IMAGE AND VIDEO STEGANOGRAPHY USING RC6 ALGORITHM

A PROJECT REPORT

Submitted by

AKILA LOURDES.MF (211420104013)

ESAIYARASI.V (211420104076)

MONICA.K(211420104166)

in partial fulfillment for the award of the degree

of

BACHELOR OF ENGINEERING

in

COMPUTER SCIENCE AND ENGINEERING

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

MARCH 2024

PANIMALAR ENGINEERING COLLEGE

(An Autonomous Institution, Affiliated to Anna University, Chennai)

BONAFIDE CERTIFICATE

Certified that this project report **"IMAGE AND VIDEO STEGANOGRAPHY USING RC6 ALGORITHM"** is the bonafide work of **AKILA LOURDES.MF(211420104013),ESAIYARASI V(211420104076),MONICA K(211420104166)** who carried out the project work under my supervision.

SIGNATURE OF THE HOD

Dr.L.JABASHEELA,M.E.,Ph.D .,
PROFESSOR &
HEAD OF THE DEPARTMENT

DEPARTMENT OF CSE,
PANIMALAR ENGINEERING COLLEGE ,
NASARATHPETTAI,
POONAMALLEE,
CHENNAI-600 123.

SIGNATURE OF THE SUPERVISOR

Dr.M.Maheswari.,M.E,Ph.D.,
ASSOCIATE PROFESSOR

DEPARTMENT OF CSE,
PANIMALAR ENGINEERING COLLEGE,
NASARATHPETTAI, POONAMALLEE,
CHENNAI-600 123.

Certified that the above candidate(s) was examined in the End Semester Project Viva-Voce Examination held on .....

INTERNAL EXAMINER **EXTERNAL EXAMINER**

DECLARATION BY THE STUDENT

We **AKILA LOURDES M.F (211420104013), ESAIYARASI V (211420104076), MONICA K (211420104166)** here by declare that this project report titled **"IMAGE AND VIDEO STEGANOGRAOHY USING RC6 ALGORITHM ",** under the guidance of **Dr. M. MAHESHWARI** is the original work done by us and we have not plagiarized or submitted to any other degree in any university by us.

Name of the students

AKILA LOURDES MF (211420104013)

ESAIYARASIV(211420104076)

MONICA K(211420104166)

ACKNOWLEDGEMENT

Our profound gratitude is directed towards our esteemed Secretary and Correspondent, **Dr. P. CHINNADURAI, M.A., Ph.D**.,for his benevolent words and fervent encouragement. His inspirational support proved instrumental in galvanizing our efforts, ultimately contributing significantly to the successful completion of this project

We want to express our deep gratitude to our Directors ,

Tmt. C. VIJAYARAJESWARI, Dr. C. SAKTHI KUMAR, M.E., Ph.D., and Dr.SARANYASREE SAKTHI KUMAR, B.E., M.B.A., Ph.D., for graciously Affording us the essential resources and facilities for undertaking of this project.

Our gratitude is also extended to our Principal, **Dr. K. MANI, M.E., Ph.D.,** whose facilitation proved pivotal in the successful completion of this project.

We express my heartfelt thanks to **Dr. L. JABASHEELA,M.E., Ph.D.,** Head of the Department of Computer Science and Engineering, for granting the necessary facilities that contributed to the timely and successful completion of project.

We would like to express our sincere thanks to Project Coordinator **Dr.M.MAHESWARI.,M.E.,Ph.D.,** and all the faculty members of the Department of CSE for their unwavering support for the successful completion of the project.

NAME OF THE STUDENT

AKILA LOURDES F (211420104013)

ESAIYARASI V (211420104076)

MONICA K (211420104166)

PROJECT COMPLETION CERTIFICATE

FABHOST
COMPLETE WEB SOLUTION

15th Mar2024

COMPLETION CERTIFICATE

This is to certify that students of ***ESAIYARASI V (Reg.No: 211420104076), AKILA LOURDES MF (Reg.No: 211420104013), MONICA K (Reg.No: 211420104166), from PANIMALAR ENGINEERING COLLEGE*** *pursing* ***BACHELOR OF COMPUTER SCIENCE AND ENGINEERING*** *degree had successfully completed educational project in our organization Fabhost Web Solutions*

Topic: *Image and Video Steganography Using Rc6 Using Algorithm*

During the project period **(from JANUARY 2024 to MARCH 2024)** *they were found punctual, hardworking and inquisitive*

With Best Regards,

(M.Mohan Raj)
Human Resource

FABHOST WEB SOLUTIONS
#102, PMG complex, South Usman Road, TNagar , Chennai – 17. Ph: 044-48519444 , 9176990190.
Email: fabhostindia@gmail.com www.fabhost.in

ABSTRACT

For secure data transmission over internet, it is important to transfer data in high security and high confidentiality, information security is the most important issue of data communication in networks and internet. Either Image or video to secure transferred information from intruders, it is important to convert the information into cryptic format the Image and video work on the same process. Different methods used to ensure data security and confidentiality during transmission like steganography and cryptography. We convert plaintext to cipher text for doing so we have used Rivest Cipher 6 (RC6) Encryption Algorithm The proposed algorithm ensure the encryption and decryption using RC6 stream cipher and RGB pixel shuffling with steganography by using hash-least significant Bit (HLSB) that make use of hash function to developed significant way to insert data bits in Least Significant Bit (LSB) bits of RGB pixels of cover image. The security evaluations for the Steganography part we will be using Modified LSB Algorithm where we overwrite the LSB bits of the selected frame (given by the user) from the cover video, with the bit of text message character with help of secret key and using Key-Scheduling Algorithm (KSA) and Pseudo-Random Generation Algorithm (PRGA). Steganography is the art and science of hiding secret messages within innocuous-looking cover media such as images or videos. This field has gained immense importance in secure communication systems due to its ability to conceal the existence of the communicated information. In this study, we propose a novel approach for image and video steganography using the RC6 encryption algorithm.The RC6 algorithm is a symmetric key block cipher known for its security and efficiency. It offers a balance between security and speed, making it suitable for embedding secret data into digital media. Our proposed system first encrypts the secret message using the RC6 algorithm, generating a ciphertext that appears random and unintelligible. Next, this ciphertext is embedded into the cover image or video using a secure and imperceptible technique

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1 OVERVIEW

In the following sections, fundamentals of data hiding, attributes and performance metrics of data hiding techniques, a discussion of surveys on data hiding in digital media, and a classification of LSB data hiding techniques are provided leading to the motivation and contributions of the work reported. The rest of this survey is then organized as follows. provides the survey of LSB data hiding in digital audio including speech and voice with respect to the temporal, transform, and coded domains. contains the LSB data hiding techniques used with digital images considering the spatial, transform, and quantum domains. A survey on LSB data hiding in raw and compressed data formats of digital videos is provided in Section. the fast improvements and the data interchanges, a lot of concerns have been brought up in the security of information transmitted output away over open channels. Particularly at the level of text and picture information. As indicated by there are three fundamental routines for secured correspondence accessible, in particular, cryptography, steganography of RC6. Among these three, the first one, cryptography manages the improvement of procedures for changing over data in the middle of understandable and incomprehensible structures amid data trade. Steganography, then again, is a procedure for concealing and separating data to be passed on utilizing a transporter signal.

PROBLEM DEFINITION

Challenge is to create a robust system for image and video steganography, employing the RC6 algorithm to embed and extract secret information within multimedia content. Steganography aims to conceal sensitive data within innocuous carriers, ensuring imperceptibility to human observers. By integrating the RC6 symmetric key block cipher algorithm, the system must facilitate encryption and decryption processes, safeguarding the concealed information against unauthorized access and cryptographic attacks. Imperceptibility is crucial to maintain the visual and auditory fidelity of the media, ensuring that alterations made during the embedding process remain undetectable. The system should also demonstrate robustness against common image and video processing operations, preserving the integrity of the hidden data across various digital formats and environments. Efficiency and user- friendliness are essential considerations, necessitating streamlined encoding and decoding processes and an intuitive user interface. Comprehensive documentation and support resources should accompany the system to aid users in understanding steganographic techniques, configuring system parameters, and addressing potential issues effectively.

SCOPE OF THE PROJECT

Due to the high speed of internet and advances in technology, people are becoming more worried about information being hacked by attackers. Recently, many algorithms of steganography and data hiding have been proposed. Steganography is a process of embedding the secret information inside the host medium (text, audio, image and video). Concurrently, many of the powerful steganographic analysis software programs have been provided to unauthorized users to retrieve the valuable secret information that was embedded in the carrier files. Some steganography algorithms can be easily detected by steganographic-analytical detectors because of the lack of security and embedding efficiency. We propose a secure video steganography.

CHAPTER 2
LITERATURE SURVEY

CHAPTER 2

LITERATURE SURVEY

Title: A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector

Author: Ramadhan J. Mstafa; Younis Mohammed Younis; Haval Ismael Hussein; Muhsin Atto

Year: 12-06-2020

Abstract:

Recent developments in the speed of the Internet and information technology have made the rapid exchange of multimedia information possible. However, these developments in technology lead to violations of information security and private information. Digital steganography provides the ability to protect private information that has become essential in the current Internet age. Among all digital media, digital video has become of interest to many researchers due to its high capacity for hiding sensitive data. Numerous video steganography methods have recently been proposed to prevent secret data from being stolen. Nevertheless, these methods have multiple issues related to visual imperceptibly, robustness, and embedding capacity. To tackle these issues, this paper proposes a new approach to video steganography based on the corner point principle and LSBs algorithm. The proposed method first uses Shi-Tomasi algorithm to detect regions of corner points within the cover video frames. Then, it uses 4-LSBs algorithm to hide confidential data inside the identified corner points. Besides, before the embedding process, the proposed method encrypts confidential data using Arnold's cat map method to boost the security level.

Title: A New Video Steganography Scheme Based on Shi-Tomasi Corner Detector

Author: Ramadhan J. Mstafa; Younis Mohammed Younis; Haval Ismael Hussein; Muhsin Atto

Year: 12-06-202

Abstract:

Recent developments in the speed of the Internet and information technology have made the rapid exchange of multimedia information possible. However, these developments in technology lead to violations of information security and private information. Digital steganography provides the ability to protect private information that has become essential in the current Internet age. Among all digital media, digital video has become of interest to many researchers due to its high capacity for hiding sensitive data. Numerous video steganography methods have recently been proposed to prevent secret data from being stolen. Nevertheless, these methods have multiple issues related to visual imperceptibly, robustness, and embedding capacity. To tackle these issues, this paper proposes a new approach to video steganography based on the corner point principle and LSBs algorithm. The proposed method first uses Shi-Tomasi algorithm to detect regions of corner points within the cover video frames. Then, it uses 4-LSBs algorithm to hide confidential data inside the identified corner points. Besides, before the embedding process, the proposed method encrypts confidential data using Arnold's cat map method to boost the security level.

Title: A Survey on Different Video Steganography Techniques

Author: J. Mary Jenifer; S. Raja Ratna; J.B. Shajilin Loret; D. Merlin Gethsy

Year: 19-04-2020

Abstract:

Steganography is the method of hiding the secret message inside the data source. It not only keeps the information as secret but also the existence of the information is kept as secret. It is used in various fields such as defense, medical and online transactions. It is mainly used in secure communication. In steganography, the message can be hidden in carriers such as text files, images, audios, and videos. The aim of this paper is to provide a general overview of various video steganography techniques. It covers related works,

the strength of steganography, types of steganography and different video steganography techniques. The comparative analysis of various video steganography techniques is also highlighted.

Title: Video steganography network based on 3DCNN

Author: Yangping Lin; Zhiqiang Ning; Jia Liu; Mingshu Zhang; Pei Chen; Xiaoyuan Yang

Year: 05-05-2022

Abstract:

In recent years, the steganography scheme based on neural network has made many significant progress on images, but it is still in the exploratory stage in the field of video steganography. By using long skip connections to extract the spatio-temporal information in the video, this paper proposes a 3DCNN full-video steganography network. The network takes a pair of cover and secret video sequences as input, and uses a stego network to output a spatio-temporal residual sequence, which is added to the cover video as a small disturbance. A video classification network is proposed, which can be used to identify the cover video frame and the stego video frame to assist the message receiver to extract the secret message correctly. We chose UCF101 video data set as the training and testing set of the network model. We used various video quality evaluation indicators (PSNR, SSIM, Pixel distribution) to measure the performance evaluation of the stego video network, and proved the anti-detection of the stego video by using some stego detection algorithms. Under the training and testing of the data set of stego videos generated by the stego network, the classification accuracy of the proposed video classification network reaches about 93%..

Title: A review on video steganography techniques in spatial domain

Author: Disha; Khushil Saini

Year: 01-07-2021

Abstract:

Steganography is a method of concealing private or delicate information inside something that emits an impression of being nothing out of regular. Diverse carrier file formats can be used, for example text documents, audio tracks, digital images, and videos. But, due to immense advancement of information over the web, video steganography has turned into a very popular decision for data hiding. In video steganography, secret information is concealed inside a video to keep it safe from gate crashers. There exists variety of techniques for hiding secret information in a video, each having their own qualities and shortcomings. However, the literature absences of sufficient review articles that talk about all techniques. On the basis of embedding method, video steganography techniques are classified into two categories namely, spatial domain and frequency domain techniques. This paper is an attempt to present a comprehensive study of various state-of-the-art video steganography methods in spatial domain developed in the past decade which are very beneficial for video steganography analysts to acquire better outcomes, high proficiency and security.

Title: **Video steganography**

Author: A.J. Mozo; M.E. Obien; C.J. Rigor; D.F. Rayel; K. Chua; G. Tangonan

Year: 28-10-2020

Abstract:

This paper aims to describe our research and software implementation in the field of video steganography. Because of security threats today through modern malevolent technology, confidential information is at risk such as medical records and banking or financial data. The group provided a solution by protecting this sensitive information inside videos. The project focused on using Flash Videos (.flv file extension) because of its simple file structure, its relatively small size compared to other video file formats, and its popularity in video-hosting websites. Intensive experimentation on how the FLV file structure can be

manipulated to hold additional data were done. Through these experiments, the characteristics of the FLV provided the group to implement a C++ program that features embedding any type of data in the FLV, extracting that same hidden information, as well as compressing the FLV to compensate for the increase in file size. Very promising results include 100% lossless extraction, perfect original picture and sound quality for the uncompressed FLV embedded with data and uncompromised integrity of hidden data when modified FLVs are transferred through the Internet through e-mail or video-hosting websites.

Title :

Author : Amin, J., Anjum, M. A., Ibrar, K., Sharif, M., Kadry, S., & Crespo, R. G.

Year:24 -03-2023

Abstract:

In their recent work, Amin, J., Anjum, M. A., Ibrar, K., Sharif, M., Kadry, S., & Crespo, R. G. (2023) focused on detecting anomalies in surveillance videos by employing quantum convolutional neural networks. Their study, published in Image and Vision Computing, showcases the implementation of cutting-edge quantum algorithms for enhancing anomaly detection in video streams. This research represents a significant advancement in leveraging quantum computing for improving surveillance and security systems.

Title :

Author : . Arafath, M. D., & Kumar, A. N.

Year:10-5-2023

Abstract: Detection of image in surveillance videos using CNN algorithm

Arafath and Kumar (2023) proposed a novel approach to anomaly detection in real-time surveillance videos using quantum computing-based neural networks. Their study, published in Computer Systems Science & Engineering, showcased the effectiveness of quantum algorithms for real-time anomaly classification in video streams. By leveraging

the power of quantum computing, the researchers demonstrated improved accuracy and efficiency in detecting anomalies, highlighting the potential applications of quantum technology in video surveillance systems.

Title :CNN computing based neural networks for video steganography

Author : Arunnehru, J

Year:11-8-2023

Abstract:

Arunnehru, J. (2023) presented a study on deep learning-based real-world object detection and improved anomaly detection for surveillance videos. The research, published in Materials Today: Proceedings, focuses on enhancing anomaly detection in video surveillance. The study showcases the integration of deep learning techniques to improve the accuracy of anomaly detection. This work provides valuable insights and advancements in the field of surveillance video analysis, potentially paving the way for further research in anomaly detection using quantum algorithms.

Title :Deep learning based image detection and improved anomaly detection

Author : Rosenhahn, B., & Hirche, C

Year:05-05-2024

Abstract:

Rosenhahn, B., and Hirche, C. (2024) introduced Quantum Normalizing Flows for Anomaly Detection in their paper titled "Quantum Normalizing Flows for Anomaly Detection." This innovative approach combines quantum algorithms with anomaly detection techniques to analyze video data efficiently. By leveraging quantum computing capabilities, the proposed method aims to provide enhanced anomaly detection performance in video streams. The paper, available as an arXiv preprint with the code arXiv:2402.02866, opens the door to exploring the potential of quantum technologies in addressing anomaly detection challenges in video data.

Title : CNN based anomaly using image detection

Author : Bustos-Brinez, O. A., Gallego-Mejia, J. A., & González, F. A

Year:22-09-2023

Abstract:

Bustos-Brinez, O. A., Gallego-Mejia, J. A., & González, F. A. presented their work on AD-DMKDE at the International Conference on Information Technology & Systems in February 2023. Their research focuses on Anomaly Detection through Density Matrices and Fourier Features, leveraging RC6 algorithms for anomaly detection in video. This innovative approach combines advanced techniques to enhance anomaly detection capabilities, offering a promising solution for surveillance and security applications. The research published by the authors in Springer International Publishing provides valuable insights into the intersection of quantum computing and video analysis for anomaly detection.

Title :Image detection through density matrices and fourier features

Author : Choudhry, N., Abawajy, J., Huda, S., & Rao, I

Year:15-02-2023

Abstract:

Choudhry, N., Abawajy, J., Huda, S., & Rao, I. (2023) conducted a comprehensive survey on machine learning methods for surveillance videos anomaly detection, as published in IEEE Access. Their research focuses on the application of quantum algorithms for detecting anomalies in video surveillance, presenting a cutting-edge approach to improving surveillance system effectiveness and accuracy. Their work sheds light on the potential of advanced technologies in enhancing anomaly detection capabilities in video surveillance, paving the way for more reliable and efficient security measures.

Title : A Comprehensive survey of machine learning methods for surveillance videos steganography

Author : Khan.K

Year:12-012-2023

Abstract:

Khan, K. (2023) published a taxonomy exploring the application of quantum computing in drone video streaming technology for anomaly detection. The study, available on Zenodo, identifies innovative ways to utilize quantum algorithms in processing video data for anomaly detection purposes. The research sheds light on the promising intersection of quantum computing and video streaming technology for enhancing anomaly detection capabilities.

Title : A taxonomy for the use of CNN algorithm in video streaming technology

Author : Zhang, H., Xie, R., Li, K., Huang, W., Yang, C., & Liu, J.

Year:29-01-2023

Abstract:

Zhang et al. (2023) explore anomaly detection in video using deep learning, offering valuable insights and opportunities in this area. Introducing quantum algorithm could potentially enhance the efficiency and accuracy of anomaly detection techniques, revolutionizing the field with cutting-edge technology.

Title : Improve the video detection performance of pixel and frame based techniques

Author : Roka, S., & Diwakar, M

Year:20-09-2023

Abstract:

Roka and Diwakar (2023) propose a deep stacked denoising autoencoder for unsupervised anomaly detection in video surveillance. Their approach aims to enhance anomaly detection accuracy in video surveillance applications through the use of advanced autoencoder techniques

CHAPTER 3
SYSTEM ANALYSIS

CHAPTER 3

SYSTEM ANALYSIS

3.1 EXISTING SYSTEM

The existing techniques are mainly based on LSB (Least Significant Bit) where LSBs of the cover file are directly changed with message bits. A significant number of methods have been proposed for LSB steganography. The proposed a LSB technique for RGB true color image by enhancing the existing LSB substitution techniques to improve the security level of hidden information.

DRAWBACK

- It may fail sometimes because for complete encryption both symmetric and asymmetric encryption is required and RSA uses asymmetric encryption only. It has slow data transfer rate due to large numbers involved. It requires third party to verify the reliability of public keys sometimes.
- This project only working on video.

3.2 PROPOSED SYSTEM

The security of data communication and especially images or video frames from images became a significant goal as the network is growing. The security of images from the video is an important research field in different trends like data security, secure data transmission and copyright security. So, Image encryption algorithms and hiding algorithms should be designed to enhance the effectiveness of transmission and keep safety from attacks by the intruders. So, the proposed method can achieve the highest level of data integrity, confidentiality and security. We are trying to verify the confidentiality of grayscale image that makes uses of pixel shufflingand RC6 stream cipher for cryptography and Hash-LSB for steganography. Then the last step this only on video Steganography arrange all the frame and form a video avi type and extract frame also same step and decrypt the RC6 stream chip then get the message.

ADVANTAGES

- providing more security to data as well as our data hiding method.
- The proposed technique uses a hash function to generate a pattern for hidingdata bits into LSB of RGB pixel values of the cover image.
- Image and video two types work also add this project.

3.3 DEVELOPMENT ENVIROMENT

HARDWARE REQUIREMENT

- Processor- I5
- Speed - 3 GHz
- RAM - 8 GB(min)
- Hard Disk - 500 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - LCD

SOFTWARE REQUIREMENT

- Operating System: Linux, Windows/7/10
- Server: Anaconda, Jupyter,pycharm
- Front End: tkinter |GUI toolkit
- Server side Script: Python

3.4 MODULE DESCRIPTION

Video steganography is the art and science of hiding secret data within a video file without altering the perceptual quality of the video. It involves embedding data in a way that is imperceptible to the human eye or ear but can be extracted by authorized parties using a specific technique.

The module for video steganography would typically include the following components:

- Encoding Algorithm
- Decoding Algorithm
- User Interface
- Video Processing Module
- Security Module

MODULE DESCRIPTION

Video steganography is the art and science of hiding secret data within a video file without altering the perceptual quality of the video. It involves embedding data in a way that is imperceptible to the human eye or ear but can be extracted by authorized parties using a specific technique.

The module for video steganography would typically include the following components:

- Encoding Algorithm
- Decoding Algorithm

- Video Processing Module
- Security Module

3.4.1 Encoding Algorithm

Least Significant Bit (LSB)

Embedding:Explanation:

LSB embedding involves replacing the least significant bits of the videoFrames with the bits of the secret data. Since the LSBs contribute the least to the overall intensity of the pixel, altering them slightly usually results in minimal perceptual changes inthe video.

Implementation:

This technique typically involves iterating through the pixels of each

frame and modifying the LSBs according to the secret data bits to be embedded. Care must betaken to ensure that the changes are distributed across the video frames to avoid detectability.

Advantages

LSB embedding is relatively straightforward to implement and can achieve High embeddingcapacity without significant perceptual distortion

Disadvantages

It's vulnerable to attacks such as histogram analysis and noise addition,

Which can potentially reveal the hidden data

.

3.4.1 Decoding Algorithm

The Decoding Algorithm is a crucial component of the video steganography module, responsible for extracting the hidden data from the video file without introducing errors or inaccuracies. Here's a detailed explanation of this module:

Algorithm Selection:

The decoding algorithm must be selected based on the encoding technique used during embedding. Different encoding techniques require specific decoding algorithms to accurately retrieve the hidden data.

For example, if the LSB embedding technique was used during encoding, the decoding algorithm would involve extracting the least significant bits from the video frames to reconstruct the hidden data.

Error Handling:

The decoding algorithm should include robust error handling mechanisms to account for potential errors or noise introduced during the embedding process or during transmission. Techniques such as error correction codes or checksum verification may be employed to ensurethe integrity of the extracted data.

Efficiency:

The decoding algorithm should be efficient in terms of computational resources and processing time to enable fast extraction of the hidden data from large video files. Optimization techniques such as parallel processing or efficient data structures may be utilized to enhance the algorithm's efficiency

Accuracy:

The decoding algorithm should prioritize accuracy to ensure that the extracted data matches theoriginal hidden information without any loss or distortion.
Techniques such as data validation and integrity checks may be integrated into the algorithmto verify the authenticity of the extracted data.

Security Considerations:

The decoding algorithm should incorporate security measures to prevent unauthorized access to the hidden data. For instance, it may require authentication or decryption using a secret keybefore extracting the data.

3.4.2 User Interface

The User Interface module plays a crucial role in facilitating user interaction with the steganography tool. Here's a detailed explanation of this module:

Input Interface:

The UI should provide users with options to input the video file and the secret data that theywish to embed within the video.

This may include file selection dialogues or drag-and-drop functionality to make it easy forusers to input their desired files.

Parameter Selection:

Users should be able to select the embedding technique and any other parameters relevant tothe steganography process, such as encryption options or embedding capacity.

The UI should provide clear explanations and guidance to help users make informed decisions about these parameters.

Initiation Process:

Once all necessary inputs and parameters have been provided, users should be able toinitiate the embedding process with a simple action, such as clicking a button.

The UI should provide feedback to users during the embedding process to indicate progress and completion.

Error Handling and Notifications:

The UI should include mechanisms for handling errors or notifying users about any issues that may arise during the embedding process, such as invalid input files or insufficientembedding capacity.

User Guidance:

The UI should provide clear instructions and guidance to users on how to use the steganographytool effectively and securely.

3.4.3 Video Processing Module

Functions for Video File Handling: This module would provide functions to read, write, and manipulate video frames. It should include capabilities for opening video files, accessing individual frames, and modifying frame properties.

Format and Resolution Handling: The module should be capable of handling various video formats (e.g., MP4, AVI, MOV) and resolutions (e.g., 1080p, 4K). It should include functionalities to automatically detect and adapt to different formats and resolutions.

Frame Manipulation: This involves operations such as resizing, cropping, filtering, and altering individual frames. These functionalities are crucial for preparing the video frames for steganographic embedding.

Error Handling: Robust error handling mechanisms should be implemented to handle issuessuch as corrupted video files or unsupported formats gracefully.

3.4.4 Security Module

Encryption and Decryption: This module would incorporate encryption algorithms (such as RC6) for encrypting the data to be embedded in the video frames. It should include functions for both encryption (to hide the data) and decryption (to retrieve the hidden data).

Password Protection: It should provide mechanisms for password protection to restrict access to the embedded data. Only authorized parties with the correct password should be able to decrypt and access the hidden information.

Watermarking: Watermarking techniques can be employed to embed additional information (e.g., copyright information, ownership details) within the video frames without altering the content significantly. This can help in identifying the source or

owner of the video.

Access Control: This module should enforce access control mechanisms to prevent unauthorized access or tampering with the embedded data. It should include features suchas access permissions and user authentication.

Integrity Verification: To ensure the integrity of the embedded data, mechanisms for verifying the authenticity and integrity of the video frames should be implemented. This can involve techniques such as digital signatures or message authentication codes (MACs).

Overall, the Video Steganography Module should seamlessly integrate the functionalities of the Video Processing Module and the Security Module to provide a secure and efficient solution for embedding and extracting hidden data within video fileswhile maintaining their quality and integrity.

CHAPTER 4
SYSTEM DESIGN

CHAPTER 4

SYSTEM DESIGN

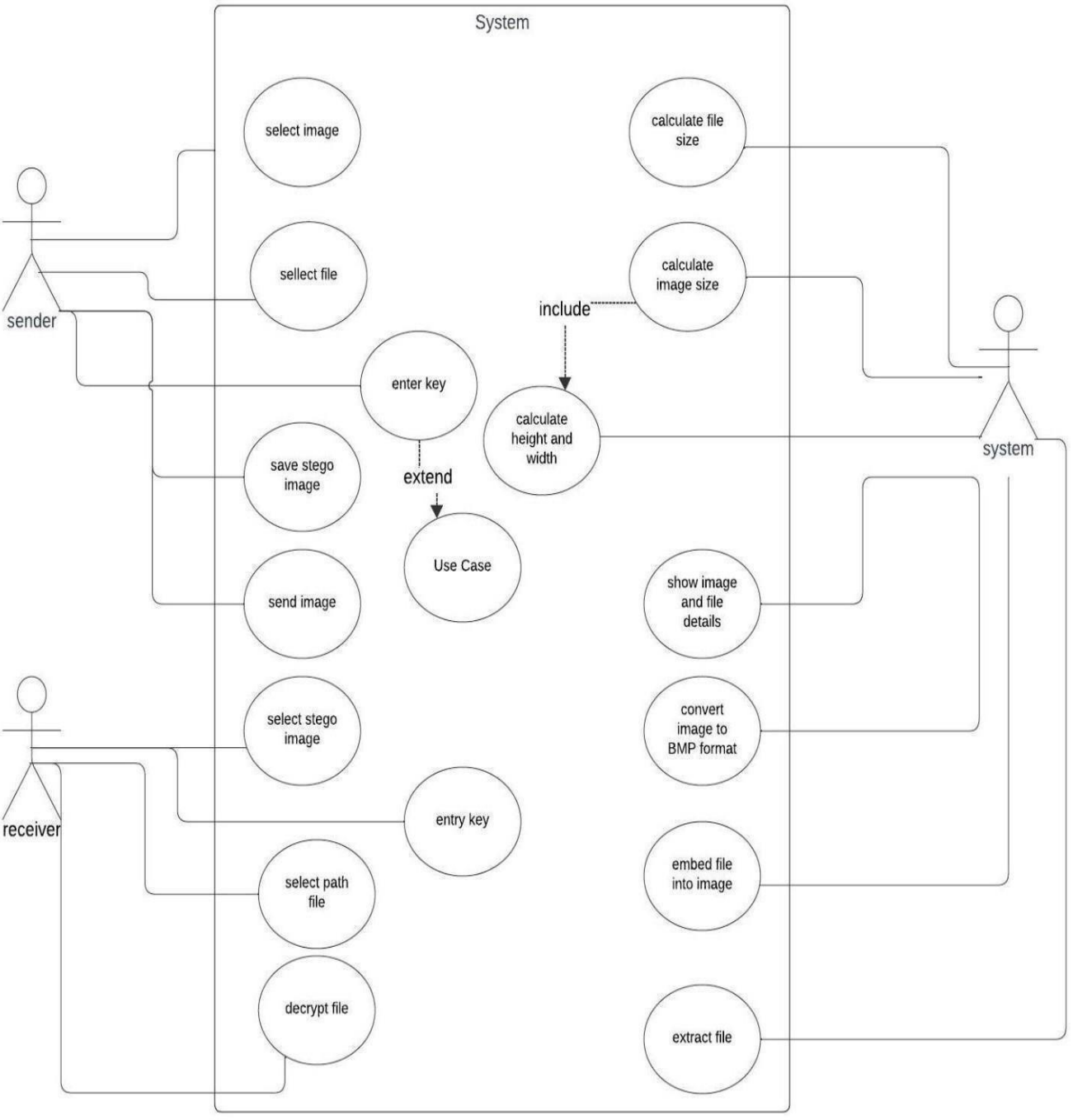
UML DIAGRAMS

4.1 USE CASE DIAGRAM

Use case diagrams capture the functional requirements of a system by identifying the interactions between actors (users or external systems) and the system itself. They depict the various use cases (functionalities) of the system and how actors are involved in them.

Cases:

1. Authentication
2. Encrypt video with stego video
3. Embedding file
4. Decrypt the video
5. Retrieve information from video
6. Retrieve video file



4.1.1 Use case diagram for Image and video steganography using RC6.

This use case diagram refers to activities done by user and system and their corresponding use case

4.2 Sequence diagram

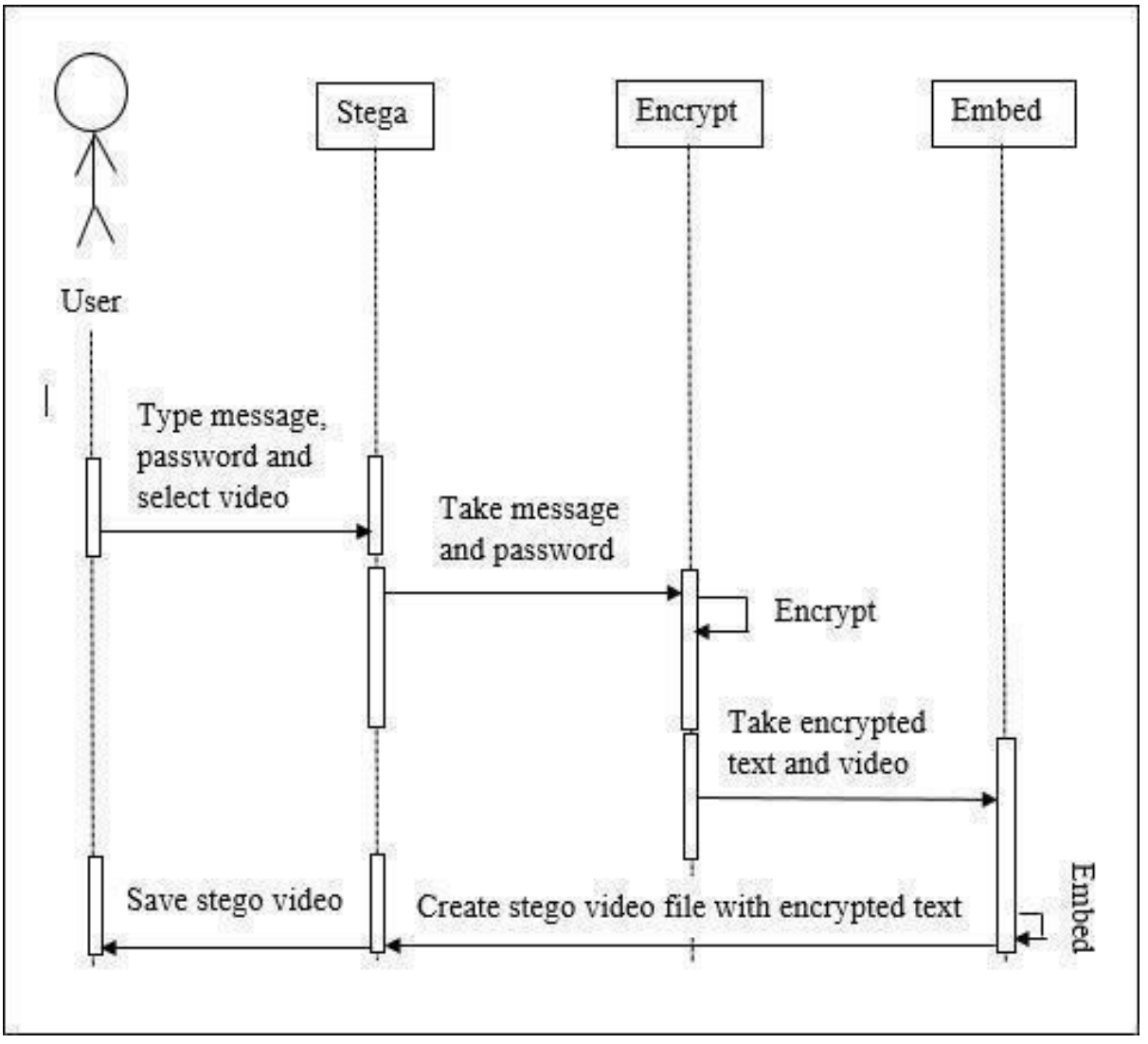


Fig 4.1.2 Sequence diagram for User in Image and Video steganography usingRC6.

4.3 ER DIAGRAMS

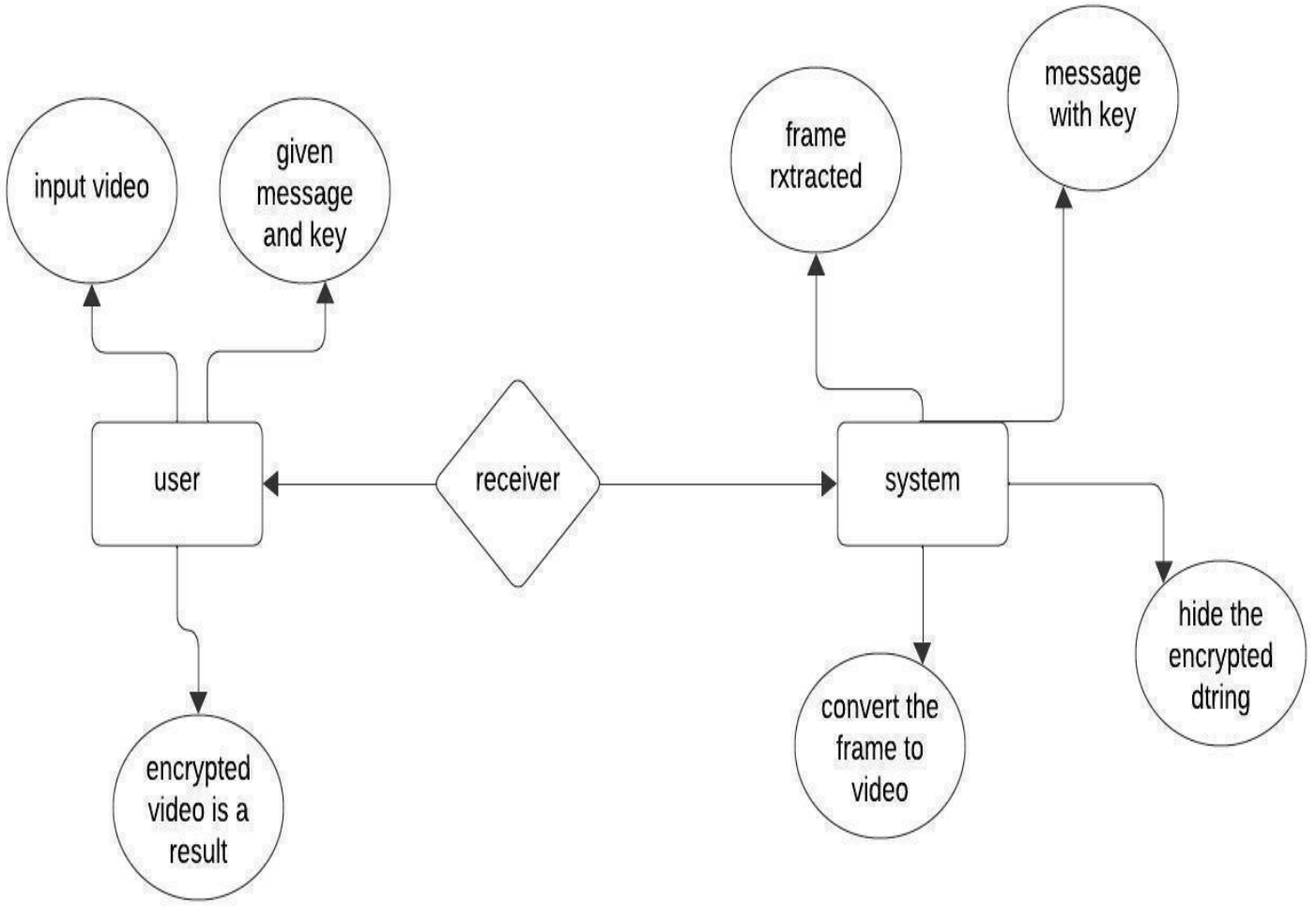


Fig 4.1.3 ER diagram for Image and Video steganography using RC6.

4.4 DATAFLOW DIAGARM

A Data Flow Diagram (DFD) is a graphical representation that illustrates the flow of data within a system. While DFDs are typically used to depict the flow of data in information systems, they can also be adapted to represent the flow of data in a Image and video steganography system.

To create a DFD diagram, you can use various diagramming tools or software that support DFD notation. These tools typically provide a visual interface to easily create and connect components, define data flows, and add descriptions or annotations to enhance the understanding of the diagram.

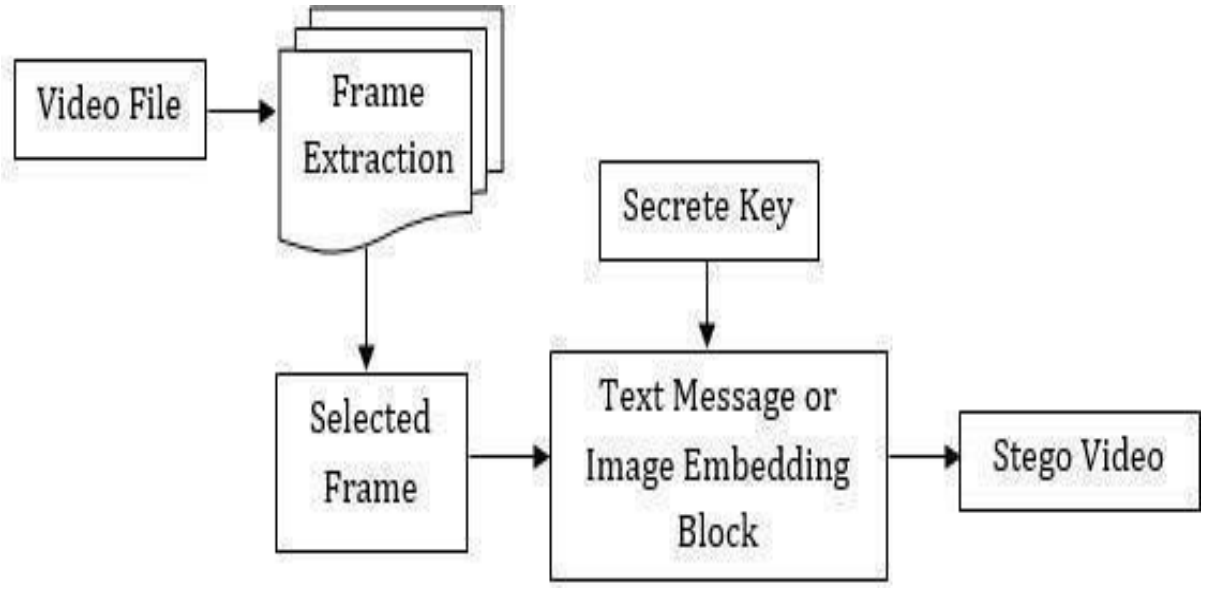


Figure 4.1.4 Data Flow Diagram for Image and Video Steganography using RC6.

SYSTEM ARCHITECTURE

4.5 ARCHITECTURE OVERVIEW

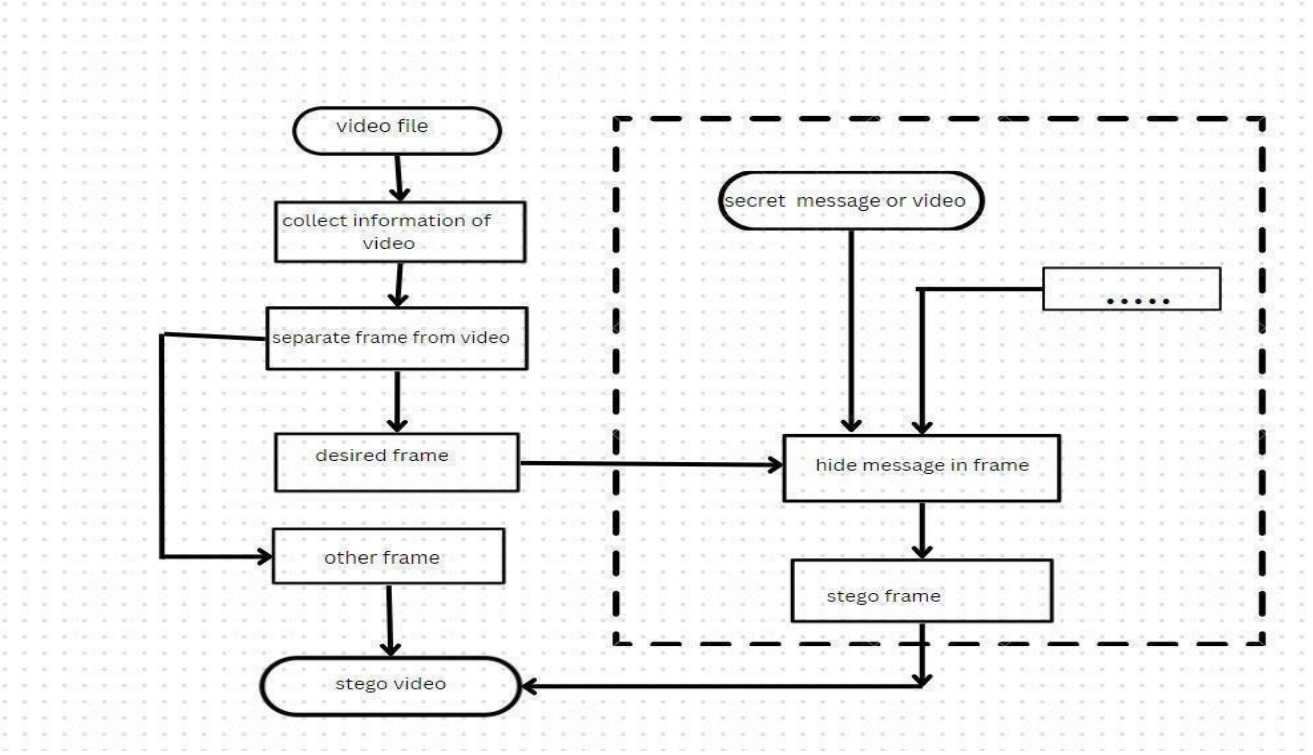


Fig 4.5 Architecture diagram for Image and video steganography using RC

The figure 5.1 The architecture diagram represents how the users first use the video file/ image file and then itgoes to image collecting information of video and then separates frame from video then desired frame after that other frame process then stego video/image will be displayed as output In this system, the architecture uses a image or video, In which we can encrypt the text which we need to hide from others, The process canbe done by using key, with the help of the algorithm and key. Then, when the end user wants to see the text they will decrypt it using the decoding algorithm and key

CHAPTER 5
SYSTEM ALGORITHM

CHAPTER 5

SYSTEM ALGORITHM

5.1 INTRODUCTION TO RC6

Cryptography is where security engineering meets mathematics. Cryptography is the art of physical scrambling of information using rearrangement and substitution ciphers which can only be read correctly by targeted person having the key. A video is a moving stream of number of images, so high amount of data can be embedded in it. Itsrelative complexity also gives an advantage over other types of media such as image and audio in terms of security against intruders.

Rivest Cipher 6 (RC6):

- RC6 is a derivative of RC5 and is a block cipher designed for RSA Security. RC6 uses four working block size registers in its algorithmic computations, whereas RC5 uses only two.
- Thus, RC6 is faster. RC6 was designed as part of the Advanced Encryption Standard (AES) competition, where it was a finalist.
- It is a propriety algorithm patented by RSA Security.
- RC6 is a fast block cipher. It was developed based on RC5 and does its job quicker than RC5 due to more registers.
- RC6 uses integer multiplication in its algorithmic computation. RC6 is also rotation-dependent on every word bit.

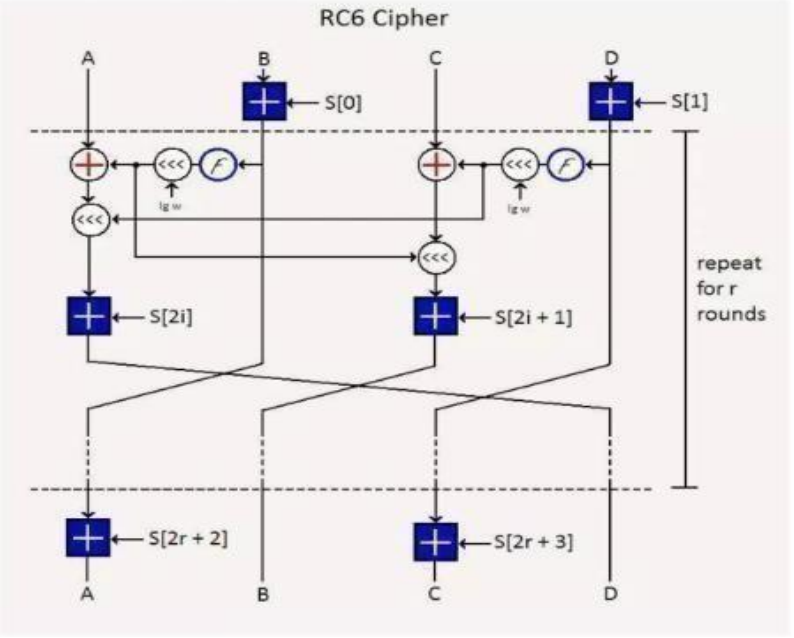


Fig 5.1.1 RC6 Cipher

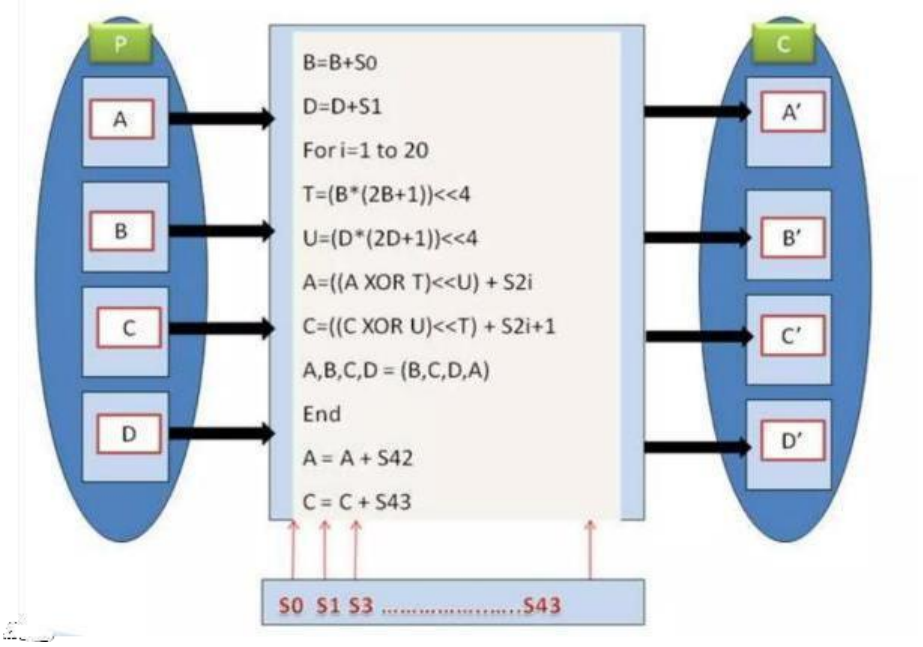


Fig 5.1.2 RC6 algorithm working

5.2 MODULES:

Video steganography is the art and science of hiding secret data within a video file without altering the perceptual quality of the video. It involves embedding data in a way that is imperceptible to the human eye or ear but can be extracted by authorized parties using a specific technique.

The module for video steganography would typically include the following components:

Encoding Algorithm:

This module would include the algorithm used to embed the secret data within the video file. There are various techniques that can be used for this purpose, such as LSB (Least Significant Bit) embedding, Spread Spectrum, and Transform Domain Techniques.

Decoding Algorithm:

This module would include the algorithm used to extract the secret data from the video file. The decoding algorithm should be able to retrieve the hidden information with high accuracy, while avoiding false positives or negatives.

User Interface:

The user interface module would provide an interface for the users to interact with the steganography tool. It would enable users to input the video file and secret data, select the embedding technique and other parameters, and initiate the embedding process.

Video Processing Module:

This module would include the functions for processing the video file, such as reading, writing, and manipulating the video frames. It should also be able to handle various video formats and resolutions.

Security Module:

This module would include security features such as encryption and decryption, password protection, and watermarking. It would ensure that the embedded data is only accessible to authorized parties and prevent unauthorized access or tampering.Overall, a video steganography module should be designed to provide a high level of security, while maintaining the quality and integrity of the video file.

5.3 WORKFLOW FOR PROPOSED SYSTEM

Video Selection:

The first step in the proposed system would be to select the input video file that needs to be hidden. This video would be the one that will be used for steganography.

Selection of the Secret Data:

The next step would involve selecting the data that needs to be hidden within the input video. This data can be in the form of text, images, or any other type of multimedia content.

Encoding the Secret Data:

Once the secret data has been selected, the system would encode this data into a form that can be easily hidden within the input video. This encoding would involve using a steganography algorithm that is specifically designed for video files.

Embedding the Secret Data:

After encoding the secret data, the system would embed it within the input video. This would involve hiding the encoded data within the video frames in a way that is not easily detectable.

Decoding the Secret Data:

To extract the secret data from the video, the system would use a decoding algorithm that is capable of retrieving the data from the hidden locations within the video frames.

Output Secret Data:

Once the secret data has been successfully decoded, it would be outputted to the user in the original format that it was encoded in.

In summary, the proposed system would involve selecting an input video file and secret data to be hidden, encoding the secret data using a steganography algorithm, embedding the encoded data within the video frames, decoding the hidden data from the video, and outputting the secret data to the user. This process would enable users tohide sensitive information within video files without arousing suspicion or detection.

5.4 METHODOLOGY AND FESSIABILITY STUDY

5.4.1 METHODOLOGY

The goals and objectives were presented and explained in detail.

In this article, the methodology to accomplish those goals and objectives . Steganography is a technique that enables party to transmit data or message to another without the communication being perceptible to others. The message is embedded in cover media in a manner that only the sender and intended receiver have knowledge of the existence of the message, and the method to retrieve it. Steganography involves hiding the contents inside a file and not scrambling the data, so it is structurally unmodified and intact. Thus, Steganography has an advantage over cryptography as it involves both encryption and obscurity. Image, text, audio can be the cover media. Data in the form of text, audio and video can be embedded in the carrier. The most commonly used carrier is image. To transmit much higher amount of secret data, a video can be used instead.

5.4.2 FESSIABILITY STUDY

This Report investigates feasibilities of technological solutions Video steganography is considered as a method of hiding information and secret communication of the most significant problems occurred on the secure the data transmission in the electronic era. Themain purpose is to important for the efficient data transfer of the data and to maintain the secrecy of the data that is to be transmitted. From the past time to present time security of confidential information is always an important issue. A novel technique is proposed to conceal the existence of the message so that it

CHAPTER 6

RESULTS AND DISCUSSIONS

CHAPTER 6

RESULTS AND DISCUSSIONS

6.1 TYPES OF TESTING

Unit testing verification efforts on the smallest unit of software design, module. This is known as "Module Testing". The modules are tested separately. This testing is carried out during programming stage itself. In these testing steps, each module is found to be working satisfactorily as regard to the expected output from the module.

BLACK BOX TESTING

Black box testing, also known as Behavioral Testing, is a software testing method in which the internal structure/ design/ implementation of the item being tested is not known to the tester. These tests can be functional or non-functional, though usually functional.

WHITE-BOX TESTING

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing).

GREY BOX TESTING

Grey box testing is a technique to test the application with having a limited knowledge of the internal workings of an application. To test the Web Services application usually the Grey box testing is used. Grey box testing is performed by end-users and also by testers and developers.

INTEGRATION TESTING

Integration testing is a systematic technique for constructing tests to uncover error associated within the interface. In the project, all the modules are combined and then the entire programmer is tested as a whole. In the integration-testing step, all the error uncovered is corrected for the next testing steps.

Software integration testing is the incremental integration testing of two or more integrated software components on a single platform to produce failures caused by interface defects. The task of the integration test is to check that components or software applications, e.g. components in a software system or – one step up – software applications at the company level – interact without error.

ACCEPTANCE TESTING

User Acceptance Testing is a critical phase of any project and requires significant participation by the end user. It also ensures that the system meets the functional requirements.

6.2 TEST CASES & REPORTS

TEST CASE ID	TESTCASE/ ACTION TO BE PERFORMED	EXPECTED RESULT	ACTUAL RESULT	PASS/ FAIL
1.	Displays Image and video screen	Displaying th image an video screen	Displaying the image and video screen	Pass
2.	Pressing the image icon	Open and displays the image page used for encryption	Open and displays the image page used for encryption	Pass

3.	Pressing the video icon	Open and displays the image page used for encryption	Open and displays the image page used for encryption	Pass
4.	Encoding the text for encryption	Encodes the text	Encodes the text	Pass
5.	Decoding the encrypted text	Decoding the text	Decoding th text	Pass

Fig 6.2 Testing table for image and video steganography using RC6

CHAPTER 7
CONCLUSION

CHAPTER 7

7.1 CONCLUSION

We proposed based In this report, a modular solution is presented to improve web based.We have proposed various methods of steganography and implemented the video steganography process. Deep steganography which is one of the video stegnography methods was implemented on python software. This method explores Steganographic techniques for placing supplementary information in images. Here a method is demonstrated to create a fully trainable system that provides excellent visual results in placing a color image into another image. The chosen system should be retrained as a hiding network where the secret image's local structure should not be exploited for encoding information. Methods are proposed to make it difficult for the attacker to recover the contents of the hidden image by reducing the similarity of cover image's residual to the hidden image.

7.1 FUTURE ENHANCEMENTS

Future work in the field of image video stegnography can focus on several aspects to further enhance the technology and its applications. Here are some potential areas for future research and development:

The future of the rapid growth of science and technology in the telecommunications world can come up with new ways for some peoplebent on abusing for threatening information security as hackers, crackers, carder, phreaker and so on. If the information is on the wrong side will result in losses. Information that must be considered is the security of confidential information. Steganography is a method that can be used to hide a message by using digital media. Digital Steganography using digital media as the container vessel such as images, sounds, text, and video. Hidden secret data can also include images, audio, text, and video. In this final audio steganography implemented. One method that can be used in steganography is the Least Significant Bit (LSB). Steganography implementation will be accompanied by the application of cryptography in the form of encryption and decryption.

APPENDICES

APPENDICES

A1. SDG: Goal 8(Decent Work and Economic Growth)

The Sustainable Development Goal 8 (SDG 8) focuses on promoting sustained,inclusive, and sustainable economic growth, full and productive employment, and decent work for all. It primarily addresses issues related to job creation, improving work conditions, and ensuring fair economic opportunities.

A2. SOURCE CODE

```
from flask import Flask,render_template,requestimport

os

from werkzeug.utils import secure_filenamefrom

encrypt import
*
from decrypt import *from
main import * import
webview


app=Flask(_____name___)
# window = webview.create_window('bala', app)
```

```
@app.route('/')
def home():
    return render_template("home.html")


@app.route("/imghome")def
img_home():
    return render_template("img.html")

    @app.route("/vidhome")de

      vid_home():
    return render_template("vid.html")

        @app.route("/image",methods=['GET',    'POST'])def
  image():
    if            request.method=="POST":
        key=request.form["key"]
        sentence=request.form["string"]
        file=request.files["upload"]


        print(key)
        print(sentence)
        print(file)
        files=file.filename
        basepath = os.path.dirname(_____file___)
        print(basepath)
        file_path=os.path.join(basepath,'uploads',secure_filename(file.filename))

        file.save(file_path)
        print(file_path)
```

```
        esentence,message,key=main(key,sentence,files) #
        main()


    #else:
    #       key  =  request.args.get('key')
    #       string = request.args.get('time')
    #       file = request.args.get('Airport Names')
    return
render_template("img.html",key=key,message=message,Encrypt_Key=esentence  )


@app.route("/deimg", methods=["POST"])def
deimg():
    file=request.files["uploads"]
    key=request.form["dkey"] files=file.filename
    basepath = os.path.dirname(_____file_)
    print(basepath)
    file_path = os.path.join(basepath, 'uploads',
secure_filename(file.filename))
    file.save(file_path)
    hidden_data,sentence=dmain(key,files)
    return render_template("img.html",hd=hidden_data,dmessage=sentence)



@app.route("/video", methods=["POST"])def
video():
```

```
    key=request.form["vkey"]
    input_string=request.form["vstring"
      file=request.files["vupload"]
    print(key)  print(input_string)
    print(file)  files=file.filename
    print(files)
    basepath = os.path.dirname(__file__)
    print(basepath)
    file_path = os.path.join(basepath, 'uploads',
 secure_filename(file.filename))
    file.save(file_path)
    print(file_path)
    esentence,input_string,key=vmain(key,input_string,files)
    return render_template("vid.html",ensentence=esentence,message=input_string,k  ey=key)


@app.route("/devid", methods=["POST"])def
 devid():
    key=request.form["vdkey"]
    file=request.files["vuploads"]
    files=file.filename print(files)
    basepath = os.path.dirname(_____file__)
    print(basepath)
    file_path=os.path.join(basepath,'uploads',
 secure_filename(file.filename))
    ]


    file.save(file_path)
    print(file_path)
```

```
    sentence,secret_dec=decode_string(key,files)
 return render_template("vid.html",dmessage=sentence,hd=secret_dec)if name
____==    "__main__":
    app.run(debug=True)#
    webview.start()
fromstegano import lsb
 from os.path import isfile,join
 from helpers import *
 import time
 #install time ,opencv,numpy modules
 import cv2
 import numpy as np
 import math
 import os
 import shutil
 from subprocess import call,STDOUTfrom
 termcolor import cprint
 import moviepy.editor
 from moviepy.editor import *
 from werkzeug.utils import secure_filenamefrom
 PIL import Image
 import PIL
```

```
def encrypt(sentence,s):
    encoded = blockConverter(sentence)
    enlength = len(encoded)
    A = int(encoded[0],2)B
    =    int(encoded[1],2)C=
    int(encoded[2],2)D          =
    int(encoded[3],2)orgi   = []
    orgi.append(A)
    orgi.append(B)
    orgi.append(C)
    orgi.append(D)
    r=12
    w=32
    modulo = 2**32
    lgw = 5
    B = (B + s[0])%modulo D
    = (D + s[1])%modulo for i in
    range(1,r+1):
        t_temp    =    (B*(2*B    +    1))%modulot    =
        ROL(t_temp,lgw,32)
        u_temp  =  (D*(2*D  +  1))%modulou  =
        ROL(u_temp,lgw,32)            tmod=t%32
        umod=u%32
```

```
        A = (ROL(A^t,umod,32) + s[2*i])%modulo

        C = (ROL(C^u,tmod,32) + s[2*i+ 1])%modulo(A, B, C,
        D) = (B, C, D, A)
    A = (A + s[2*r + 2])%moduloC =
    (C + s[2*r + 3])%modulocipher =
    []
    cipher.append(A)
    cipher.append(B)
    cipher.append(C)
    cipher.append(D)
    return orgi,cipher

def decrypt(secret_dec,s):

    encoded = blockConverter(secret_dec)
    enlength = len(encoded)
    A = int(encoded[0],2)B

    = int(encoded[1],2)C =
    int(encoded[2],2)D =
    int(encoded[3],2)cipher
    = [] cipher.append(A)
    cipher.append(B)
    cipher.append(C)
    cipher.append(D)  r=12
    w=32
```

```
    modulo = 2**32
    lgw = 5
    C = (C - s[2*r+3])%moduloA =
    (A - s[2*r+2])%modulo for j in
    range(1,r+1):
        i = r+1-j

        (A, B, C, D) = (D, A, B, C)

        u_temp = (D*(2*D + 1))%modulou = ROL(u_temp,lgw,32)
        t_temp = (B*(2*B + 1))%modulot =
        ROL(t_temp,lgw,32)              tmod=t%32
        umod=u%32
        C = (ROR((C-s[2*i+1])%modulo,tmod,32) ^u)A =
        (ROR((A-s[2*i])%modulo,umod,32)                ^t)
    D = (D - s[1])%moduloB

    = (B - s[0])%moduloorgi

    = [] orgi.append(A)
    orgi.append(B)
    orgi.append(C)
    orgi.append(D)
    return cipher,orgi


def frame_extraction(files):

    if not os.path.exists("./tmp"):
```

```
        os.makedirs("tmp")
    temp_folder="./tmp"
    print("[INFO] tmp directory is created")


    vidcap = cv2.VideoCapture("uploads/{}".format(files))count =
    0

    while True:

        success, image = vidcap.read()if
        not success:
            break

        cv2.imwrite(os.path.join(temp_folder,                "{:d}.png".format(count)),
image)

        count += 1

    print("video encodesucess")


def decframe_extraction(files): if not
    os.path.exists("./tmps"):
        os.makedirs("tmps")                temp_folder="./tmps"
    print("[INFO] tmp directory is created")


    vidcap   =   cv2.VideoCapture(files)
    count = 0

    while True:
```

```
        success, image = vidcap.read()if
        not success:
            break
        cv2.imwrite(os.path.join(temp_folder,                "{:d}.png".format(count)),
image)
        count += 1
    print("video encodesucess")


def                encode_string(esentence,root="./tmp/"):
    files="{}{}.png".format(root,0)
    secret_enc=lsb.hide(files,esentence)
    secret_enc.save(files)



# def audio(files):


#       video = moviepy.editor.VideoFileClip("uploads/{}".format(files))#
        audio = video.audio
#       audio.write_audiofile("sample.mp3")#
        clip = VideoFileClip("finish.mov")
#       audioclip = AudioFileClip("sample.mp3")#
        videoclip = clip.set_audio(audioclip)
```

```
def con_video(files):
    image_folder = 'tmp'
    video_name = 'video.avi'

    images = [img for img in os.listdir(image_folder) if
img.endswith(".png")]
    frame = cv2.imread(os.path.join(image_folder, images[0]))
    height=720
    width=1280

    video = cv2.VideoWriter(video_name, 0, 30, (width,height))for image in
   images:
        video.write(cv2.imread(os.path.join(image_folder, image)))
   cv2.destroyAllWindows()
    video.release()


def decode_string(key,files):#
    files=files[ :-4]
    #         files="{}.mp4".format(files)
    decframe_extraction(files)
 root="./tmp/"
  secret=[]
    # for i in range(len(os.listdir(root))):
    f_name="{}{}.png".format(root,0)
    secret_dec=lsb.reveal(f_name)
    print(secret_dec)
    if secret_dec == None:
        print("none")
```

```
secret.append(secret_dec)
clean_tmp()

# print(hidden_data)

print ("DECRYPTION: ") #key='A
WORD IS A WORD'
# key =input("Enter Key(0-16 characters): ")if
len(key) <16:
    key = key + " "*(16-len(key))key

= key[:16]


print ("UserKey: "+key )s =
generateKey(key)

cipher,orgi = decrypt(secret_dec,s)
sentence = deBlocker(orgi)
print ("\nEncrypted String list: ",cipher) print
("Encrypted String: " + secret_dec)
print ("Length of Encrypted String: ",len(secret_dec))print
("\nDecrypted String list: ",orgi)
print ("Decrypted String: " + sentence )

print ("Length of Decrypted String: ",len(sentence))
clean_tmp()
clean_tmps()

return sentence,secret_dec
```

```
        def    clean_tmp(path="./tmp"):try:
                if os.path.exists(path):
                    shutil.rmtree(path)
                    print("[INFO] tmp files are cleaned up") except:
                print("[INFO] tmp files are cleaned up")
def      clean_tmps(path="./tmps"):try:     if
os.path.exists(path): shutil.rmtree(path)
                    print("[INFO] tmp files are cleaned up") except:
                print("[INFO] tmp files are cleaned up")
        def vmain(key,input_string,files):
            # input_string = input("Enter the input string :")#
            f_name=input("Enter the name of video: ") print
            ("ENCRYPTION: ")
            #key='A WORD IS A WORD'
            # key = input("Enter Key(0-16 characters): ")if
            len(key) <16:
                key = key + " "*(16-len(key))key
            = key[:16]
```

```
        print ("UserKey: "+key )s =
        generateKey(key)
        #sentence = 'I WORD IS A WORD'

        # sentence =input("Enter Sentence(0-16 characters): ")if
        len(input_string) <16:
            input_string = input_string + " "*(16-len(input_string))
        input_string = input_string[:16]


        orgi,cipher = encrypt(input_string,s)
        esentence = deBlocker(cipher)


        print ("\nInput String: "+input_string )print
        ("Original String list: ",orgi)
        print ("Length of Input String: ",len(input_string))
        print ("\nEncrypted String list: ",cipher)print
        ("Encrypted String: " + esentence)
        print ("Length of Encrypted String: ",len(esentence))# f =
        open("encrypted.txt", encoding="utf-8","w")
        with open("encrypted.txt", "w", encoding="utf-8") as f:
            f.write(esentence)
            f.close()
        frame_extraction(files)
        encode_string(esentence)
        con_video(files)
        return esentence,input_string,key
#       audio(files)#
clean
```

A3. SCREEN SHOTS

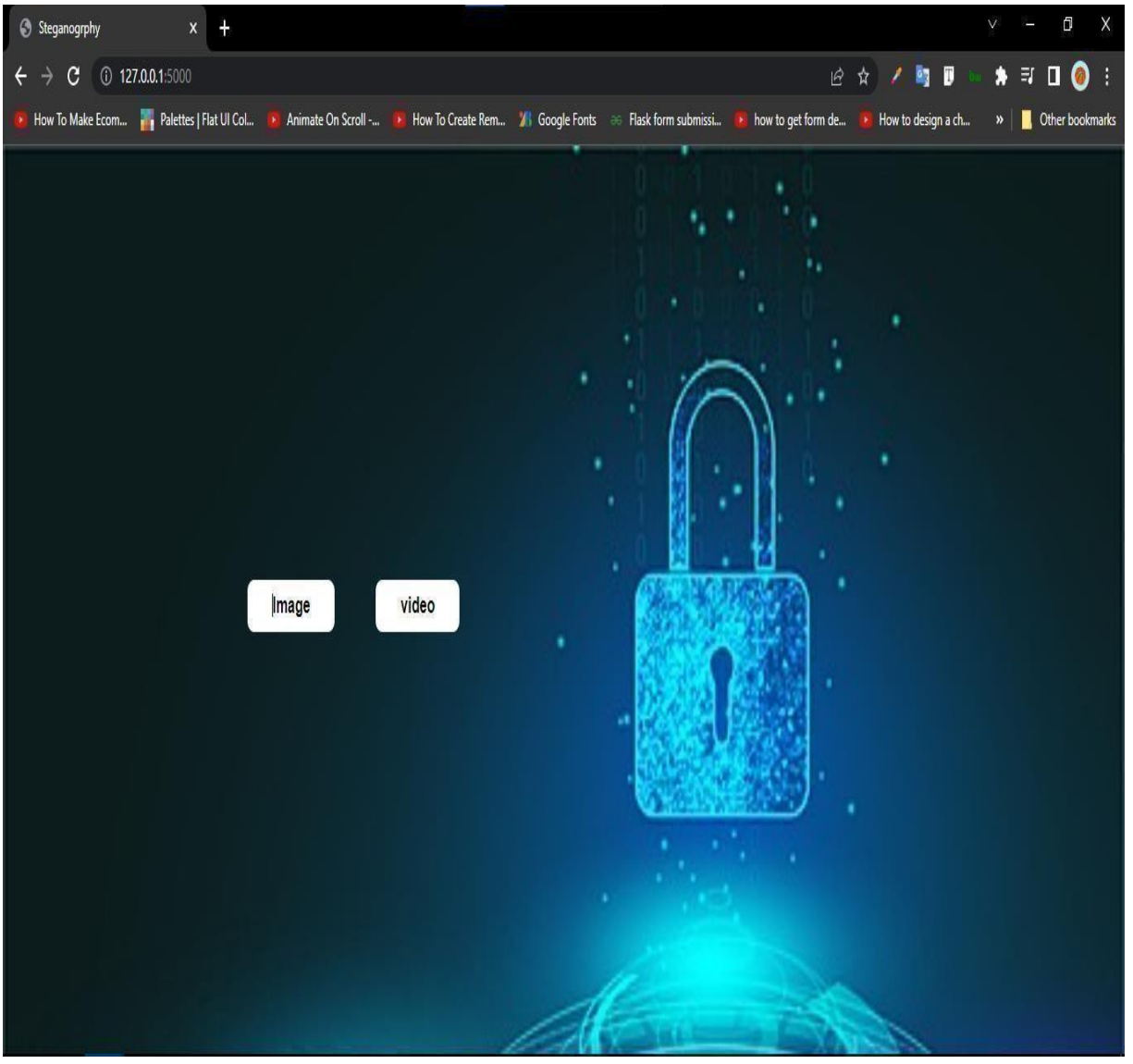


Fig A.3.1 Displays image and video button for steganography

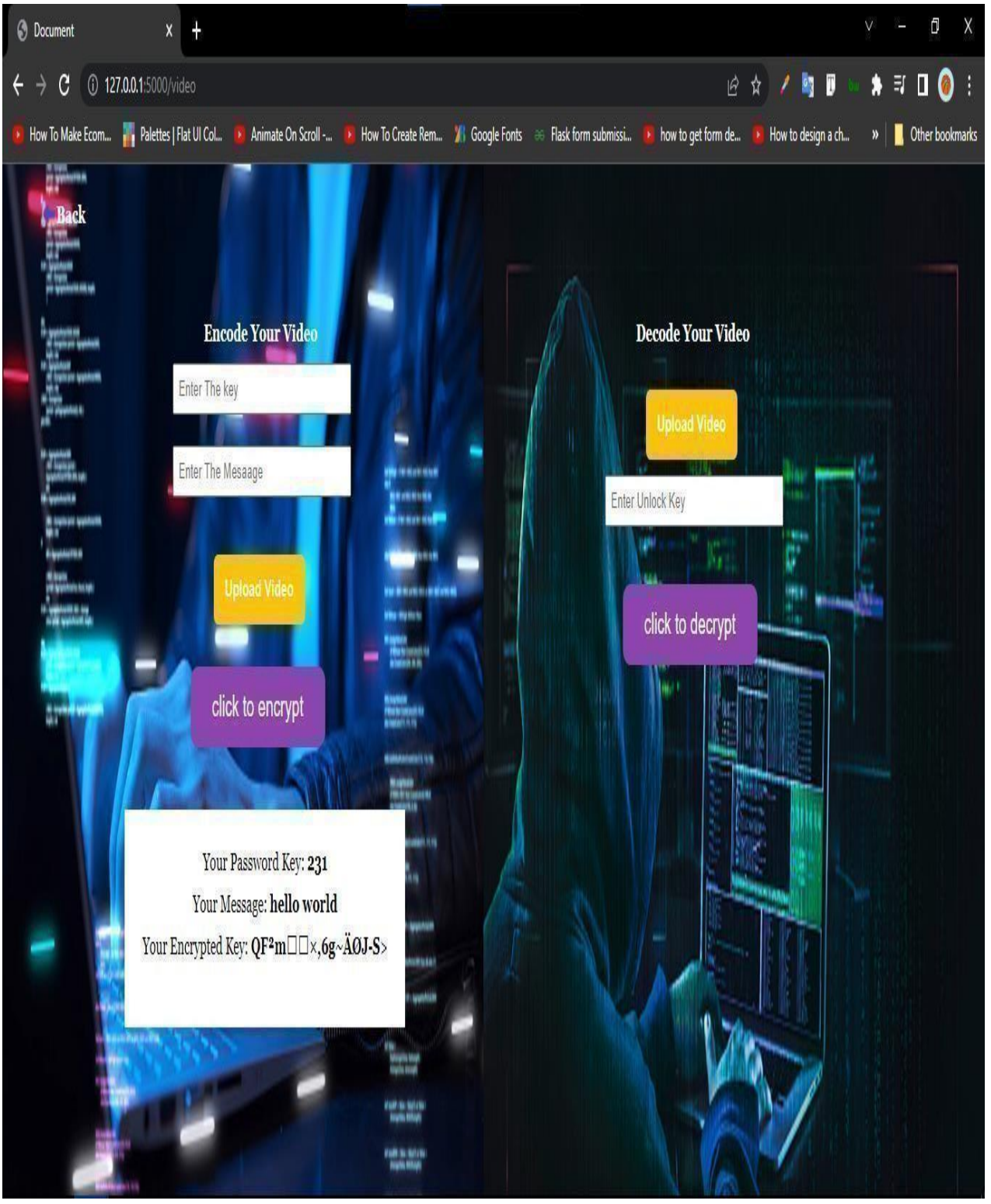


Fig A.3.2 choosing a video for steganography and entering the text which need to be encrypt and also entering the key for encryption.

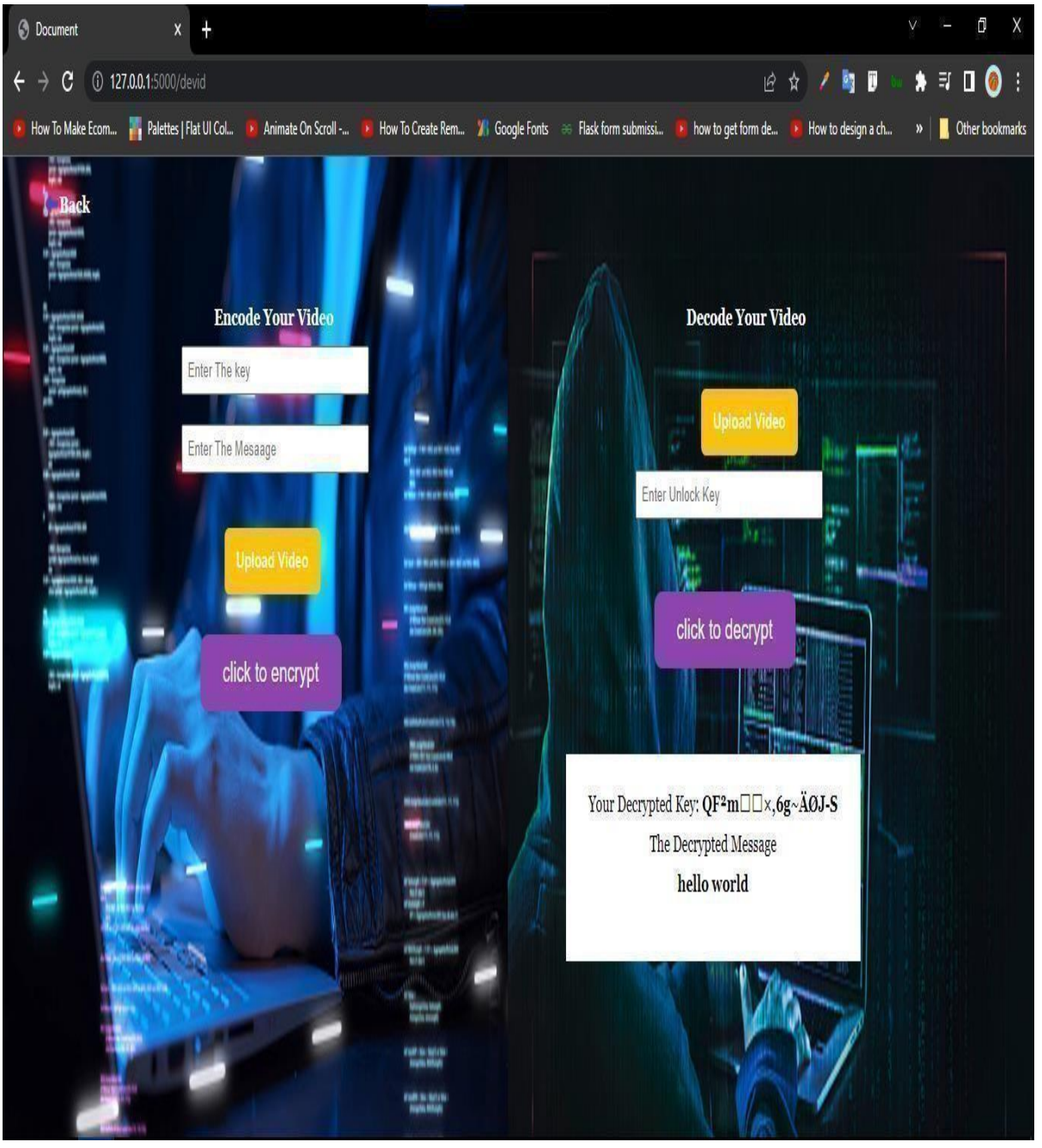


Fig A.3.3 Decrypts the text using the key and decrypting algorithm

PLAGIARISM REPORT

RE-2022-219744-plag-report

ORIGINALITY REPORT

5%	1%	4%	2%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	CRYPTOGRAPHY IS A ART OF PHYSICAL SCRAMBLING OF INFORMATIONS IN IT PUBLICATIONS	1%
2	IT IS A PROPRIETY ALGORITHM BY RSA PUBLICATIONS	1%
3	RC6 IS FASTER BLOCK OF CIPHER STUDENT PAPER	1%
4	DECODING ALGORITHM HAVE HIDDEN INFORMATION WITH HIGH ACCURACY INTERNET SOURCE	<1%
5	DATA IN THE FORM OF TEXT, AUDIO AND VIDEO INTERNET SOURCE	<1%
6	MODULES ARE TESTED STUDENT PAPER	<1%
7	INTEGRATION TESTING INTERNET EXPLORER	<1%

Paper Publication

International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI-2024) ×

Dear Monica K,
Title: Image and Video Stegnography using RC6
Paper ID: ACCAI-24-T3-6113
Your Paper has been successfully submitted.
If you need more clarification, please send mail to accai@stjosephs.ac.in.

Close

7.3 REFERENCES

[1] Ramadhan J. Mstafa, Khaled M. Elleithy,and Abdelfattah, "A Robust and Secure Video Steganography Method in DWT- DCT Domains Based on Multiple Object Tracking and ECC".

[2] Sofyane Ladgham Chikouche and Noureddine Chikouche, "An Improved Approach for LSB-Based Image Steganography using AES Algorithm" The 5th International Conference on Electrical Engineering – ICEE-B October 29- 31, 2017.

[3] Jorg J. Buchholz, "Advanced Encryption Standard" http://buchholz.hs- bremen.de , December 19, 2001.

[4] Shumeet Baluja "Hiding Images in Plain Sight : Deep Steganography" 31st Conference on Neural Information Processing Systems NIPS 2017.

[5] Priya Paresh Bandekar and Suguna G C, "LSB Based Text and Image Steganography using AES Algorithm" the International Conference on Communication and Electronics systems (ICCES 2018) IEEE Xplore Part Number: ISBN:978-1-5386-4765-3.

[6] Q. Kester, "A cryptographic Image Encryption technique based on the RGB PIXEL shuffling A cryptographic Image Encryption technique based on the RGB PIXEL shuffling", International Journal of Advanced Research in Computer Engineering & Technology, vol. 2,no.2 pp.848-854, January 2013.

[7] P. Sahute, S. Waghamare, S. Patil, and A. Diwate, " Secure Messaging Using Image Steganography", International Journal of Modern Trends in Engineering and Research,vol.2,no.3, pp. 598–608, March 2015.

[8] N. Agarwal and P. Agarwal, "An Efficient Shuffling Technique on RGB Pixels for Image Encryption", MIT International Journal of Computer Science & Information Technology, vol. 3, no. 2, pp. 77–81, August 2013.

[9]

[9] K. Hamdnaalla, A. Wahaballa, and O. Wahballa, “Digital Image Confidentialit Depends upon Arnold Transformation and RC4 Algorithms”, International Journal of Video & Image Processing and Network Security, vol.13, no. 04,August 2013.

[10] N. G. A. P. H. Saptarini, Y. A. Sir, “Digital Color Image Encryption Using RC4Stream Cipher and Chaotic Logistic Map”, Information Systems International Conference, December, pp. 2–4, December 2013.

[11] Amin, J., Anjum, M. A., Ibrar, K., Sharif, M., Kadry, S., & Crespo, R. G. (2023). Detection of anomaly in surveillance videos using quantum convolutional neural networks.Image and Vision Computing, 135, 104710.

[12] Arafath, M. D., & Kumar, A. N. (2023). Quantum Computing Based Neural Networks forAnomaly Classification in Real-Time Surveillance Videos. Computer Systems Science & Engineering, 46(2).

[13] Arunnehru, J. (2023). Deep learning-based real-world object detection and improvedanomaly detection for surveillance videos. Materials Today: Proceedings, 80, 2911-2916.

[14] Rosenhahn, B., & Hirche, C. (2024). Quantum Normalizing Flows for Anomaly Detection.arXiv preprint arXiv:2402.02866.

[15] Bustos-Brinez, O. A., Gallego-Mejia, J. A., & González, F. A. (2023, February). AD-DMKDE: Anomaly Detection through Density Matrices and Fourier Features. In International Conference on Information Technology & Systems (pp. 327-338). Cham: Springer InternationalPublishing.

[16] Choudhry, N., Abawajy, J., Huda, S., & Rao, I. (2023). A Comprehensive

Survey ofMachine Learning Methods for Surveillance Videos Anomaly Detection. IEEE Access.

[17] Khan, K. (2023). A taxonomy for the use of quantum computing in drone video streamingtechnology. Zenodo (CERN European Organization for Nuclear Research), 10.

[18] Zhang, H., Xie, R., Li, K., Huang, W., Yang, C., & Liu, J. (2023, July). Anomaly detectionbased on deep learning: insights and opportunities. In 2023 IEEE 10th International Conferenceon Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 30-36). IEEE.

[19] Roka, S., & Diwakar, M. (2023). Deep stacked denoising autoencoder for unsupervised anomaly detection in video surveillance. Journal of Electronic Imaging, 32(3), 033015-033015. Video Anomaly Detection Performance of Pixel-and Frame-Based Techniques Using MachineLearning Algorithms. Computation, 12(2), 19.

[21] Zhang, H., Xie, R., Li, K., Huang, W., Yang, C., & Liu, J. (2023, July). Anomaly detectionbased on deep learning: insights and opportunities. In 2023 IEEE 10th International Conferenceon Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom) (pp. 30-36). IEEE.

[22] Roka, S., & Diwakar, M. (2023). Deep stacked denoising autoencoder for unsupervised anomaly detection in video surveillance. Journal of Electronic Imaging, 32(3), 033015-033015

.