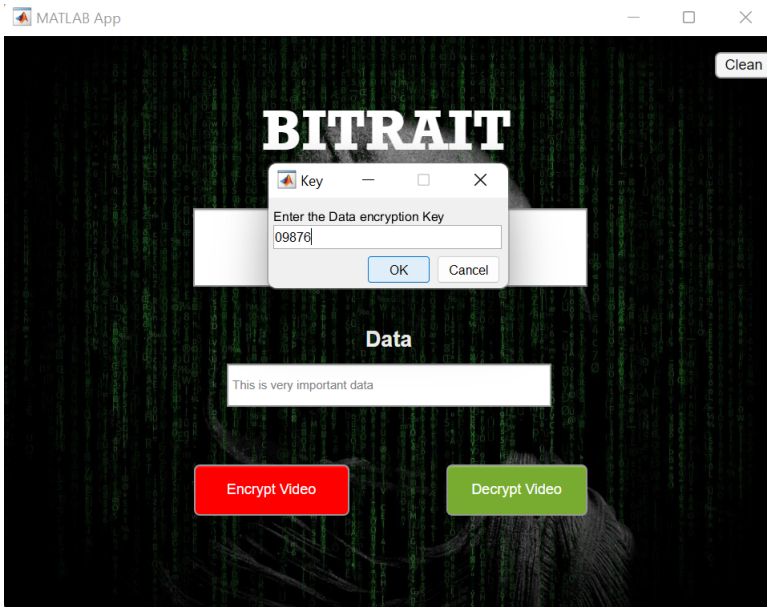


Figure C.3: Key for data encryption

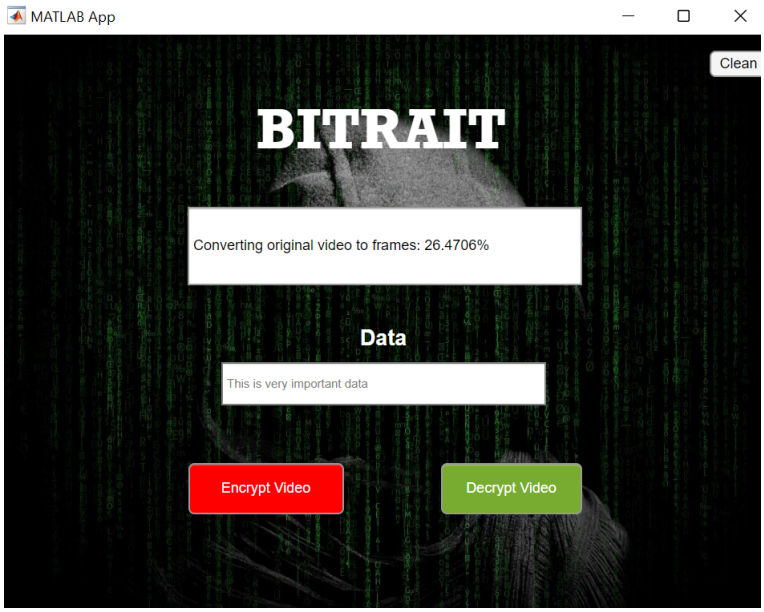


Figure C.4: Converting original video to frames

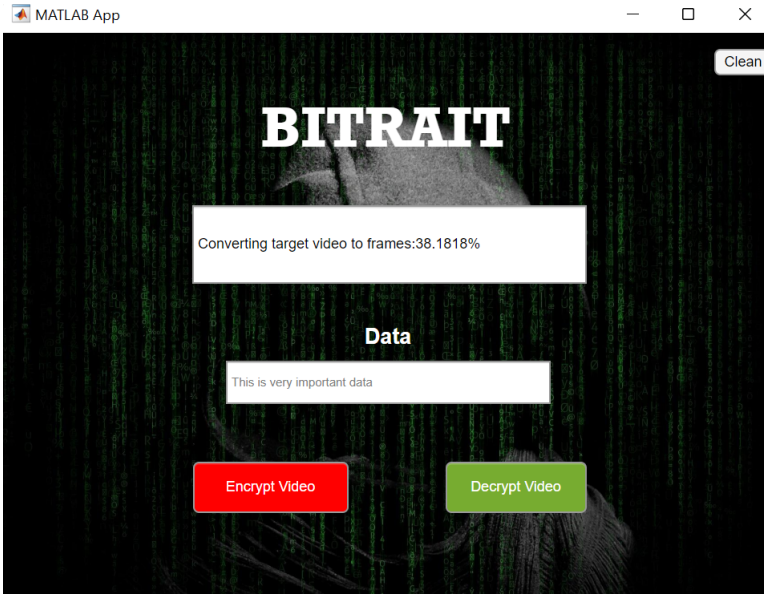


Figure C.5: Converting target video to frames

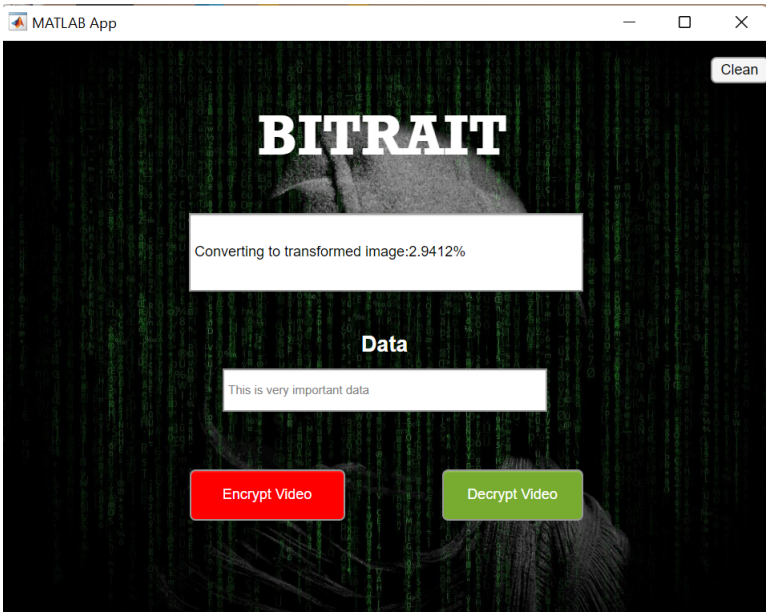


Figure C.6: Converting to transformed Image

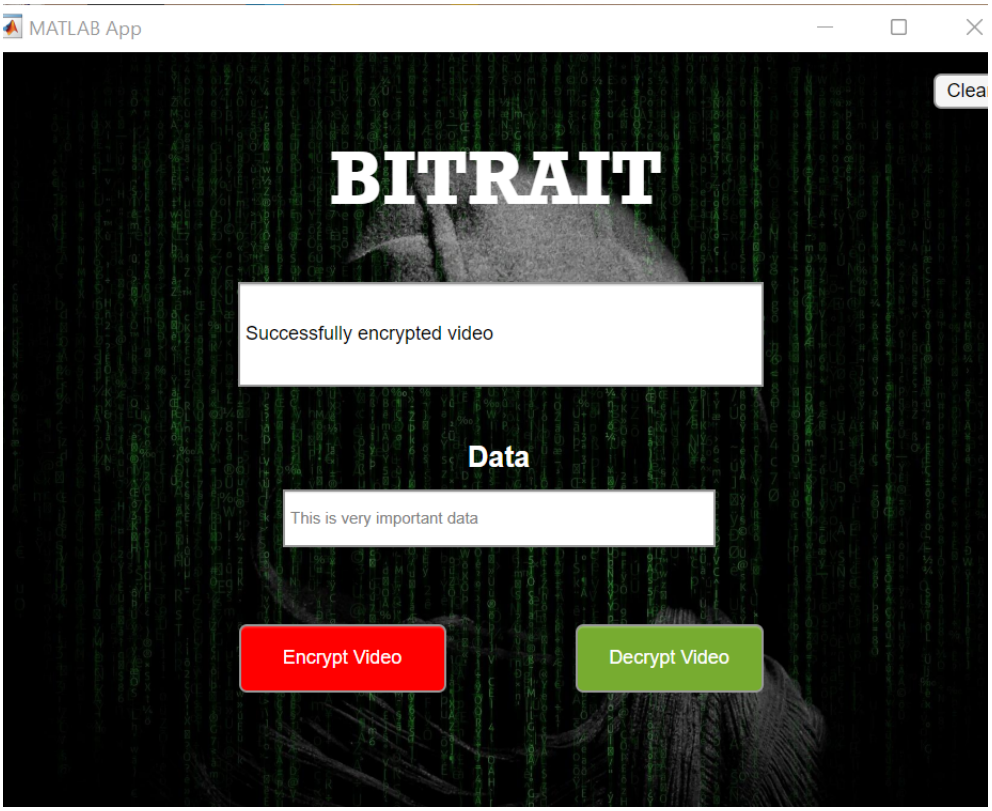


Figure C.7: Final encrypted video

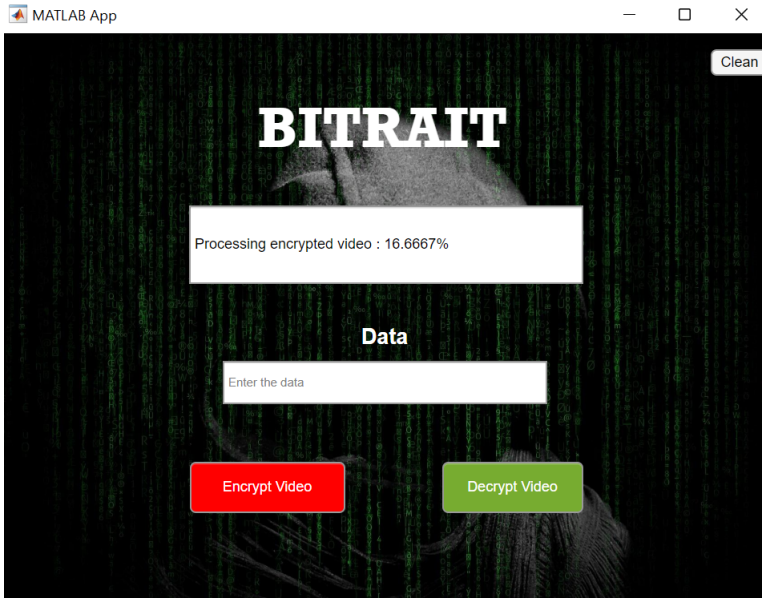


Figure C.8: Processing of encrypted video

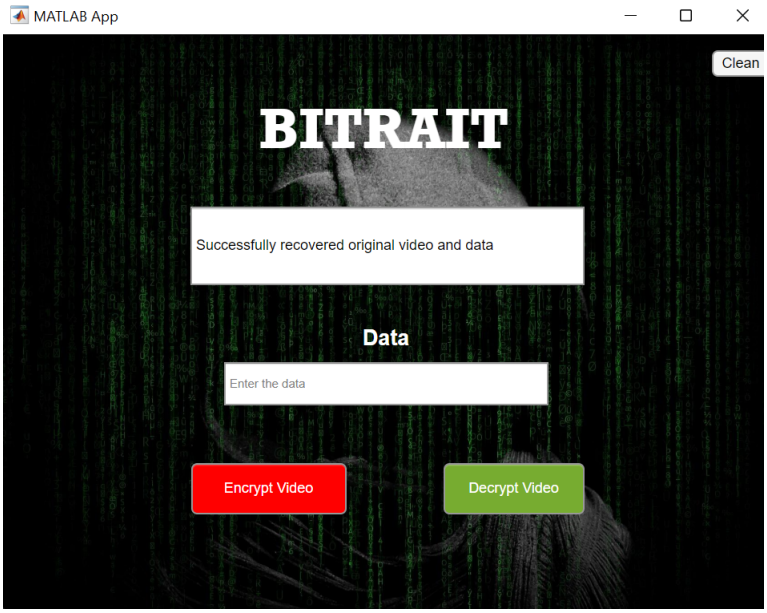


Figure C.9: Recovery of original video

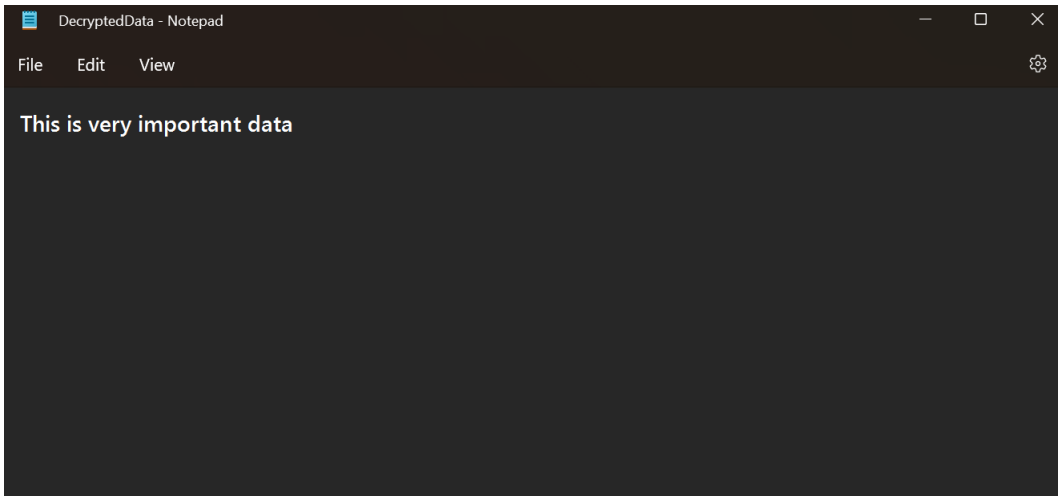


Figure C.10: Decrypted data