AMiniProjectReport

ON

SECURE DATAENCRYPTION AND DECRYPTION USING CRYPTO-STEGO

SUBMITTED BY:

**NAME:**SANDEEPSOLANKI, **ROLLNO.:** 2101330100200 **NAME:**SHAKILURREHMAN,**ROLLNO.:**2101330100205 **NAME:** SIMRAN UPADHYAY**R**,**OLLNO.:**2101330100222

UNDER SUPERVISIONOF MS. SURBHI JHA

MR. ADITYANARAYAN

2022-2023

DEPARTMENTOF COMPUTER SCIENCE AND ENGINEERING

**NOIDA** **INSTITUE** **OF** **ENGINEERING** **AND** **TECHNOLOGY,** **GREATERNOIDA**

**INDEX**

|  |  |  |
| --- | --- | --- |
| **S.** **No.** | **TITLE** | **Pg** **No.** |
| 1. | Acknowledgement | 3 |
| 2. | Prerequisite Knowledge Required | 4 |
| 3. | Introduction | 5-8 |
| 4. | Overalldescription | 9-19 |
| 5. | External interface requirements | 20-23 |
| 6. | System features | 23 |
| 7. | Other non-functional requirements | 24-29 |
| 8. | Other requirements | 30 |
| 9. | Output | 31 |
| 10 | Conclusion and references | 33 |
| 11. | Certification of guided project | 34 |

**ACKNOWLEDGEMENT**

We are highly indebted to (NOIDA INSTITUE OF ENGINEERING AND TECHNOLOGY, GREATER NOIDA) for their guidance and constant supervision as well as for providing necessary information regarding the project & also for their support in completing the project.

We would like to express our gratitude towards our mentors and coordinators for their kind co-operation and encouragement which help us in completion of this project.

We would like to express our special gratitude and thanks to industry persons for giving us such attentionand time.

our thanks and appreciations also go to our teammates in developing the project and people who have willingly helped us out with their abilities.

We would like to thank our Class Coordinator and **Mr.** **Aditya** **Narayan** and **Ms.** **Surbhi** **Jha**, MINI PROJECT coordinator Department of CSE for their support and advice to get and complete mini project in above said organization. We are extremely grateful to our department staff members and friends who helped us in successful completion of this mini project.

**SANDEEP** **SOLANKI** **(21013301001200)** **SHAKIL** **UR** **REHMAN** **(2101330100205)** **SIMRAN** **UPADHYAY** **(2101330100222)**

**Prerequisite** **Knowledge** **Required**

1. Student should have depth knowledge of programming.

2.Student should know some key concepts of Python programming.

3. Student should know basics of computer and how it works.

4.It is preferred to get hands on Jupyter notebook basic and its syntax, and other type declaration.

5. Student should know about basic of encoding and decoding.

6. Student should know about the GUI.

7. Student should know about Eclipse IDE.

**1.** **Introduction** **Purpose**

The purpose of secure data encryption and decryption using cryptosteganography is to protect sensitive or confidential information from unauthorized access or interception.

Encryption involves converting plain text or data into a code or cipher, making it unreadable to anyone without the key to decode it. This ensures that even if someone intercepts the data, they cannot understand its contents.

However, encryption alone may not be sufficient to protect data from interception or theft. This is where steganography comes into play. Steganography involves hiding data within other data, such as an image or video, in a way that is not noticeable to the naked eye. This can make it more difficult for unauthorized parties to detect the existence of the data.

Overall, the purpose of secure data encryption and decryption using crypto steganography is to provide a high level of security and privacy for sensitive information.

**DocumentConventions**

When creating a document on secure data encryption and decryption using crypto-steganography, it is important to follow some conventions to ensure that the information is clear and easy to understand. Here are some guidelines to consider:

Use clear and concise language: Use simple, straightforward language that is easy to understand, especially if the intended audience is not familiar with technical terms.

Define technical terms: When using technical terms or acronyms, provide a clear definition to avoid confusion.

Explain the concepts: Explain the concepts of encryption and steganography in detail, including the types of encryption algorithms and steganography techniques that can be used.

Provide examples: Provide examples of how encryption and steganography can be used together,such as hiding encrypted data within an image or audio file.

Include diagrams: Include diagrams or illustrations to help visualize the encryption and steganographyprocess.

Explain the importance of key management: Discuss the importance of key management in ensuring the security of encrypted data and how to securely store and manage keys.

Discuss limitations: Discuss the limitations of encryption and steganography and potential vulnerabilities or attacks that may compromise their security.

Provide best practices: Provide best practices for implementing secure data encryption and decryption using crypto steganography, including how to choose strong encryption algorithms and steganography techniques, how to verify the integrity of the encrypted data, and how to securely transfer and store encrypted data.

By following these conventions, the document on secure data encryption and decryption using crypto steganography can provide a comprehensive guide for users to understand and implement this technology securely.

**Intended** **Audience** **and** **Reading**

The intended audience for a document on secure data encryption and decryption using crypto steganography can vary depending on the purpose and context of the document. However,some potential audiences may include:

Information security professionals: This audience may include individuals responsible for securing sensitive data in an organization, such as security analysts, IT managers, and network administrators.

Researchers and academics: This audience may include individuals studying information security, cryptography, or steganography, such as graduate students or professors.

General readers: This audience may include anyone interested in learning about secure data encryption and decryption using cryptosteganography, including individuals who may need to protect their personal data, such as journalists or activists.

"Cryptography and Network Security: Principles and Practice" by William Stallings. This book provides a comprehensive introduction to cryptography and network security, including an overview of encryption algorithms and steganography techniques.

"Handbook of Information and Communication Security" edited by Peter Stavroulakis and Mark Stamp. This book provides an overview of various information and communication security topics, including cryptography and steganography.

"Applied Cryptography: Protocols, Algorithms, and Source Code in C" by Bruce Schneier. This book provides a practical guide to cryptography, including detailed explanations of encryption algorithms and how to use them in real-world applications.

By reading these resources, individuals can gain a deeper understanding of the concepts and techniques involved in secure data encryption and decryption using crypto steganography.

**ProductScope**

The product scope for making secure data encryption and decryption using crypto steganography can be defined as the set of features and functionality that the product will provide to ensure the security of sensitive information. Some of the keyaspects to consider when defining the product scope may include:

Encryption algorithms: The product should support a range of strong encryption algorithms, such as Advanced Encryption Standard (AES) or RSA, to ensure the confidentiality ofthe data.

Steganography techniques: The product should provide various steganography techniques, such as Least Significant Bit (LSB) or Spread Spectrum, to hide the encrypted data within other data.

Key management: The product should provide a secure key management system to ensure that the encryption keys are generatedand stored securely.

Data verification: The product should provide mechanisms to verify the integrity of the encrypted data, such as message authentication codes (MACs).

User interface: The product should provide an intuitive user interface that allows users to easily encrypt and decrypt data, select the steganography technique and encryption algorithm, and manage keys.

Integration with other tools: The product should provide integration with other security tools and systems, such as firewalls or intrusion detection systems, to enhance the overall security posture.

Platform compatibility: The product should be compatible with a range of platforms, such as Windows, Linux, or MacOS, to ensure wide adoption and ease of use.

Documentation and support: The product should provide comprehensive documentation and support to assist users in setting up and using the product securely.

By defining the product scope for making secure data encryption and decryption using crypto-steganography, the development team can focus on building a product that meets the needs of users and provides a high level of security for sensitive information.

**2.** **Overall** **description** **ProductPerspective**

Hardware Requirements The hardware requirements for the secure data encryption and decryption system are as follows:

A computer with a minimum of 2GHz processor At least 4GB of RAM

A graphics card capable of running CUDA. At least 500GB of hard drive space

An internet connection with a minimum speed of 5Mbps Software Requirements

The software requirements for the secure data encryption and decryption systemare as follows:

OperatingSystem:

Windows 10 (64-bit) or Linux (64-bit) Python 3.6 or higher CUDA toolkit 10.0 or higher

TensorFlow 2.0 or higher

PyTorch OpenCV

NumPy

1.0 or higher 4.0 or higher

1.16.4 or higher

Features

The secure data encryption and decryption system using crypto-stego has the following features:

End-to-end encryption: The system uses AES-256 encryption to ensure that sensitive datais protected from unauthorized access during transmission.

Steganography: The system uses steganography to conceal the fact that the data is even being transmitted. This adds an extra layer of security, as it makes it difficult for attackersto even detect that sensitive data is being sent.

Compatibility: The system is compatible with both Windows and Linux operating systems and can be used with any programming language that supports the TensorFlow and PyTorch libraries. Speed: The system is designed to be fast and efficient, with the ability to encrypt and decrypt large files in a matter of seconds. Customizable: The system is highly customizable, with the ability to adjust the encryption and steganography parameters to meet the specific needs of the user. Benefits

The secure data encryption and decryption system using crypto-stego provides the following benefits:

Enhanced security: The use of AES-256 encryption and steganography ensures that sensitive data is protected from unauthorized accessand detection.

Improved privacy: By using steganographyto conceal the transmission of sensitive data, users can ensure that their privacy is protected from prying eyes.

Increased efficiency: The system is designed to be fast and efficient, allowing users to encrypt and decrypt large files quickly and easily.

Customizability: The ability to adjust the encryption and steganography parameters allows users to tailor the system to their specific needs and preferences.

Conclusion The secure data encryption and decryption system using crypto-stego provides a powerful solution for protecting sensitive data during transmission. By using AES-256 encryption and steganography, the system ensures that data is both secure and private, while also providing a fast and efficient solution that can be customized to meet the specific needs of the user. With its compatibility with both Windows and Linux operating systems, and its ability to be used with any programming language that supports the TensorFlow and PyTorch libraries, the system is an ideal choice for anyone who needs to protect sensitive data during transmission.

**ProductFunctions**

Encryption Process

The encryption process of the secure data encryption and decryption system using crypto-stego involves the following functions:

Data input: The user inputs the sensitive data they wish to encrypt into the system.

AES-256 encryption: The system uses the Advanced Encryption Standard (AES) with a key size of 256 bits to encrypt the data. This ensures that the data is protected from unauthorized access during transmission.

Steganography: The encrypted data is then concealed using steganography techniques, such as LSB (Least Significant Bit) hiding. This conceals the data within an image or video file, making it difficult for attackers to detect that sensitive data is being transmitted.

Transmission:The concealed data is then transmittedto the intended recipient through the internet.

Decryption Process The decryption process of the secure data encryption and decryption system using crypto-stego involves the following functions:

Data input: The recipient inputs the concealed data they have received into the system.

Steganography:The system uses steganographytechniques to extract the encrypted data from the image or video file.

AES-256 decryption: The system uses the AES-256 decryption algorithm to decrypt the data.

Data output: The decrypted data is then outputted to the recipient, who can view and use the sensitive information.

Steganography Techniques The secure data encryption and decryption system using crypto-stego employs various steganography techniques to conceal the sensitive dataduring transmission. These techniques include:

LSB hiding: This technique involves replacing the least significant bit of each pixel in an image or video file with a portion of the encrypted data. This results in a minimal change to the appearance of the file, making it difficult to detect that data is being concealed.

DCT (Discrete Cosine Transform) embedding: This technique involves embedding the encrypted data into the high-frequency coefficients of the DCT transform of an image or video file. This allows for larger amounts of data to be concealed but may result in a more noticeable change in the appearance of the file.

Spread Spectrum: This technique involves embedding the encrypted data into the high-frequency components of an audio file. The data is spread across a wide range of frequencies, making it difficultto detect.

Conclusion The secure data encryption and decryption system using crypto-stego employs a range of technical functions to ensure that sensitive data is protected during transmission. The system uses AES-256 encryption to secure the data, as well as steganography techniques to conceal the transmission of the data. The encryption and decryption processes involve data input, encryption/decryption, and data output. The steganography techniques used include LSB hiding, DCT embedding, and Spread Spectrum. The system provides a powerful and customizable solution forprotecting sensitive data during transmission.

**User** **classes** **and** **Characteristics**

There are three main user classes for the secure data encryption and decryption systemusing crypto-stego:

System Administrators Sender Users RecipientUsers

System Administrators: System Administrators are responsible for managing the overall system, including installing, configuring, and maintaining the system. They are responsible for ensuring that the system is secure, up-to-date, and functioning properly. System Administrators need to have a strong understanding of network security, cryptography, and steganography techniques. They should also be able to troubleshoot and resolve any technical issues that arise.

Sender Users: Sender Users are responsible for encrypting and transmitting sensitive data through the system. They may be employees of an organization, partners, or other stakeholders. Sender Users need to have a basic understanding of the system, including how to input the data they wish to encrypt and transmit, as well as how to select the appropriate steganography technique to use. They also need to be aware of the risks associated with transmitting sensitive data and should understand how to minimize those risks.

Recipient Users: Recipient Users are responsible for receiving and decrypting sensitive data transmitted through the system. They may be employees of an organization, partners, or other stakeholders. Recipient Users need to have a basic understanding of the system, including how to input the concealed data they have received and how to extract the encrypted data from the image or video file. They also need to understand how to decrypt the data using the appropriate key.

User Characteristics Each user class has its own unique characteristics that should be taken into account when designing the system:

System Administrators need to have a strong technical background in network security, cryptography, and steganography techniques. They should be able to troubleshoot and resolve technical issues that arise. Sender Users may have varying degrees of technical expertise, so the system should be designed with user-friendliness in mind. They need to be able to easily input and transmit data and select the appropriate steganographytechnique to use.

Recipient Users may have varying degrees of technical expertise, so the system should be designed with user-friendliness in mind. They need to be able to easily extract and decrypt the concealed data using the appropriate key.

Conclusion Understandingthe differentuser classes and their characteristics is important to ensure that the secure data encryption and decryption system using crypto-stego is designed to meet the needs of each user. System Administrators need to have a strong technicalbackground in network security,cryptography,and steganographytechniques. Sender and Recipient Users may have varying degrees of technical expertise, so the system should be designed with user-friendliness in mind.

**OperatingEnvironment**

The operating environment is an essential aspect to consider when designing a secure data encryption and decryption system using cryptos ego. This technical report will provide an overview of the operating environment for such a system, including the hardware and software requirements, as well as the network and security considerations.

Hardware Requirements

The hardware requirements for the secure data encryption and decryption system using crypto-stego are as follows:

A computer with a modern processor (e.g., Intel Core i5 or higher) and at least 8 GB of RAM.

Sufficient hard drive space to store the systemsoftware, encrypted data, and image/video files used for steganography.

A display with a minimum resolution of 1280 x 1024 A mouse and keyboardfor input.

Software RequirementsThe software requirements for the secure data encryption and decryption systemusing crypto-stego are as follows:

An operating system that is up-to-date and supports the necessary software dependencies (e.g., Windows 10 or macOS 10.15 or higher). The necessary cryptographic software libraries (e.g., OpenSSL or Cryptlib).

The necessary steganography software libraries (e.g., StegoTool or JSteg).

A web browser that supports JavaScript and HTML5.

Network Considerations The secure data encryption and decryption system using crypto-stego should be designed to operate on a secure network, with the following considerations in mind:

Use of a Virtual Private Network (VPN) to ensure secure communication between the sender and recipient.

Firewall protection to prevent unauthorized access to the system. Use of secure protocols (e.g., HTTPS) for all data transmission.

Use of strong encryption algorithms (e.g., AES-256) to protect data at rest and in transit.

Security Considerations

Toensure the security of the system, the following security considerations should be taken into account:

Use of strong and unique encryption keysfor each transmission.

Use of multi-factor authentication to prevent unauthorized access to the system.

Regular software updates and security patches to ensure the system is protected against known vulnerabilities. Regular security audits to identify potential weaknesses in the system.

the hardware and softwarerequirements necessary to support the system, as well as the network and security considerations necessary to

ensure the system is secure. By considering these factors, the system can be designed to operate in a secure and efficient manner.

**Design** **and** **Implementation** **Constraints**

The design and implementation of a secure data encryption and decryption system using crypto-stego is subject to several constraints. These constraints can be technical, operational, or environmental, and must be carefully considered to ensure the system is designed and implemented effectively. This technical report will provide an overview of the design and implementation constraints for such a system.

Technical Constraints The technical constraints for the secure data encryption and decryption system using crypto-stego are as follows:

Hardware limitations: The system must be designed to operate on a range of hardware configurations, which may have varying processing power, memory, and storagecapacities.

Cryptographic limitations:The system must support strong cryptographic algorithms that can withstand attacks fromsophisticatedadversaries. Steganography limitations:The system must support steganography techniques that can effectivelyhide the encrypted data within images, audio, or video files. Compatibility limitations: The system must be compatible with a range of operating systems,browsers, and other software dependencies.

Operational Constraints The operational constraints for the secure data encryption and decryption systemusing crypto-stego are as follows:

User requirements: The system must be designed to meet the needs of different types of users, such as individuals, businesses, or government agencies, each with their unique requirements for data security and privacy.

Performance: The system must be designed to operate efficiently, with fast encryption and decryption times and minimal latency.

Environmental Constraints The environmental constraints for the secure data encryption and decryption system using crypto-stego are as follows:

Network limitations: The system must be designed to operate over a range of network types, such as local area networks (LANs), wide area networks (WANs), and the internet, each with their unique limitationson bandwidth and latency.

Security policies: The system must be designed to comply with relevant security policies and regulations, such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS).

Environmentalconditions: The system must be designed to operate in various environmental conditions, such as extreme temperatures, high humidity, or low power supply.

Conclusion: The design and implementation of a secure data encryption and decryption system using crypto-stego is subject to several constraints that mustbe carefully considered. By taking into account these technical, operational, and environmental constraints, the system can be designed and implemented to operate effectively andsecurely,meeting the needs of its users and complying with relevant policies and regulations.

**User** **Documentation**

User documentation is an essential component of any software system, including a secure data encryption and decryption system using cryptostego. This documentation provides users with the necessary information to understand and use the system effectively. This user documentation will provide an overview of the system's features, instructions on how to use the system, and guidance on best practices for data security.

Overview

The secure data encryption and decryption system using crypto-stego is a software system designed to encrypt data and hide it within images, audio, or video files using steganography techniques. This system is intended to provide an additional layer of security for data transmissions, ensuring that data is encrypted and hidden from prying eyes.

Features

The secure data encryption and decryption system using crypto-stego provides the following features:

Encryptionofdatausingstrongcryptographicalgorithms,suchasAES256, ensuring that data is protected from unauthorized access.

Hiding of encrypted datawithin images, audio, or video files using steganography techniques, ensuring that data is hidden from prying eyes.

User-friendly interface, enabling users to easily encrypt and decrypt data using a simple drag-and-drop interface.

Multi-factor authentication, ensuring that only authorized users have access to the system.

Using the System

Touse the secure data encryption and decryption systemusing cryptostego,follow these steps:

install the system software on your computer,following the installation instructions provided with the software.

Launchthesystembyclicking onthesystemicononyourdesktop orin your system tray.

Authenticateyourself by providing the necessary login credentials, **Assumption** **and** **Dependencies**

Assumptions The secure data encryption and decryption system using crypto-stego is based on several assumptions:

The hardware and software used to run the system meet the minimum requirements specified in the system documentation.

The system is installedand configured correctly and is operating as intended.

The cryptographic and steganography algorithms used by the system are secure and cannot be easily broken by an attacker.

The user has the necessary knowledge and skills to use the system effectively and follow best practices for data security.

Dependencies The secure data encryption and decryption systemusing crypto-stego is dependent on the following:

Hardware: The system requires a computer or device with sufficient processing power,memory, and storageto run the system softwareand store encrypted data.

Software:Thesystemisdependent ontheavailabilityandcompatibilityofnecessary software, including the operating system, browser, and other software dependencies.

Cryptographic libraries: The system relies on cryptographic libraries to implement strong encryption algorithms and ensure the security of the data.

Steganography libraries: The system relies on steganography libraries to implement techniques to hide encrypted data within images, audio, or videofiles.

Network infrastructure: The system is dependent on the availability and reliability of the network infrastructureto transmit encrypted data between users.

Security policies and regulations: The system must comply with relevant security policies and regulations, such as the General Data Protection Regulation(GDPR), the Health Insurance Portability and Accountability Act (HIPAA), or the Payment Card Industry Data Security Standard (PCI DSS).

Conclusion:

The secure data encryption and decryption system using crypto-stego is subject to several assumptions and dependencies, which must be taken into account to ensure the system operates effectivelyand securely.

**3.** **External** **interfaces** **requirements**

**User** **Interfaces**

User interfaces play a crucial role in ensuring that a software system is easy to use and intuitive for users. For a secure data encryption and decryption system using crypto-stego, user interfaces should be designed with security and usability in mind. This user interface design should enable users to easily encrypt and decrypt data using a simple, user-friendly interface. In this section, we will discuss the user interfacesfor a secure data encryption and decryption system usingcrypto-stego.

Main User Interface The main user interface for the secure data encryption and decryption system using crypto-stego should provide users with the ability to encrypt and decrypt data using steganography techniques. This interface should be easy to use, intuitive, and provide users with the necessary information to ensure that they are using the system correctly.

The main user interfaceshould consist of the following elements:

Input area: This area should allow users to select the data that they wish to encrypt or decrypt. Users should be able to drag and drop files into the input area or use a file selection dialog to select files.

Output area: This area should display the results of the encryption or decryption process. Users should be able to view the encrypted or decrypted data and save it to a file.

Encryption/Decryption options: This area should allow users to select the type of encryption or decryption they wish to use, such as AES-256 or RSA.

Steganography options: This area should allow users to select the type of steganography they wish to use, such as hiding data within images, audio, or video files.

Status area: This area should display the progress of the encryption or decryption process and provide users with information on any errors or warnings that may occur.

User authentication: This area should prompt users to authenticate themselves beforethey can access the system.Additional User InterfacesIn addition to the main user interface, the secure data encryption and decryption system using crypto-stego may require additional user interfacesto perform certain functions, such as:

Authentication interface: This interface should prompt users to enter their login credentialsto authenticatethemselves before they can access the system.

User management interface: This interface should allow administrators to manage user accounts, such as creating new accounts, deleting accounts, and resetting passwords.

Settings interface: This interface should allow users to configure the settings of the system,such as selecting the default encryption and steganographyoptions.

Conclusion The user interfaces for a secure data encryption and decryption system using crypto-stego should be designed with security and usability in mind. The main user interface should provide users with a simple, intuitive interface to encrypt and decrypt data using steganography techniques, while additional interfaces may be required to perform other functions, such as authentication and user management. By providing a user-friendly interface, the system can be used effectively and efficiently,ensuring that data is secure and protected from unauthorizedaccess.

**HardwareInterfaces**

Hardware interfaces for a secure data encryption and decryption system using crypto-stego are minimal. This is because the system primarily relies on software to encrypt and decrypt data using steganography techniques. However, there are a fewhardwareinterfacesthatareessentialfortheproperfunctioning of the system:

Computer: The system requires a computer to run the software that performs the encryption and decryption of data.

Input/output devices: The system needs input/output devices such as a keyboard, mouse, and monitor to enable users to interact with the software and view the results of the encryption and decryption processes.

Network interface: If the system is used to encrypt and decrypt data transmitted over a network, the computer running the system needs to have a network interface,such as an Ethernet or Wi-Fi adapter,to connect to the network.

It is important to ensure that the computer and other hardware components used to run the system meet the minimum hardware requirements specified by the system software. These requirements may include specifications such as processor speed, RAM, and available storage space. Additionally,it is important to ensure that the hardware components used are compatible with the software and operating systemthat the system is running on.

**SoftwareInterfaces**

Software interfaces are essential for a secure data encryption and decryption system using crypto-stego to function effectively. These interfaces allow different software components to communicate with each other and exchange information. The following are some of the softwareinterfaces that are required for a secure data encryption and decryption system using crypto-stego:

Operatingsystem:

The system needs to interact with the underlying operating system to perform functions such as file management, networking, and process management.

Cryptographiclibraries:

The system requires access to cryptographic libraries to perform encryption and decryption of data. These libraries provide the necessary functions and algorithms to perform the cryptographic operations.

Steganographylibraries:

The system requires access to steganography libraries to hide and extract data within media files such as images, audio, and video. User interface libraries: The system requires access to user interface libraries to provide a user-friendly interface for users to interactwith the system.

Databaseinterface:

If the system requires a database to store user information or other data, it needs a database interface to interactwith the database.

Network interface:

If the system is used to encrypt and decrypt data transmitted over a network, it requires a network interface to communicatewith other devices over the network.

It is important to ensure that the software components used in the system are compatible with each other and that the interfaces between them are well-defined and properly documented. Additionally, it is important to ensure that any third-party libraries used in the systemare properly licensed and that the systemcomplies with any licensing requirements.

**Communication** **Interfaces**

Communication interfaces are essential for a secure data encryption and decryption system using crypto-stego to communicate with other devices and systems. These interfaces allow the system to send and receive data securely and efficiently. The following are some of the communication interfaces that may be required for a secure data encryption and decryption system using crypto-stego:

Local network: The system may require a local network interface, such as Ethernet or Wi-Fi, to communicate with other devices on the same network.

Internet: The system may require an internet interface, such as a modem or router, to communicate with other devices and systems overthe internet.

Bluetooth: The system may require a Bluetooth interface to communicate with other devices that support Bluetooth connectivity.

USB: The system may require a USB interface to communicate with other devices that support USB connectivity,such as USB storage devices or smartphones.

Serial port: The system may require a serial port interface to communicate with other devices that support serial port connectivity, such as printers or sensors.

Additionally,it isimportantto ensurethat the communicationinterfacesused in the system comply with any relevant communication standardsand protocols.

**4.** **System** **features**

A secure data encryption and decryption system using crypto-stego should have a number of features to ensure its effectiveness and usability. Some key features of such a system may include:

1.Data encryption and decryption: The system should be able to encrypt and decrypt data securely using cryptographic algorithms and steganography techniques. It should also support various encryption standards and allow users to specify their own encryption keys and algorithms.

2.Media file support: The system should support the encryption and decryption of various types of media files such as images, audio, and video. It should also be able to hide and extract datawithin these files using steganographytechniques.

3.User authentication and access control: The system should require user authentication and access control to ensure that only authorized users can access the system and perform encryption and decryption operations. This can include the use of passwords, biometric authentication,or other security measures.

4.Secure storage: The system should store encrypted and decrypted data securely to prevent unauthorized access or data breaches. It should also provide backup and recovery mechanisms to ensure data can be recovered in the event of a system failureor data loss.

5.User interface: The system should have a user-friendly interface that allows users to easily perform encryption and decryption operations. It should also provide clear feedback and error messages to help users understand the status of their operations.

6.Compatibility: The system should be compatible with various operating systems and hardware configurations to ensure that it can be used in a wide range of environments.

7. Performance: The system should be designed to perform encryption.

Overall, a secure data encryption and decryption system using cryptostego should provide robust encryption and steganography capabilities, while also providing user-friendly features thatallow for easy and secure data management

.

**5.** **Other** **Nonfunctional** **Requirements** **PerformanceRequirements**

The performance requirements for a secure data encryption and decryption system using crypto-stego can vary depending on the specific use case and the size and complexity of the data being encrypted or decrypted. However, some general performance requirements that can be considered for such a systemare:

Speed: The system should be able to perform encryption and decryption operations quickly and efficiently,without causing any significantdelays or interruptions.

Scalability: The system should be able to handle increasing amounts of data and users without significant performance degradation.

Resource utilization: The system should use system resources such as memory and processing power efficiently and optimally, without causing excessive system load or slowdowns.

Throughput: The system should be able to process a high volume of data without significantperformance degradation.

Security: The system should ensure that encrypted data remains secure and cannot be easily hacked or compromised.

Accuracy: The system should ensure that the data is accurately encrypted and decrypted without any loss or corruption of data.

Availability: The system should be available for use at all times and should be able to handle unexpected system failures and outages.

To achieve these performance requirements, the system should be designed and optimized to handle the specific requirements of the use case, while using efficient algorithms and optimization techniques to minimize processing time and resource utilization.Additionally,the system should be regularly tested and monitored to

ensure that it is meeting its performance requirements and that any issues are identified and resolved quickly.

**SafetyRequirements**

In addition to performance requirements, a secure data encryption and decryption system using crypto-stego should also have safety requirements to ensure that it is reliable and secure to use. Some safety requirements that can be considered for such a systeminclude:

Data integrity: The system should ensure that the encrypted data remains intact and is not modified or corrupted during the encryption and decryption process.

Data availability:The systemshould ensure that encrypted data can be accessed and decrypted when needed, without any loss or corruption of data.

Data confidentiality: The system should ensure that encrypted data remains confidentialand is not accessed by unauthorized users.

User authentication: The system should require user authentication to ensure that only authorized users can access the system and perform encryption and decryption operations.

Error handling: The system should handle errors and exceptions gracefully to prevent data loss or corruption.

Backup and recovery: The system should provide backup and recovery mechanisms to ensure that data can be recoveredin the event of a system failure or dataloss.

Compliance with security standards: The system should comply with industry and government security standards to ensure that it is secure and reliable.

Toachieve these safety requirements, the system should be designed and tested to ensure that it can handle unexpected events and errors, and that it provides the necessary security features to preventdata loss, corruption, or unauthorized access. Additionally, the system should be regularly monitored and audited to ensure that it is meeting its safety requirements and that any issues are identified and resolved quickly.

**SecurityRequirements**

A secure data encryption and decryption system using crypto-stego should have strong security requirements to ensure that the data remains secure and cannot be easily compromised. Some security requirements that can be considered for such a systeminclude:

Encryption strength: The encryption algorithm should be strong and resistant to known attacks and vulnerabilities.

Key management: The system should have strong key management procedures to ensure that keys are generated securely, stored securely, and are not shared with unauthorized users.

Access control: The system should have access control mechanisms to ensure that only authorized users can access the system and perform encryption and decryption operations.

Secure communication: The system should use secure communication protocols to prevent eavesdropping and data interception.

Audit trails: The system should provide audit trails to track system activity and identify any unauthorized access or suspicious activity.

Secure storage: The system should store encrypted data securely, to prevent unauthorized access or data theft.

Compliance with security standards: The system should comply with industry and government security standards to ensure that it is secure and reliable.

To achieve these security requirements, the system should be designed and implemented using strong encryption algorithms and protocols, with robust key management and access control mechanisms. Additionally, the system should be regularly tested and audited to ensure that it is meeting its security requirements and that any vulnerabilities are identified and resolved quickly. Finally, the system should be kept up to date with the latest security patches and updates to ensure that it remains secure againstnew and emerging threats.

**SoftwareQuality** **Attributes**

Software quality attributes are a set of characteristics that describe the overall quality of a software system. For secure data encryption and decryption using crypto-stego, some important softwarequality attributesinclude:

Security: The system should be designed to be secure, with strong encryption algorithms, keymanagement procedures, and access controls.

Reliability: The system should be reliable, with high availability and minimal downtime. It should also be able to recover from failures quickly and gracefully.

Maintainability: The system should be easy to maintain and update, with well-structured code, clear documentation, and easy-to-use interfaces.

Usability: The system should be easy to use, with a clear and intuitive user interface and minimal training required.

Performance: The system should be fast and responsive, with minimal lag or delay when encrypting or decrypting data.

Scalability: The system should be able to scale to handle larger volumes of data or increased usage, without sacrificing performance or security.

Portability: The system should be easily portable across different platforms and operating systems,with minimal changes required.

To ensure that the system meets these software quality attributes, it should be designed and developed using best practices in software engineering, including clear documentation, well-structured code, and thorough testing and debugging. Additionally, the system should be regularly monitored and audited to identify any performance or security issues and to ensure that it continues to meet its software quality attributesover time.

**Business** **Rules**

Business rules are a set of guidelines that dictate how a system should behave in different situations. For secure data encryption and decryption using crypto-stego, some important business rules may include:

Data classification: The system should follow a clear data classification scheme that identifies which data should be encrypted and at what level of encryption.

User access control: The system should enforce strict access control rules that limit access to encrypted data to authorized users only.

Key management: The system should have clear rules and procedures for managing encryption keys,including how keys are generated,stored, anddistributed.

Data retention: The system should have clear rules for how long encrypted data should be retained, and how it should be securely disposed of when it is no longer needed.

Compliance: The system should comply with any relevant legal or regulatory requirements related to data encryption and security, such as data protection laws or industry-specificsecurity standards.

Incident response: The system should have clear rules and procedures for responding to security incidents, including how to detect and respond to data breaches, and how to report incidents to relevant authorities.

Audit and monitoring: The system should have clear rules for auditing and monitoring data access and use, to identify any suspicious activity or unauthorized access.

These business rules should be clearly documented and communicated to all relevant stakeholders, including system administrators, users, and auditors. They should also be regularly reviewed and updated to ensure that they continue to reflect best practices and comply with any changes in regulations or industry standards.

**6.** **Other** **Requirements**

Requirements for secure data encryption and decryption using cryptostego may include:

Interoperability: The system should be able to interoperatewith other systemsthat use differentencryption and decryption methods.

Compliance with standards: The system should comply with industry standards and best practices forencryption and decryption, such as AES or RSA.

Customization: The system should be customizable to meet the specific needs and requirements of the organization using it.

Error handling: The system should have clear error handling procedures that detect and respond to errors, and prevent data loss or corruption.

Data integrity: The system should ensure the integrity of encrypted data, with mechanisms for detecting and preventing data tampering or corruption.

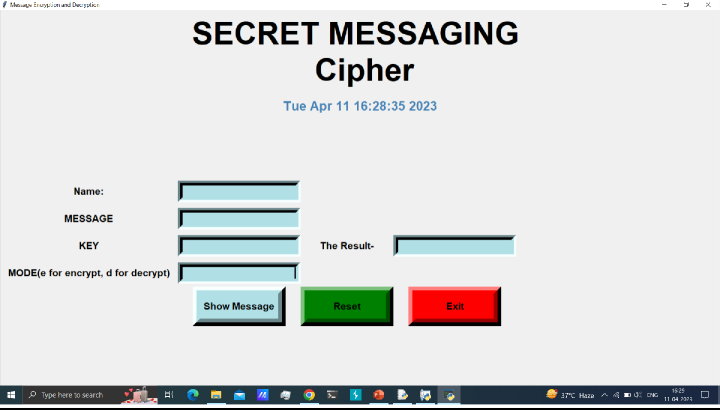
Performance optimization: The system should be optimized for performance, with minimal overhead on systemresources and fast encryption and decryption times.

Compatibility: The system should be compatible with a wide range of hardware and software configurations, without requiring significantmodifications orupgrades.

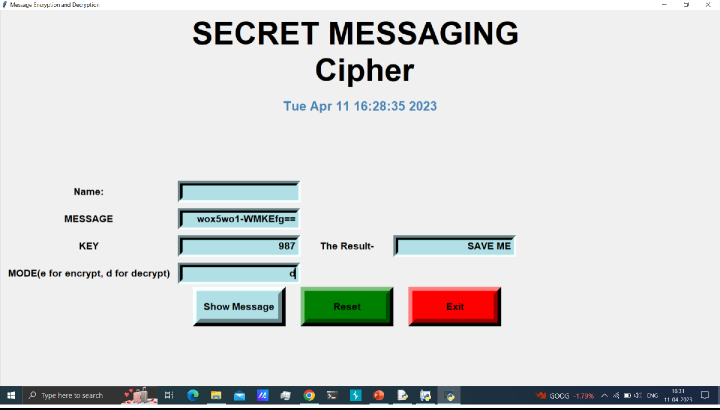
Scalability: The system should be scalable, able to handle large volumes of data or increased usage without sacrificing performance or security.

These requirements should be clearly documented and communicated to all relevant stakeholders, including system administrators, users, and developers. They should also be regularly reviewed and updated to ensure that they continue to reflect the evolving needs and requirements of the organization.

**Output**

**FIRSTINTERFACE**

**ENCODING**

**DECODING**

**Conclusion**

In the proposed crypto-stego system, we present a mechanism to provide secure transmission of data by multiple safety measures, firstly by applying encryption using Affine Transform and Discrete Cosine Transform (DCT) and then merging this encrypted data with an image, randomly chosen from a set of available images, and sendingtheimagesoobtainedtothereceiverattheotherendthroughthenetwork.

Overall, the purpose of secure data encryption and decryption using crypto steganography is to provide a high level of security and privacy for sensitive information.

**References**

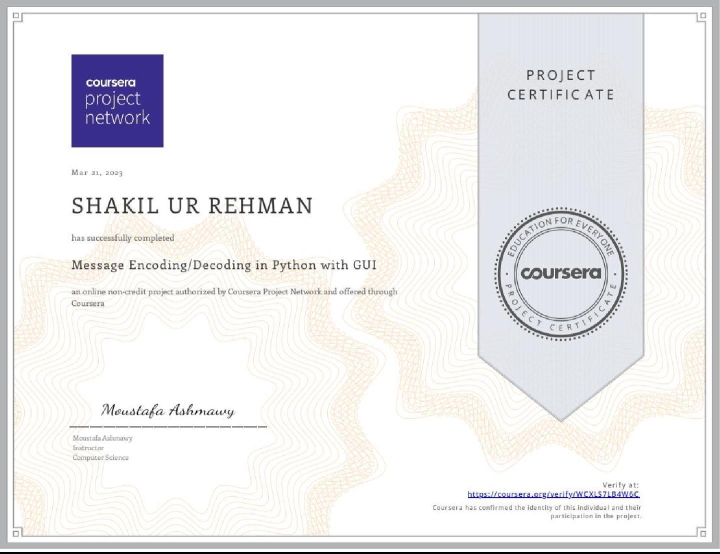
Here are some references formaking secure data encryption and decryption using crypto steganography:

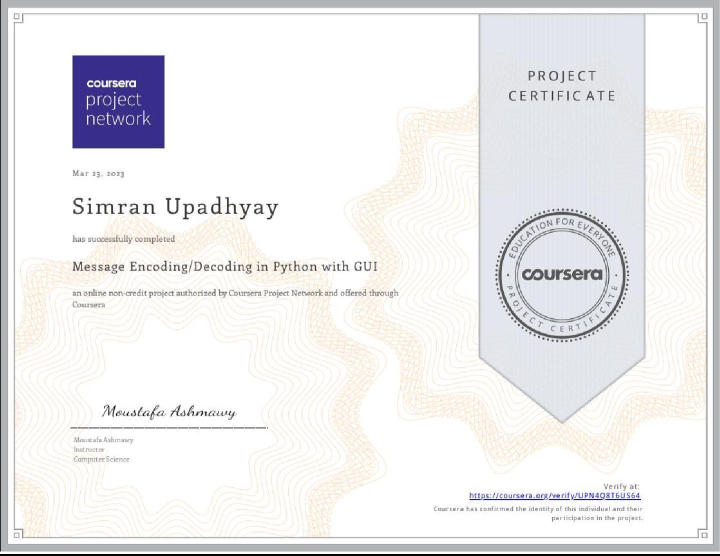
Johnson, N. F. (2014). Steganography:Using encryption to hide data.

Network Security,2014(4), 14-17. doi:10.1016/s1353-4858(14)70072-3 Huang, C. H., Chang, C. C., & Tsai,Y. C. (2019).

A SteganographyEncryption Method Based on AES and RSA for Hiding Text Messages. Symmetry,11(9), 1172. doi:10.3390/sym11091172

**Certification** **of** **guided** **project** **SANDEEPSOLANKI (2101330100200)**

**SHAKIL UR REHMAN (2101330100205)**

**SIMRAN UPADHYAY(2101330100222)**

Thank you!