DATA HIDING TECHNIQUES IN MULTIMEDIAL OBJECTS USING STEGANOGRAPHY

Project Reference No.: *47S_BE_4571*

College ***:*** *P.D.A. College of Engineering, Kalaburagi*
Branch ***:*** *Department of Computer Science and Engineering*
Guide(s) ***:*** *Dr. Sharanabadappa Gandage*
Student(S) ***:*** *Mr. Srivatsa*
Mr. Sanket S. Biradar
Mr. Shashank G. Sonth

Introduction:

Steganography, derived from the Greek words "steganos" (meaning covered or concealed) and "graphie" (meaning writing), is a fascinating and ancient practice that involves the art and science of concealing information within a seemingly innocuous carrier medium to ensure its secrecy. Unlike cryptography, which focuses on rendering the content of a message unreadable, steganography seeks to obfuscate the very existence of the message itself. This clandestine technique has been employed throughout history as a means of covert communication, with applications ranging from espionage and secure data transmission to digital watermarking and copyright protection.

The carrier medium, the vessel that conceals the hidden message, can take various forms, such as images (JPEG, PNG, BMP), audio files (MP3, WAV), or even text files. The hidden message, the information intended to be kept confidential, can be anything from plain text and files to images or other data. The challenge lies in embedding this information within the carrier without arousing suspicion.

The process of hiding the message within the carrier is known as embedding or encoding. Numerous steganographic algorithms and techniques have been developed to achieve this, each tailored to the characteristics of the carrier medium. For instance, in image steganography, a common technique involves the least significant bit (LSB) insertion, where the least significant bits of the pixel values are altered to encode the hidden information without significantly altering the visual appearance of the image.

Audio steganography, on the other hand, may utilize frequency domain manipulation or spread spectrum techniques to embed data within the audio signal. Video steganography often involves manipulating individual frames or embedding data within the video stream without perceptible changes.

Steganography is the practice of concealing a message, file, image, or video within another medium in such a way that it is difficult to detect or decipher. Unlike cryptography, which focuses on making the content of a message unreadable, steganography aims to hide the existence of the message itself.

Here are some key concepts and techniques in steganography:

1. Carrier Medium: This is the file or data that contains the hidden message. Common carrier media include images (JPEG, PNG, BMP), audio files (MP3, WAV), videos, and even text files.
2. Hidden Message: This is the information that the sender wants to conceal. It could be text, another image, a file, or any other data.
3. Embedding: The process of hiding the message within the carrier is known as embedding or encoding. Various techniques can be employed for this purpose, depending on the type of carrier.
4. Steganographic Algorithms:These are the methods and algorithms used to embed and extract hidden messages. Different algorithms suit different types of carriers. Some common techniques include LSB (Least Significant Bit) insertion in images, frequency domain manipulation in audio, and frame manipulation in videos.
5. Steganalysis: This is the study of methods to detect the presence of hidden messages. Steganalysis techniques aim to reveal the existence of concealed information and are often employed by security professionals to identify potential threats.
6. Security and Applications: Steganography is used for various purposes, ranging from secure communication and data hiding to digital watermarking and copyright protection. It has applications in fields such as information security, law enforcement, and digital forensics.

It's important to note that while steganography can be used for legitimate and ethical purposes, it can also be employed for malicious activities, such as hiding malware or facilitating covert communication in cyberattacks. As a result, understanding both steganography and steganalysis is crucial for those involved in information security and digital forensics.

1.1 Domain Introduction

In the cybersecurity domain, steganography plays a crucial role in enhancing security and privacy through various applications. Here are some key points highlighting the importance of steganography in cybersecurity:

1.Covert Communication: Steganography enables covert communication by hiding information within seemingly innocuous files or communication channels. This can be valuable in situations where maintaining the secrecy of communication is essential, such as in military or intelligence operations.

2.Data Concealment:Cyber attackers often attempt to hide malicious code, malware, or sensitive information within files to evade detection. Steganography provides a means to conceal such data, making it challenging for security systems to identify and block malicious activities.

3.Evasion of Detection:Steganographic techniques make it difficult for security tools and algorithms to detect the presence of hidden information. This evasion of detection can be advantageous for both offensive and defensive cybersecurity strategies.

4.Cryptography Complement:Steganography can complement cryptographic methods by adding an extra layer of concealment. While cryptography focuses on securing the content of messages, steganography addresses the issue of hiding the existence of the communication itself.

5.Digital Watermarking:In the context of cybersecurity and intellectual property protection, steganography is employed for digital watermarking. Watermarks are embedded within digital assets, such as images or videos, to prove ownership or authenticate the source, aiding in the prevention of unauthorized use or distribution.

6.Secure Communication Channels:Steganography can be utilized to establish secure communication channels where the fact that communication is occurring is hidden.

7.Forensic Analysis:On the defensive side of cybersecurity, steganography is critical for digital forensics. Security professionals use steganalysis techniques to detect and analyze hidden information in files, helping uncover potential security threats or incidents.

8.Preventing Data Alteration:Steganography can be used to embed digital signatures or checksums within files, ensuring their integrity. This helps in detecting any unauthorized alterations or tampering, adding a layer of protection against data manipulation.

It's important to note that while steganography has legitimate applications in cybersecurity, it can also be misused for malicious purposes. Security professionals need to be aware of steganographic techniques and employ steganalysis tools to identify and mitigate potential threats in cyberspace.

1.2 Project Implementation

The theoretical concept behind implementing a steganography project using Java, Swing library for GUI, and encoding/decoding algorithms involves a combination of graphical user interface design, image processing, and the application of steganographic techniques. Here's a breakdown of the theoretical concepts:

1. Steganography Basics: Encoding:In steganography, encoding is the process of hiding information within a carrier medium. This involves embedding the secret data into the carrier, such as an image, audio file, or text, in a way that is imperceptible to the human senses.Decoding: Decoding is the reverse process, extracting the hidden information from the carrier without altering the carrier's apparent properties.

2. Java Programming Language: Java is a versatile, platform-independent programming language. Its object-oriented nature and extensive standard libraries make it suitable for implementing various applications, including steganography projects. Swing is a GUI toolkit for Java that provides a set of components for building desktop applications. It includes components like buttons, text areas, and file choosers that are essential for creating a user-friendly interface.

3. Steganography Algorithms:Encoding Algorithm: The encoding algorithm is responsible for embedding the secret message into the carrier. It must ensure that the modification is subtle enough to avoid detection while allowing for reliable extraction later. Common techniques include LSB (Least Significant Bit) substitution in image pixels.Decoding Algorithm: The decoding algorithm reverses the encoding process, extracting the hidden information from the carrier. It should accurately identify and recover the hidden data without errors.

4. Graphical User Interface (GUI): A GUI provides an interactive interface for users to interact with the steganography application. It typically includes components such as text areas for inputting messages, buttons for triggering actions like encoding and decoding, and file choosers for selecting carrier files. The GUI design aims to make the steganography process user-friendly, guiding users through the steps of encoding and decoding.

5.File Handling:The application must handle file operations for loading and saving images. The Java Image I/O API can be used for reading and writing image files.

6.Event Handling Event handling mechanisms in Java, such as ActionListeners, are used to respond to user actions like button clicks. For example, when the user clicks the "Encode" button, the application should respond by initiating the encoding process.

7.Security Considerations: Security in steganography involves ensuring the confidentiality and integrity of hidden information. Password protection and encryption can be incorporated to enhance the security of the hidden data.

Understanding these theoretical concepts provides a foundation for designing and implementing a steganography project using Java and Swing. The practical implementation involves translating these concepts into code, integrating steganographic algorithms with GUI components, and ensuring a robust and user-friendly application.

Literature Survey:

[1] The research paper titled “Image steganography” :A review of the advances”.The paper discusses about the Steganography can be defined as the process of hiding a secret small multimedia data inside another but much larger multimedia data such as image, text, file or video . Image steganography is a technique to hide an image inside another image. In image steganography, the cover image is manipulated in such a way that the hidden data is not visible thus making it not suspicious as in the case of cryptography. Inversely, Steganalysis is used to detect the presence of any secret message covered in the image

and to extract the hidden data . Steganalysis helps in classifying if the image is either a stego image or a normal image. Apart from classifying the image, further investigation is carried out to detect the location and the content of the secret image inside the cover image.

[2] The research paper titled “A Study and literature Review on Image Steganography .The paper discusses about the In the year of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier transform (FrFT), Investigated on as a generalization of the classical Fourier transform, introduced years ago in mathematics literature. The enhanced computation of fractional Fourier transform, the discrete version of FrFT came into existence DFrFT. This study of illustrates the advantage of discrete fractional Fourier transform (DFrFT) as compared to other transforms for steganography in image processing. The result shows same PSNR in both domain (time and frequency) but implemented a variation of plain LSB (Least Significant Bit) algorithm. The stego-image quality has been improved by using bit-inversion technique. LSB method improving the PSNR of stegoimage. Through storing the bit patterns for which LSBs are inverted, image may be obtained correctly. For the improving the robustness of steganography, RC4 algorithm had been implemented to achieve the randomization in hiding message image bits into cover image pixels instead of storing them sequentially. This method randomly disperses the bits of the message in the cover image and thus, harder for unauthorized people to extract the original message. The presented method shows good enhancement to Least Significant Bit technique in consideration to security as well as image quality DFrFT gives an advantage of additional stego key. The order parameter of this transform.

[3]The research paper titled “A Survey on Text Based Steganography”. the paper discusses about Text steganography [2,3,8], which is what this paper specifically deals with, uses text as the medium in which to hide information. It is the most difficult kind of steganography; this is due largely to the relative lack of redundant information in a text file as compared with a picture or a sound file. The structure of text documents is identical with what we observe, while in other types of documents such as in picture, the structure of document is different from what we observe. Therefore, in such documents, we can hide information by introducing changes in the structure of the document without making a notable change in the concerned output. Contrary to other media such as pictures, sounds and video clips, using text documents has been common since very old times. Even after invention of printing machine, most of the books and documents have contained only texts. This has extended until today and still, using text is preferred over other media, because the texts occupy lesser memory, communicate more information and need less cost for printing as well as some other advantages.

[4]The research paper titled “A Review on Text Steganography Techniques”. the paper discusses about A text steganography technique based on text format was suggests. This method enhances hidden data storage using the justified formatted text contained inside PDF documents. This process initially uses Huffman coding (HC) to process the message. Next, specific lines from the cover text are designated as host lines. The embedding process comprises the spaces contained in the host lines to replace the inserted spaces. This process uses a key for enhancing communication security. This technique hides more

information inside cover text compared with other techniques. Additionally, the cover file size remains the same, thereby suspicion from being raised. Moreover, because text originality is preserved, there is no chance of syntactical or grammatical errors.

[5] The research paper titled “Digital audio steganography” : Systematic review, classification, and analysis of the current state of the art”. The paper discusses To understand the reviewed methods in this paper and the reasons behind such a level of diversity, discussing the three main requirements of audio steganography and existing trade-offs is vital. The performance improvement in each audio steganography method remains connected to approximately one of the three main requirements, namely, capacity, perceptual transparency, and robustness. Capacity is related to a message size that can be embedded in an audio second or represented as the percentage. Audio steganography is the process of hiding a message inside an audio cover file. In this paper, a review has been conducted on the methods of audio steganography. The methods have been collected in a systematic manner on five major digital databases using a unified query. The proposed review aims to shed light on the ideas and methods proposed in audio steganography. Existing reviews suffer from the high overlapping level or low level of segregation among the methods due to poor.

[6]The research paper titled “E. Arun Pravin1*, S. Navaneethan2, K. Karthick Raja3, S. Ponni41,2,3,4Departmentof Information Technology, Dr .Mahalingam College of Engineering and Technology, Pollachi, India”. The paper discusses In this paper we have presented a strong strategy for indistinct sound information stowing away. Along these lines we reason that sound information concealing method scan be utilized for various purposes other than incognito correspondence or deniable information stockpiling, data following and finger printing, alter recognition.

Existing System:

Huge data is available is in the media such as text, image, audio and video in the several formats such as JPEG and MPEG. Several stega components are used to provide the various functions .such as the stegahide, open stego, Audacity, camoflage ,S-tools. Every media has there own data hiding technique which evaluates the form of data.

Stegahide- Steghide is a powerful open-source steganography tool known for its ability to conceal data within various file types, including images and audio files. Operating through a command-line interface, Steghide provides a versatile solution for users on different platforms, such as Linux, Windows, and macOS. One of its standout features is its support for a range of file formats, including JPEG, BMP, WAV, and AU, making it adaptable for various carrier media. The tool places a strong emphasis on security by offering encryption capabilities, allowing users to safeguard the hidden data with robust algorithms. Additionally, Steghide incorporates passphrase protection during both the embedding and extraction processes, enhancing the overall security posture of the concealed information.

OpenStego- OpenStego is a user-friendly, open-source steganography tool known for its intuitive graphical user interface (GUI) designed to hide data within digital media files. Operating seamlessly on various platforms including Windows, Linux, and macOS,

OpenStego offers a versatile solution for users seeking to conceal information in different media types. The tool supports a range of carrier file formats such as JPEG, BMP, WAV, and AU, providing flexibility in choosing the most suitable medium for steganographic purposes. OpenStego incorporates encryption options to enhance the security of the concealed information, allowing users to specify passwords for added protection. With multiple steganographic algorithms at its disposal, OpenStego caters to different user requirements and scenarios.

Audacity- Audacity is a widely-used and versatile open-source audio editing and recording software available for Windows, macOS, and Linux. Renowned for its user-friendly interface, Audacity offers a range of powerful features suitable for both amateur and professional users in the audio editing and production realm. Users can perform various tasks, including recording live audio through a microphone, capturing streaming audio, and editing multiple tracks simultaneously.

One of Audacity's notable features is its comprehensive set of editing tools, allowing users to cut, copy, paste, and apply various effects to manipulate audio tracks. The software supports a diverse array of audio file formats, enabling users to import and export files in formats like WAV, MP3, FLAC, and OGG. This compatibility facilitates seamless integration with other software and devices.

While Audacity is known for its user-friendly design, it may have a learning curve for users new to audio editing, especially when exploring more advanced features. Regular updates and an active community contribute to Audacity's continued relevance and popularity in the realm of digital audio editing. Overall, Audacity remains a powerful, free, and accessible tool for audio enthusiasts and professionals alike.

S-tools I S-Tools, also known as "Steganography-Tools," was a software suite that included tools for digital steganography. Steganography is the practice of concealing messages or information within other non-secret data, such as images or audio files. S-Tools allowed users to hide text messages or files within digital images, making the hidden information inconspicuous and difficult to detect.

Key features of S-Tools included:

1. Image Steganography:

S-Tools primarily focused on hiding information within digital images. Users could embed text messages or files into the pixel data of images, and the changes made were often imperceptible to the human eye.

2. Password Protection

- The tool provided password protection for the concealed data, adding an additional layer of security to prevent unauthorized access.

3. Multiple File Format Support

S-Tools supported various image file formats, allowing users to choose the format that best suited their needs.

PROPOSED SYSTEM

1. Java Programming Language: Java is chosen for its built-in security libraries that provide tools and functions for encryption, decryption, and secure communication. These libraries offer a robust foundation for implementing secure systems.

2. Data Concealment: The system involves hiding the existence of data in various formats such as text, images, and audio. This likely involves techniques like steganography (hiding data within other data) or encryption to conceal sensitive information.

3. GUI Libraries - Swing and JavaFX: These are popular Java libraries used for creating graphical user interfaces (GUIs). They allow developers to create user-friendly interfaces for interacting with the system. Swing is older and more established, while JavaFX provides more modern features.

4. Encryption Algorithms:

Caesar Cipher: A simple substitution cipher where each letter in the plaintext is shifted a certain number of places down or up the alphabet.

LSB (Least Significant Bit) Steganography: A technique to hide information within the least significant bits of an image or other media files.

PBE (Password-Based Encryption) with MD5 and DES: PBE is a method that uses passwords to generate encryption keys. MD5 (Message Digest Algorithm 5) and DES (Data Encryption Standard) are cryptographic algorithms used in this context.

5. Protocols:

ZWC: Not a widely recognized protocol. It might refer to Zero Width Characters, which can be used for steganography or data hiding.

RTF (Rich Text Format): A document file format used for cross-platform document interchange.

LSB (Least Significant Bit): As mentioned earlier, this might refer to the steganography technique.

Phase Coding: Often associated with signal processing or encoding techniques used in communication systems.

6. Advantages:

Free Accessibility: Java is an open-source language, and many of its libraries and tools are freely accessible.

Software Orientation: The system seems focused on software-based security measures and functionalities.

Large Amount of Storage Capacity: This implies the system can handle and secure significant volumes of data.

This system aims to leverage these tools and techniques to create a secure and functional software system with robust encryption, GUI interaction, and hidden data capabilities.

CHAPTER V

DESIGN AND IMPLEMENTATION OF TEXT STEGANOGRAPHY

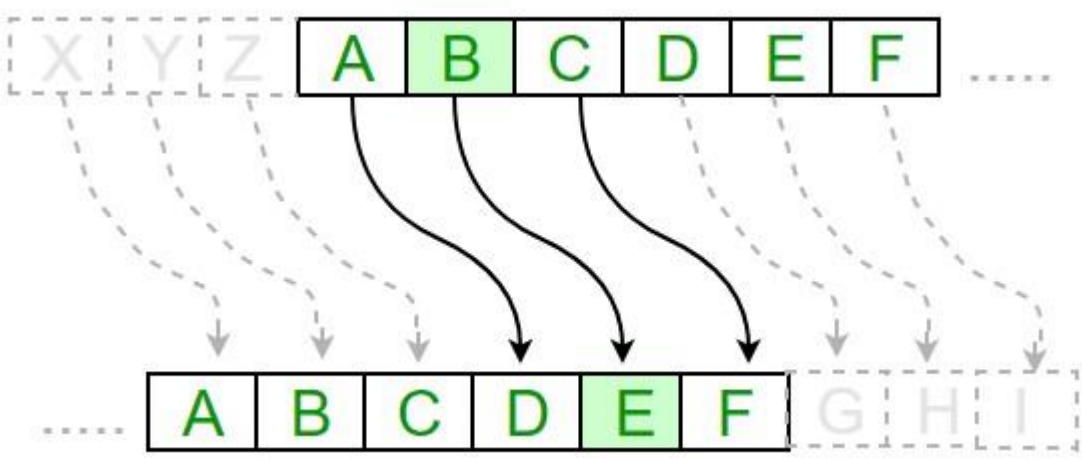

Fig 5.1: Diagrammatic Representation of Caesar Cipher Algorithm

The Caesar cipher is a simple encryption technique that was used by Julius Caesar to send secret messages to his allies. It works by shifting the letters in the plaintext message by a certain number of positions, known as the “shift” or “key”.

The Caesar Cipher technique is one of the earliest and simplest methods of encryption technique. It’s simply a type of substitution cipher, i.e., each letter of a given text is replaced by a letter with a fixed number of positions down the alphabet. For example with a shift of 1, A would be replaced by B, B would become C, and so on. The method is apparently named after Julius Caesar, who apparently used it to communicate with his officials.

Thus to cipher a given text we need an integer value, known as a shift which indicates the number of positions each letter of the text has been moved down.

The encryption can be represented using modular arithmetic by first transforming the letters into numbers, according to the scheme, A = 0, B = 1,…, Z = 25. Encryption of a letter by a shift n can be described mathematically as.

For example, if the shift is 3, then the letter A would be replaced by the letter D, B would become E, C would become F, and so on. The alphabet is wrapped around so that after Z, it starts back at A.

Here is an example of how to use the Caesar cipher to encrypt the message “HELLO” with a shift of 3:

1. Write down the plaintext message: HELLO
2. Choose a shift value. In this case, we will use a shift of 3.
3. Replace each letter in the plaintext message with the letter that is three positions to the right in the alphabet.

H becomes K (shift 3 from H)

E becomes H (shift 3 from E)

L becomes O (shift 3 from L)

L becomes O (shift 3 from L)

4. The encrypted message is now “KHOOR”.

To decrypt the message, you simply need to shift each letter back by the same number of positions. In this case, you would shift each letter in “KHOOR” back by 3 positions to get the original message, “HELLO”.

Results And Discussion:

Step 01: Login in to the interface by user credentials.

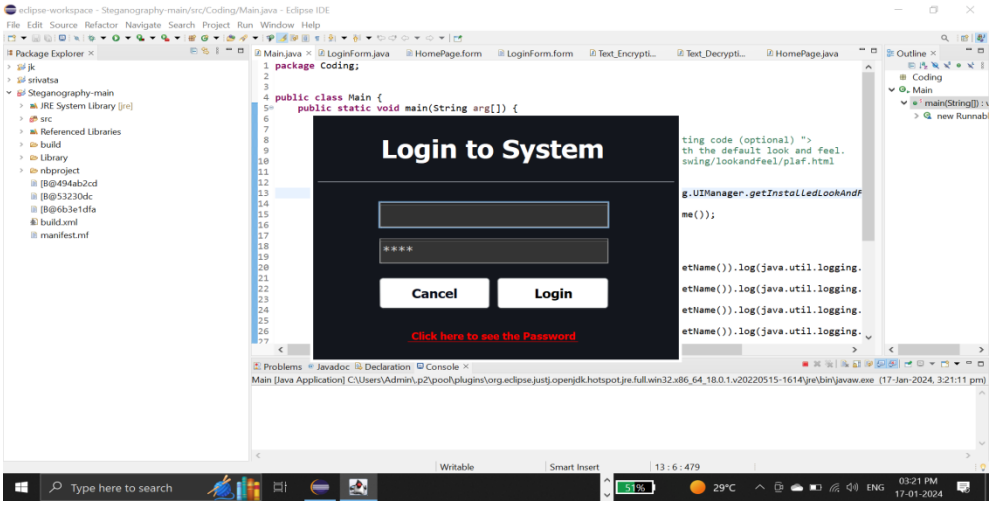

Fig 6.1 login page of the text steganography

Step 02: Entering credentials as username “PDA” and password “123”.

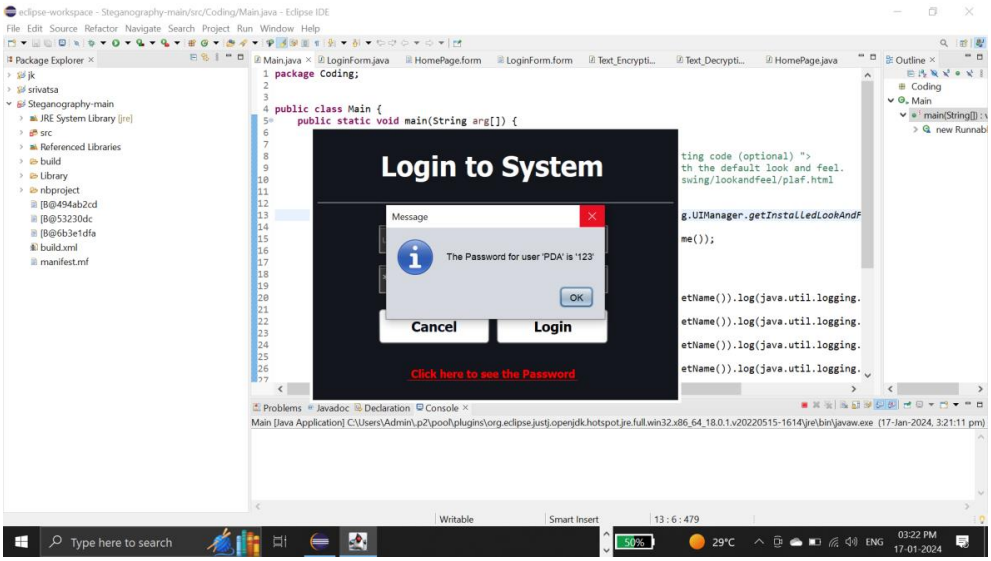

Fig 6.2 User Credentials of the System

Step 03: Visiting the GUI of the Steganographic project. Through the Message Incryption.

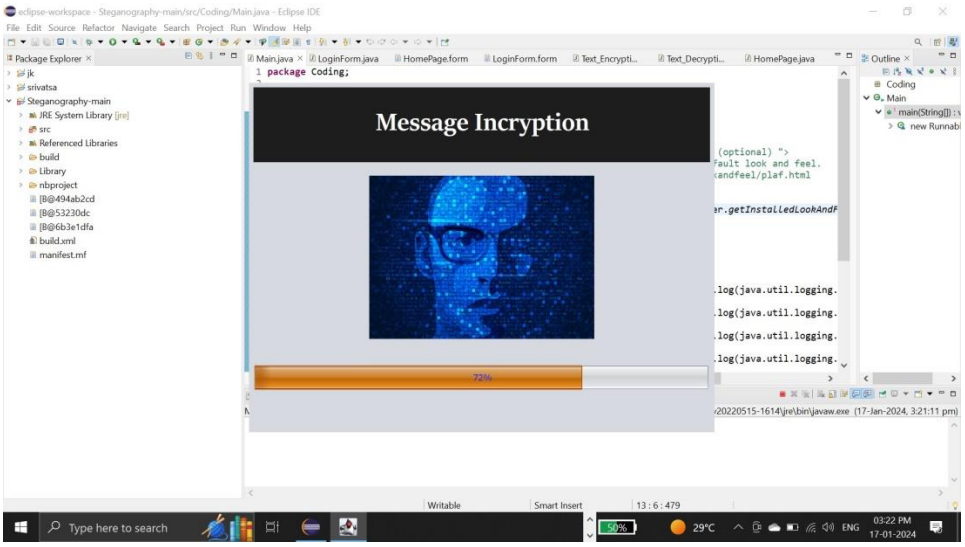

Fig 6.3 Message Incryption Interface

Step 04: Medial Interface of the Steganography

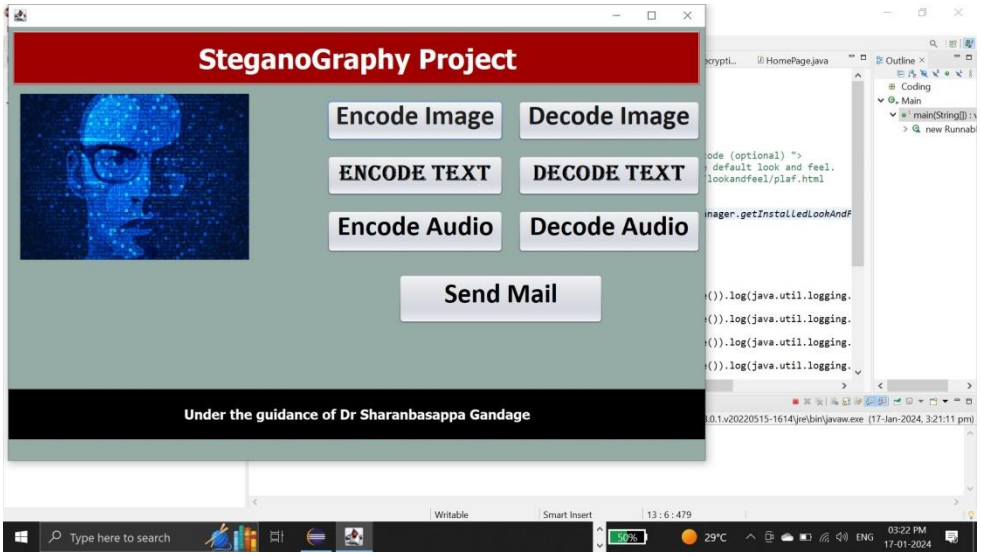

Fig 6.4 Medial Interface of Steganography

Step 05:Text Encoding with the key value.

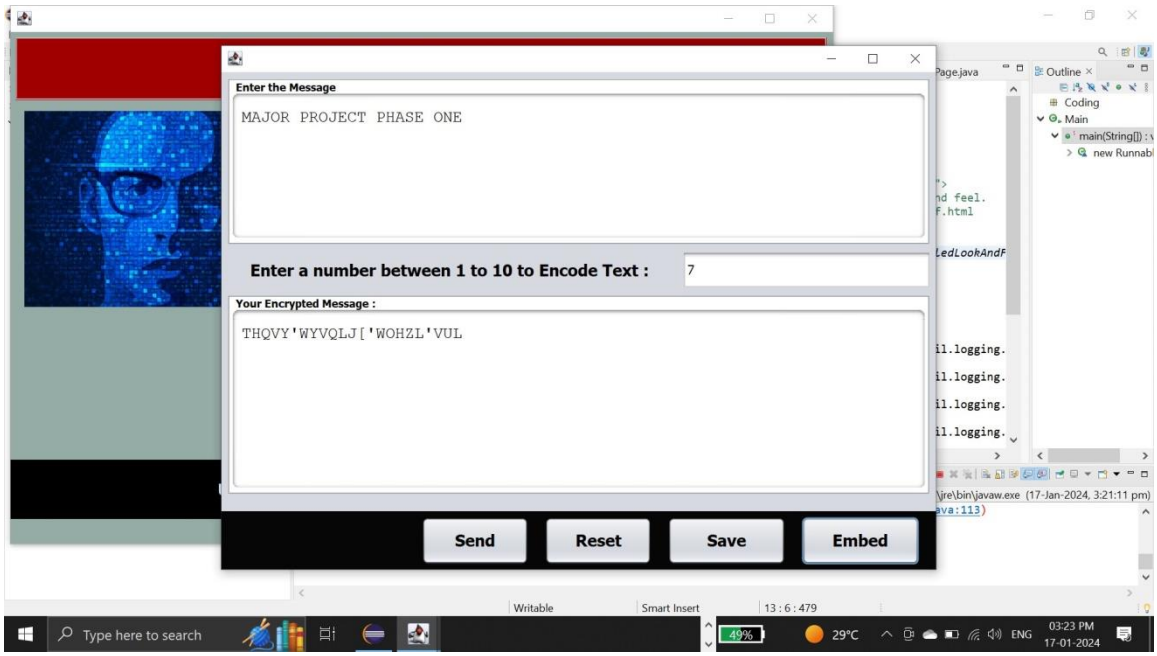

Fig 6.5 Diagrammatic Representation of Text Encoding with the key value.

Step 06: Text Decoding and returning the key value to get the original text.

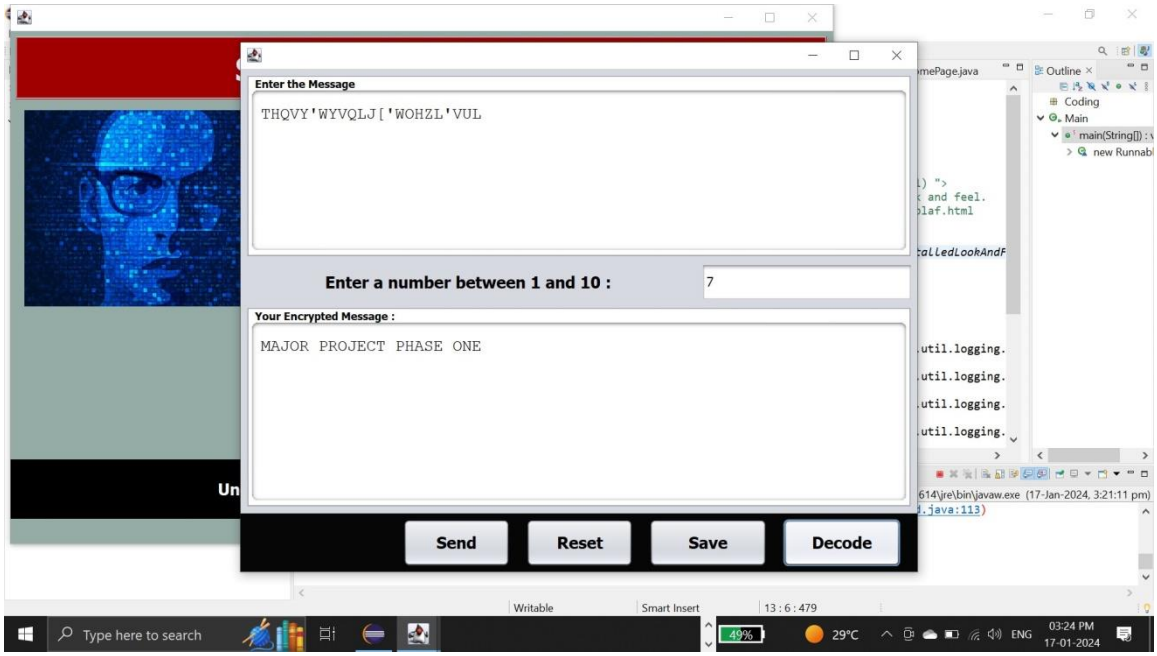

Fig 6.6 Diagrammatic Representation of Text Decoding with the Returning the key value to get the original text.

Conclusion:

Steganography serves as a powerful tool in the realm of cybersecurity and information protection. Its ability to conceal information within seemingly innocuous carriers has practical applications in secure communication, media file protection, and network security. As technology continues to advance, the future of steganography may witness more sophisticated techniques and integrations, potentially finding roles in IoT security, biometrics, blockchain, and quantum computing. However, it is essential to approach the use of steganography with a balanced perspective, recognizing its potential for both legitimate and malicious purposes. Striking a careful balance between privacy and security considerations will be crucial in harnessing the benefits of steganography responsibly.

Future Implementations:

1. Advanced Techniques:As computing power and algorithms advance, steganography methods will likely become more sophisticated, making detection even more challenging.Integration with artificial intelligence (AI) may lead to the development of smarter steganographic tools that can adapt to different detection mechanisms.

2. IoT Security:With the increasing adoption of Internet of Things (IoT) devices, steganography may find applications in securing communication between these devices, ensuring data privacy and integrity.

3. Biometric Security: Steganography might be applied in biometric security, hiding sensitive biometric data within images or other media for secure authentication purposes.

4.BlockchainandSteganography:Exploring the combination of steganography with blockchain technology to enhance privacy in transactions by hiding transaction details.

5.Quantum Steganography:Investigating how quantum computing may impact steganography, potentially leading to the development of quantum-resistant steganographic techniques.

6. Augmented Reality (AR) Security: As AR technologies become more prevalent, steganography may play a role in securing augmented reality content and interactions.

While steganography offers various technological applications today, its future implementations will likely evolve in response to advancements in computing, communication technologies, and emerging security challenges. As with any technology, the ethical use of steganography will be crucial to balance privacy and security concerns.

References:

[1] The research paper titled “Image steganography :A review of theadvances”. The paper discusses about the Steganography can be defined as the process of hiding secret small multimedia data inside another but much larger multimedia data such as image, text, file or video.

[2] The research paper titled “A Study and literature Review on Image Steganography. The paper discusses about the In the year of 2013 Soni, A.; Jain, J.; Roshan, R.

[3] The research paper titled “A Survey on Text Based Steganography”. the paper discusses about Text steganography [2,3,8], which is what this paper specifically deals with, uses text as the medium in which to hide information.

[4] The research paper titled “A Review on Text Steganography Techniques”. the paper discusses about A text steganography technique based on text format was suggests. This method enhances hidden data storage using the justified formatted text contained inside PDF documents.

[5] The research paper titled “Digital audio steganography”: Systematic review, classification, and analysis of the current state of the art”.

[6] The research paper titled “E. Arun Pravin1*, S. Navaneethan2, K. Karthick Raja3, S. Ponni41,2,3,4 Departmentof Information Technology, Dr .Mahalingam College of Engineering and Technology, Pollachi, India” on “Implementation of Text Steganography”.