STEGMED

A PROJECT REPORT

Submitted by

VANI SETH (201B299)

TANISH KHANDELWAL (201B283)

SHREYASH SHUKLA (201B259)

Under the guidance of **Dr. RAVINDRA KUMAR SINGH**

Submitted in partial fulfilment of the degree

Of

Bachelor Of Technology

In

COMPUTER SCIENCE AND ENGINEERING

at

JAYPEE UNIVERSITY OF ENGINEERING AND TECHNOLOGY GUNA,

MADHYA PRADESH (INDIA) – 473226

May-2022

DECLARATION

We hereby declare that the project entitled "**STEGMED**" was submitted for the B.Tech. (CSE) the degree is our original work and the project has not formed the basis for the award of any other degree, diploma, fellowship, or any other similar titles.

VANI SETH (201B299)

TANISH KHANDELWAL (201B283)

SHREYASH SHUKLA (201B259)

Signature of the Students

Place: JUET GUNA

Date:

CERTIFICATE

I certify the project entitled, "**STEGMED**" submitted by **VANI SETH (201B299), TANISH KHANDELWAL (201B283), and SHREYASH SHUKLA (201B259)** in partial fulfilment of the Degree of Bachelor of Technology in Computer Science and Engineering at the Department of Computer Science and Engineering, Jaypee University of Engineering and Technology is a work under my supervision. To the best of my knowledge and belief, there is no infringement of copyright and intellectual property rights. Also, this work has not been submitted partially or wholly to any other Institute or University for the award of any other degree or diploma. In case of any violation concern, students will solely be responsible.

SUPERVISOR

Dr. RAVINDRA KUMAR SINGH

ACKNOWLEDGEMENT

Any endeavour cannot lead to success unless and until a proper platform is provided for the same. This is the reason why; we find ourselves very fortunate to complete our work on a minor project under supervision of **Dr. RAVINDRA KUMAR SINGH.** Our sincere gratitude to him, for having faith in us and thus allowing us to carry out a project on technology completely new to us, for which we had to research and learn many new things, which will help us deal with advanced work in future. He helped immensely by guiding us throughout the project in any of the possible ways he could. Last but not the least, we would like to thank the Dept. Of Computer Science and Engineering who created this opportunity.

VANI SETH (201B299)

TANISH KHANDELWAL (201B283)

SHREYASH SHUKLA (201B259)

ABSTRACT

The increasing use of electronic health records (EHRs) has led to a growing concern about the security of sensitive medical information. Steganography and cryptography are two complementary technologies that can be used to improve the security of EHRs. Steganography is the art of hiding data within another piece of data, while cryptography is the art of transforming data into an unreadable form. By combining steganography and cryptography, it is possible to create a secure system for transferring sensitive medical documents.

Keywords: Steganography, Cryptography, Watermarking, Encryption

TABLE OF FIGURES

Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Problem Definition

The security of sensitive medical data is becoming a bigger problem as electronic health records (EHRs) [1] are used more frequently. Patient names, residences, dates of birth, Social Security numbers, medical histories, and treatment plans are just a few of the personal and medical data that may be found in EHRs. Although it is sensitive and could be exploited for identity theft, fraud, or other crimes, this information is valuable to both patients and healthcare professionals. The absence of a safe means for transferring delicate medical documents is the issue that this project will try to solve. The current systems are either too complex for patients and healthcare professionals to use, or they are not secure enough. Two complementary technologies, steganography, and cryptography [2], can be utilised to increase the security of EHRs. While cryptography is the discipline of converting data into an unreadable form, steganography is the art of concealing data within another piece of data. Steganography and cryptography can be used together to build a secure system for sending delicate medical documents. This project will develop a system that is both secure and easy to use, and it will be evaluated using a variety of security tests.

1.2 Project Overview

The project "StegMed" mainly focuses on:

1. Taking medical images from the user.
2. Hiding them into another image using LSB Steganography
3. Encrypting the resultant image with AES Cryptography along with Discrete Cosine Transformation (watermarking).
4. Sending the image to the receiver.
5. Decrypting and extracting the original image.

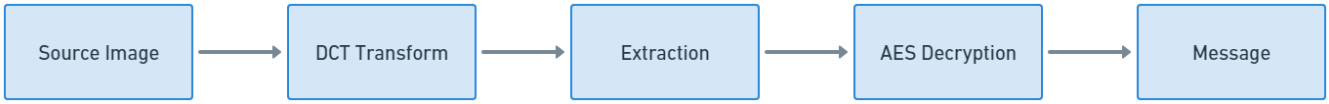

Figure 1. Block Diagram of General Framework

Figure 1 represents a block diagram that showcases the flow of how the project proceeds.

CHAPTER-2

LITERARTURE SURVEY

2.1 RELATED WORKS

2.1.1 Steganography

Steganography [3] is the art of hiding information in a cover medium in such a way that the presence of the information is unknown. Steganography focuses on concealing the existence of the message itself. The primary goal of steganography is to ensure that the embedded message remains undetectable to unintended recipients. This is achieved by subtly modifying the cover media in such a way that the alterations are imperceptible to the human eye or ear, yet the hidden message can be extracted by the intended recipient using a decoding process. One of the most common types of steganography is image steganography, where information is concealed within the pixels of an image. The cover image acts as a carrier for the hidden message, and the bits of the message are embedded in the least significant bits of the pixel values. This technique takes advantage of the fact that small changes in pixel values are often imperceptible to the human eye. Steganography has found applications in various domains, including digital forensics, covert communication, and data security [4]. Moreover, steganography can be combined with encryption to provide an additional layer of security. By encrypting the hidden message before embedding it within the cover media, even if the steganography technique is discovered, the encrypted message remains secure and unintelligible without the decryption key.

2.1.2 Cryptography

Cryptography [5] is the practice of securing information by converting it into an unreadable format, known as ciphertext, using mathematical algorithms and keys. It involves the use of mathematical algorithms and protocols to convert readable information, or plaintext, into a form that is unintelligible to unauthorized individuals, called ciphertext. Cryptography has been used for centuries to protect sensitive information, such as military intelligence and

diplomatic correspondences. With the growth of the internet and the increasing reliance on digital communication, cryptography has become a critical aspect of modern information security, with applications [6] ranging from online banking and e-commerce to secure messaging and data storage. The primary goals of cryptography are to ensure confidentiality, integrity, and authentication of data, thereby preserving the privacy and trust of individuals and organizations in the digital age. Cryptography involves two fundamental processes: encryption and decryption. Encryption involves converting plaintext (original data) into ciphertext using an encryption algorithm and a secret key, making it unintelligible to unauthorized individuals. Decryption, on the other hand, is the reverse process of converting the ciphertext back into plaintext using a decryption algorithm and the correct key.

2.1.3 Application of Steganography and Cryptography in Medicine

Steganography and cryptography play significant roles in the field of medicine, ensuring the security and privacy of sensitive medical data and enhancing communication between healthcare professionals. Steganography, the art of hiding information within other data, finds applications in medical imaging [7]. With the increasing use of digital medical images, steganography techniques can be employed to embed additional patient information or annotations within the images themselves. This hidden data can include patient demographics, medical history, treatment plans, or even watermarking for copyright protection. By concealing the information within the image, steganography ensures that it remains intact and easily accessible, while maintaining the confidentiality of the data. Cryptography, on the other hand, is widely used to protect the privacy and integrity of medical records and communications. Encryption algorithms and cryptographic protocols are employed to secure sensitive patient information, such as electronic health records (EHRs), medical test results, and personal identification data. By encrypting this data, it becomes unreadable and can only be accessed by authorized individuals with the appropriate decryption keys. Cryptography also helps in authenticating the integrity of medical records, ensuring that they have not been tampered with during storage or transmission. In telemedicine and remote healthcare services, steganography and cryptography play a crucial role in securing communication channels. Patient-doctor consultations, transmission of medical images, and exchange of confidential information are protected through encryption

techniques. This ensures that the privacy of patient data is maintained, and only authorized parties can access and interpret the transmitted information [8].

2.1.4 Watermarking

Watermarking is a technique used to embed hidden information or markings within digital media, such as images, videos, or audio files. These hidden markings, known as watermarks, are designed to be imperceptible to the human eye or ear but can be detected and extracted using specialized algorithms. The primary purpose of watermarking is to protect intellectual property rights and provide proof of ownership or authenticity [9]. Watermarks can be used for various applications, including copyright protection, content identification, tamper detection, and digital forensics. Watermarking techniques can be categorized into two main types: spatial domain and frequency domain. Spatial domain watermarking modifies the pixel values directly within the image or audio data, embedding the watermark in the spatial domain. Frequency domain watermarking, on the other hand, applies transformations, such as the Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT), to convert the data into the frequency domain. The watermark is then embedded in the transformed domain. Watermarking techniques often take advantage of the frequency domain properties provided by the DCT. In the context of watermarking, the DCT coefficients of an image can be modified to embed a watermark without significantly altering the perceptual quality of the image [10]. The watermark is typically embedded by modifying a subset of DCT coefficients, which are chosen carefully to minimize visibility and maintain robustness against various attacks.

CHAPTER-3

SYSTEM ANALYSIS AND DESIGN

3.1 SYSTEM REQUIREMENT

The process of deciding on the requirements of a software system, which determines the responsibilities of a system, is called requirement analysis. Requirement analysis is a software engineering task that bridges the gap between system level requirements engineering and software design. Requirement reengineering activities result in the specification of software's operational characteristics indicate the software's interface with other system elements and establish constraints that the software must meet.

The following section presents the detailed requirement analysis of our project.

3.1.1 HARDWARE REQUIREMENTS:

- CPU (3.0 GHz or faster) or faster 64-bit Dual Core processor like Intel core-2 duo.
- Memory: 4GB (DDR4 | DDR2) RAM or more
- GPU: 2GB dedicated GPU or Intel IrisXe integrated
- Storage: 256 GB SSD or higher
- Internet Connection: Broadband or high-speed internet

3.1.2 SOFTWARE REQUIREMENT:

- Operating System: Windows 8, 10, 11 or maxOS Mojave (or later version)
- Development Tools: Python 3.7 or high, Google Colab, Visual Studio Code
- Additional Libraries and dependencies: Pandas, Numpy, Opencv, Pillow, Pycryptodome, Tkinter, CryptoCipher

3.2 SYSTEM ARCHITECTURE

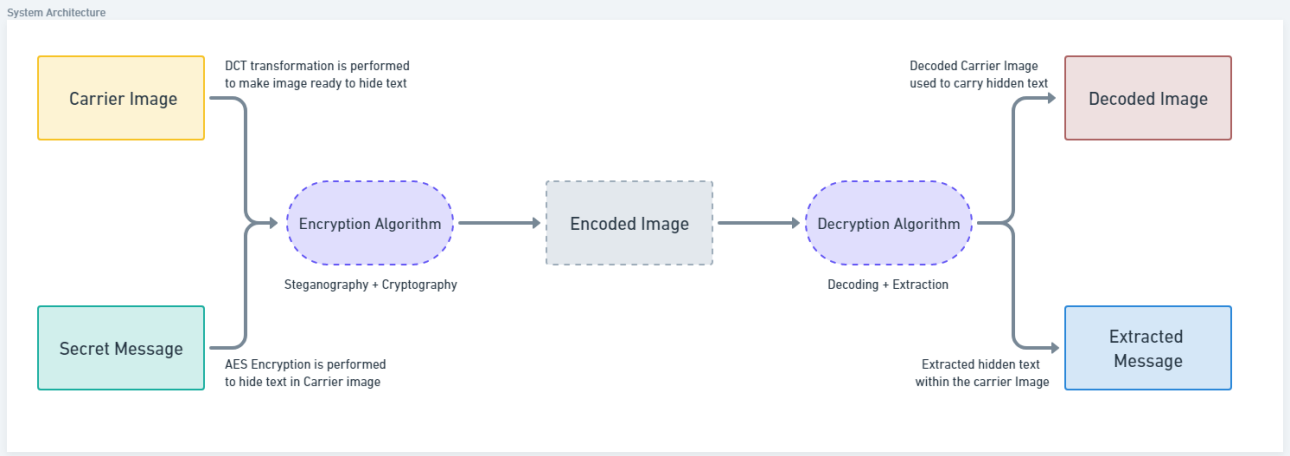

Figure 2. System Architecture

Figure 2 describes the system architecture of the whole project. It represents how at the sender's end; carrier image is encrypted with a secret message. The carrier image first goes through a watermarking technique called DCT transformation, then the image is encrypted using a symmetric encryption algorithm to maintain the security of the transmission. Similarly, at the receiver's end a decryption algorithm runs which does the decoding of the image along with the extraction of message. Finally, we get the decoded image and the secret text as the output.

The above System Architecture makes sure that the carrier image after suitable transformations and preparation to be embedded with the secret text is passed through channels and encryption algorithm to successfully hide the sensitive information within the Image which in our use case will be a medical image of any individual. Once the encoded image is received at the receiver end, a decryption algorithm based on the similar encryption method is performed on the image to extract the hidden secret message within the image. It is done so that we obtain a decoded image which will closely resemble the original carrier image and extracted secret text which was meant to be transmitted without the fear of being leaked or any kind of data security issue. Moreover, the watermarking technique makes sure that the received image is provided by an authenticated source and not tampered throughout its way course through the channel. The various architecture of Steganography, Cryptography and Watermarking are further explained in detail.

3.2.1 Steganography Architecture

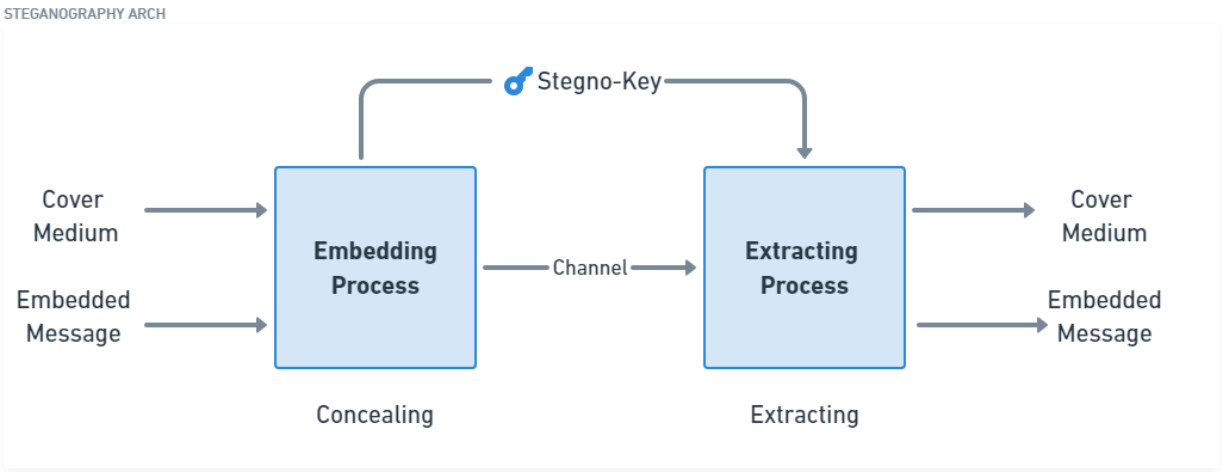

Figure 3. Steganography Architecture

Figure 3 describes the architecture of the steganography process. It involves the use of the embedding process which utilizes a stegno-key to hide a message into a cover medium which in this case is an image. The resultant image is then sent via a channel to the receiver. Here the process of extraction occurs. After the successful completion of the extracting process the original message and the cover image is separated to reveal the original message being sent by the user.

3.2.2 Cryptography Architecture

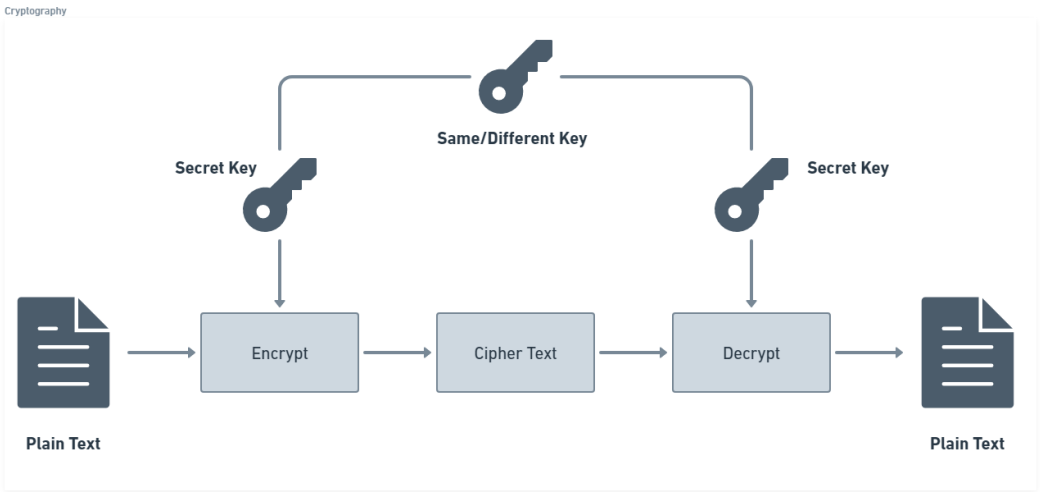

Figure 4. Cryptography Architecture

Figure 4 describes the process of cryptography. It involves encrypting a text or a file with the help of a hidden key. The resultant encrypted file is then sent to the receiver. At this stage the file is decrypted with the same key and then the original file can be viewed by the user.

3.2.3 Watermarking Architecture

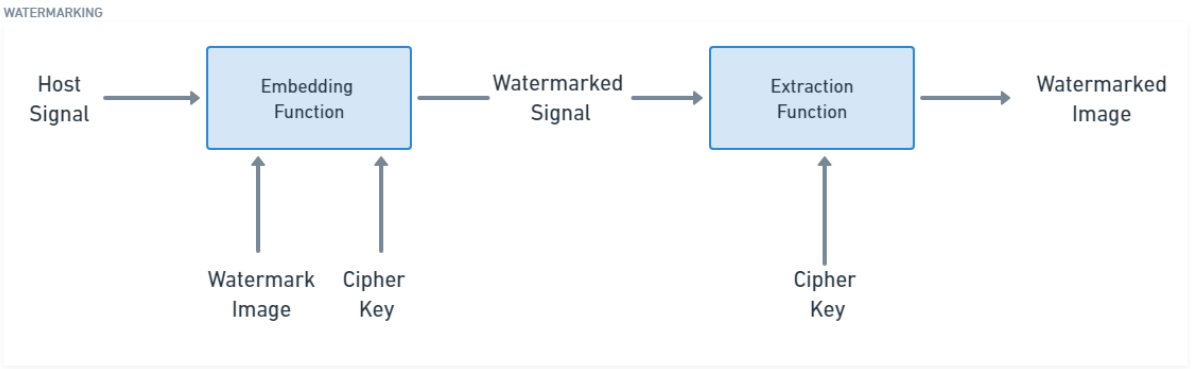

Figure 5. Watermarking Architecture

Figure 5 describes the process of watermarking. the digital media (e.g., image) is prepared for watermark embedding. This may involve resizing, normalizing, or converting the media to a suitable format. The watermark data or message to be embedded is generated. It can be a text, image, or any other form of data that represents the desired hidden information. The watermark data may be encrypted to enhance its security and prevent unauthorized removal or tampering. The embedding algorithm defines how the watermark is inserted into the digital media. It typically modifies specific elements or features of the media, ensuring that the watermark is imperceptible or difficult to remove.

3.3 METHODOLOGY

To hide information in a medical image we followed a series of steps that included methods of Steganography, AES encryption as a cryptography method and Discrete Cosine Transform (DCT) as a watermarking method. First, a suitable medical image is selected as the host image, which will serve as the carrier for the hidden information. The information to be hidden is encrypted using a AES algorithm, ensuring its confidentiality and security. Then the encrypted message is divided into smaller blocks, treating each block as an independent entity for embedding. DCT is applied to these blocks, transforming them into the frequency domain. The selection of appropriate DCT coefficients plays a crucial role in maintaining both the visual quality of the host image and the imperceptibility of the hidden message. Once the DCT coefficients are selected, the encrypted message is embedded within them using LSB steganography. The embedding process modifies the chosen coefficients slightly, allowing them to carry the hidden information while still appearing like their original values. The embedding is performed in such a way that the hidden message remains concealed and undetectable to the human eye. We feel that using Steganography, cryptography and watermarking together is the best and secure way to hide information in any medical image [11].

3.4 FEASIBILITY STRUCTURE

- **Financial Stability**: Although the technology may be expensive, it only requires a single investment because images may be produced with ease once the software has been developed. Additionally, doing such a work on the cloud can significantly lower costs and be more effective due to the increased availability of cloud resources.

- **Technical feasibility**: The technologies utilised are open source, which allows anybody to contribute to them, and all of the hardware and software used are readily available on the market. The information gathered from the user will be kept on their local system and utilized to enhance the application's functionality and accuracy.

- **Economic Feasibility**: Economic feasibility defines whether the expected benefit equals or exceeds the expected costs. It is also commonly referred to as cost/benefit analysis. The procedure is to determine the benefits and the savings expected from the system and compare them with the costs. A proposed system is expected to outweigh the costs.

- **Operational Feasibility**: Operational feasibility is the measure of how well a proposed system solves the problems with the users. Operational feasibility is dependent on human resources available for the project and involves projecting whether the system will be used if it is developed and implemented. The project is operationally feasible for the users as nowadays almost all the teachers/staffs are familiar with digital technology.

CHAPTER - 4

FEATURE EXTRACTION

4.1 LSB STEGANOGRAPHY

LSB steganography [12] is a method of hiding data in a digital image by replacing the least significant bits (LSBs) of the image's pixels with the bits of the hidden data. The LSBs are the least significant bits of a byte, and they are often the least noticeable when changed. This makes LSB steganography a good method for hiding data in images, as it is difficult to detect the changes that have been made. To hide data using LSB steganography, the sender and receiver must agree on a secret key. The secret key is used to encrypt the data that will be hidden in the image. The encrypted data is then converted to bits, and the bits are replaced with the LSBs of the image's pixels. The receiver can then use the secret key to decrypt the data that has been hidden in the image. LSB steganography is a simple and effective method for hiding data in images. However, it is not a perfect method. The changes that are made to the image's pixels can sometimes be detected, and the hidden data can be extracted by an attacker.

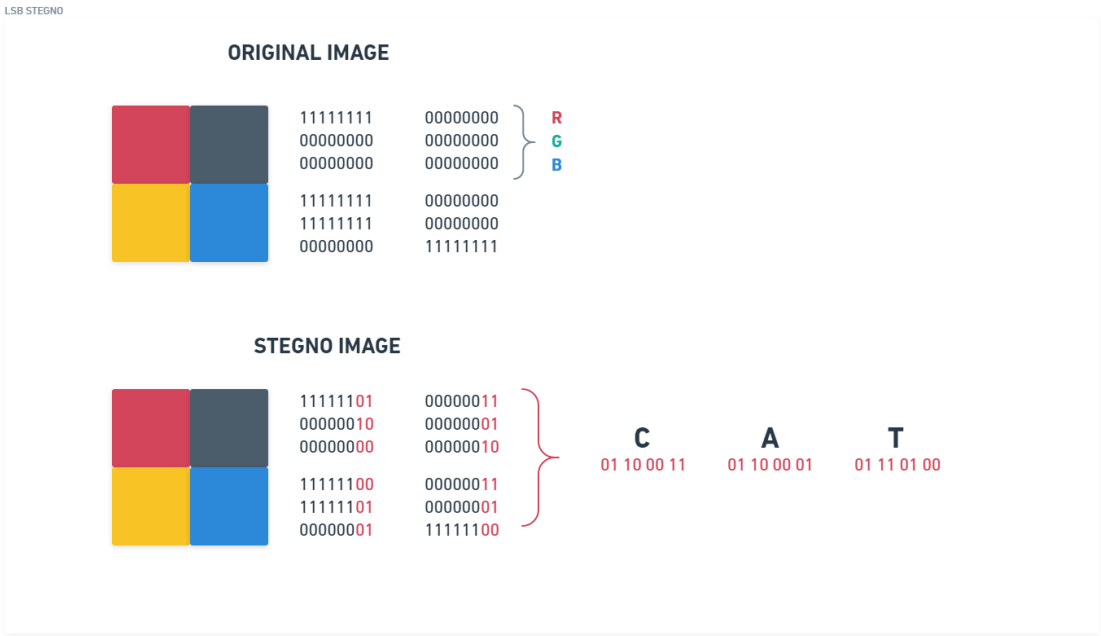

Figure 6. LSB Steganography

Figure 6 represents the working of LSB Steganography, the LSB bits of each pixel of the image is changed slightly to encode the message.

4.2 AES ENCRYPTION

AES (Advanced Encryption Standard) [13] is a widely used symmetric encryption algorithm that provides strong security for protecting sensitive data. It is a block cipher, which means it operates on fixed-size blocks of data. AES was chosen as the U.S. government's default encryption method by the National Institute of Standards and Technology (NIST) in 2001. AES is one of the most secure encryption algorithms in use since no serious flaws have been discovered in it. AES is a very secure algorithm because it is very difficult to find the key that was used to encrypt the data. The key is a very long string of bits, and it is very difficult to guess. Even with the most powerful computers, it would take billions of years to find the key.

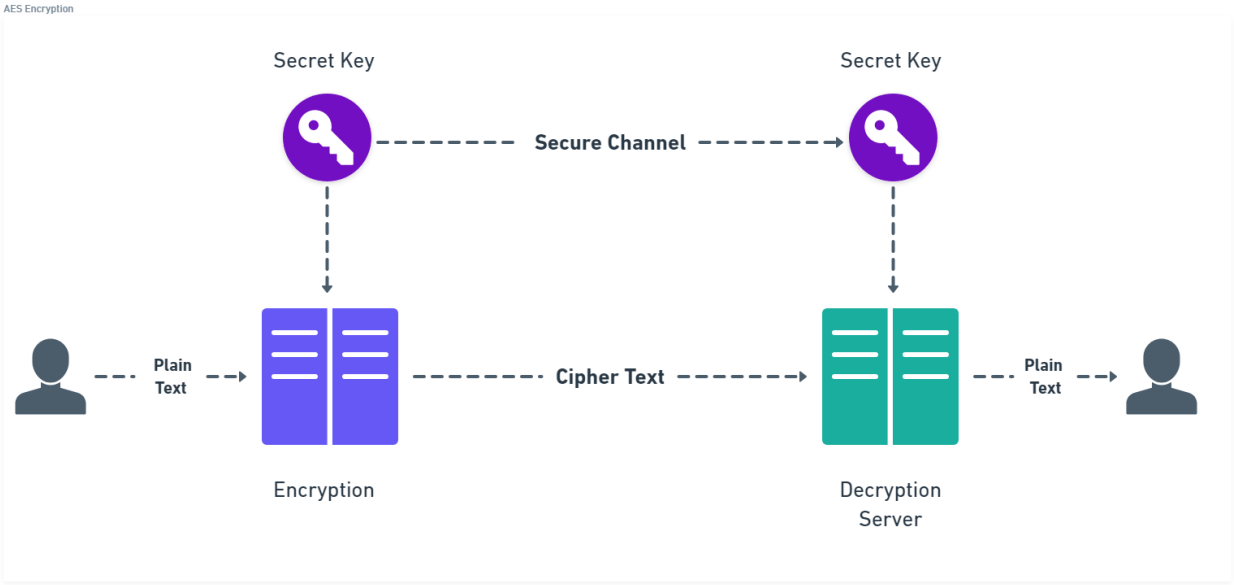

Figure 7. AES Encryption

Figure 7 explains the working of AES Encryption. AES being a symmetric encryption algorithm uses the same key for both encryption and decryption. The encryption process is reversible using the same key. The decryption process uses the same rounds as the encryption process, but in reverse order.

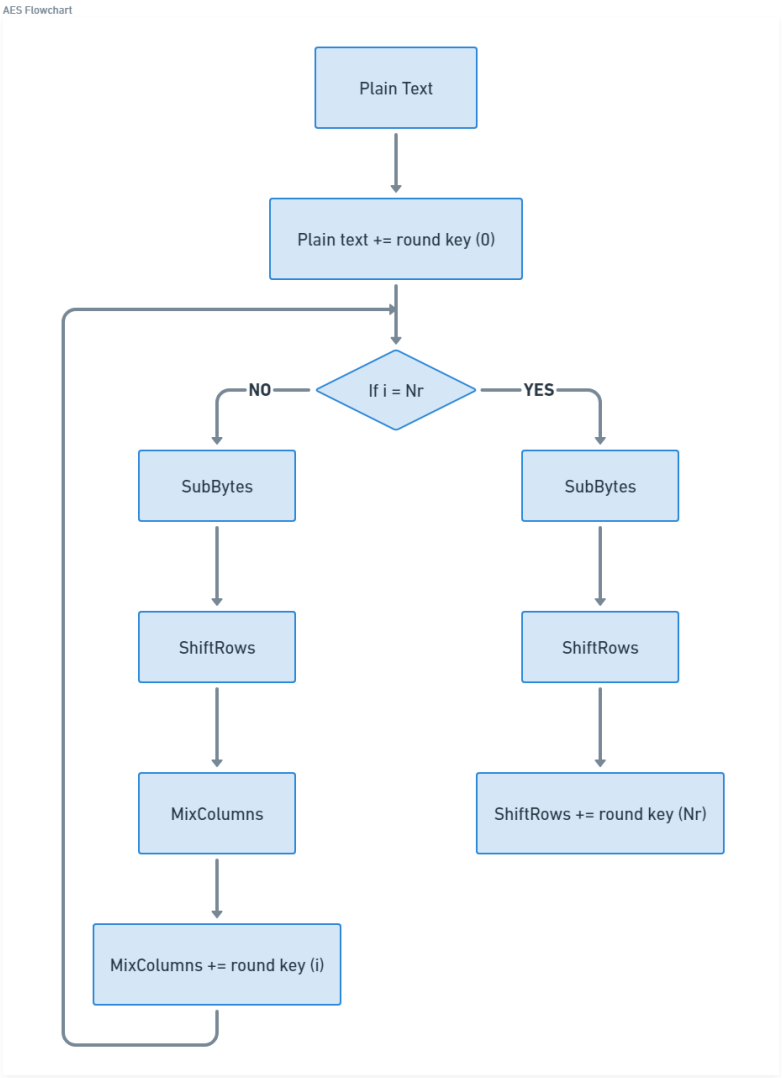

Figure 8. AES Flowchart

Figure 8 describes how AES algorithm works:

1. **Key Expansion:** The original secret key is expanded into a set of round keys, one for each round of encryption. This key expansion process uses a combination of bitwise operations, such as substitution and permutation, to generate the round keys.
2. **Initial Round:** The plaintext is divided into fixed-size blocks (128 bits for AES) and undergoes an initial round of transformation. During this round, the plaintext is combined with the first-round key using a bitwise XOR operation.
3. **Rounds:** Each round consists of four main operations performed on the data:
    a. SubBytes
    b. ShiftRows
    c. MixColumns
    d. AddRoundKey

4. **Ciphertext:** After all the rounds are completed, the resulting data block is the ciphertext, which is the encrypted form of the original plaintext.

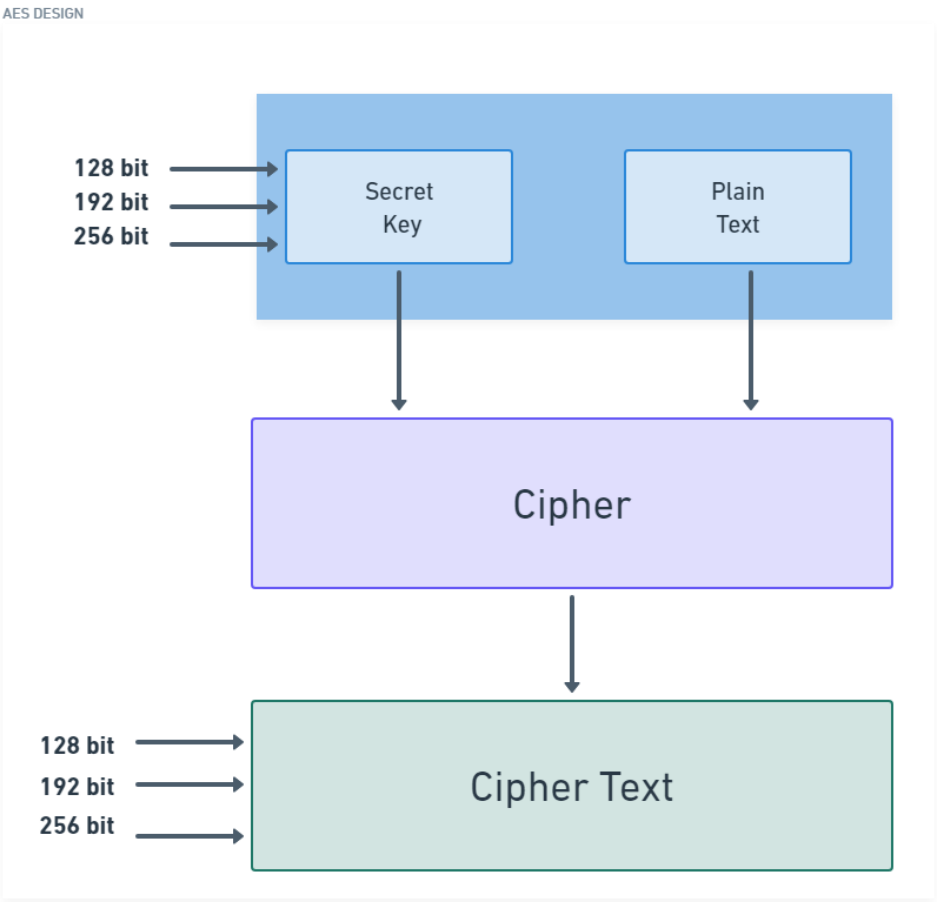

Figure 9. AES Design

Figure 9 explains the AES Design structure that works by transforming plaintext (the original data) into ciphertext (the encrypted data) using a secret key. The key length determines the level of security provided by AES, with AES-128, AES-192, and AES-256 being the most used key sizes. Block cypher AES encrypts data in units of 128 bits [14]. AES keys can have a size of 128, 192, or 256 bits.

4.3 DISCRETE COSINE TRANSFORM (DCT)

Discrete cosine transform (DCT) is a mathematical process which converts a series of data points from the spatial domain to the frequency domain. DCT [15] can be used as a watermarking technique in the field of digital image processing. The DCT is a widely employed transformation that converts a spatial domain image into a frequency domain representation. It is like the Fourier transform but is more suited for image compression and manipulation. The DCT is used in a variety of applications, including image compression, image denoising, and image watermarking.

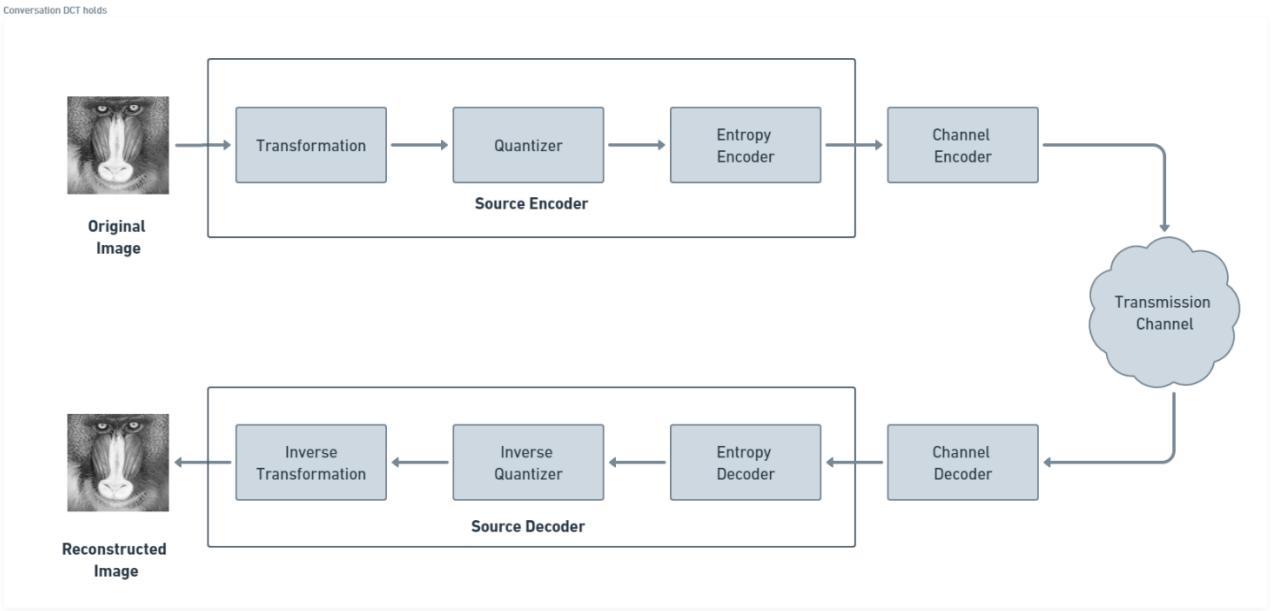

Figure 10. Working of DCT

Figure 10 briefly explains how DCT works:

1. At the sender's end the following steps take place:
    a. **Original Image**: The original image is the starting point of the process. It is typically represented as a matrix of pixel values.
    b. **Transformation**: The DCT is applied to the original image. This transforms the image from the spatial domain to the frequency domain.
    c. **Quantizer**: Quantization reduces the precision of the DCT coefficients by mapping them to a smaller range of values. This step introduces loss of information and helps in compressing the image.
    d. **Entropy Encoding**: It is a compression technique that assigns shorter codes to more frequently occurring coefficients and longer codes to less frequent

coefficients. This reduces the overall number of bits required to represent the coefficients.

e. **Channel Encoder:** The encoded data is further processed by a channel encoder, which adds error correction codes or performs additional encoding to enhance the reliability of data transmission over a specific channel.

2. Then similarly decoding is done at the receiver's end.

4.3.1 WATERMARKING WITH ENCRYPTION

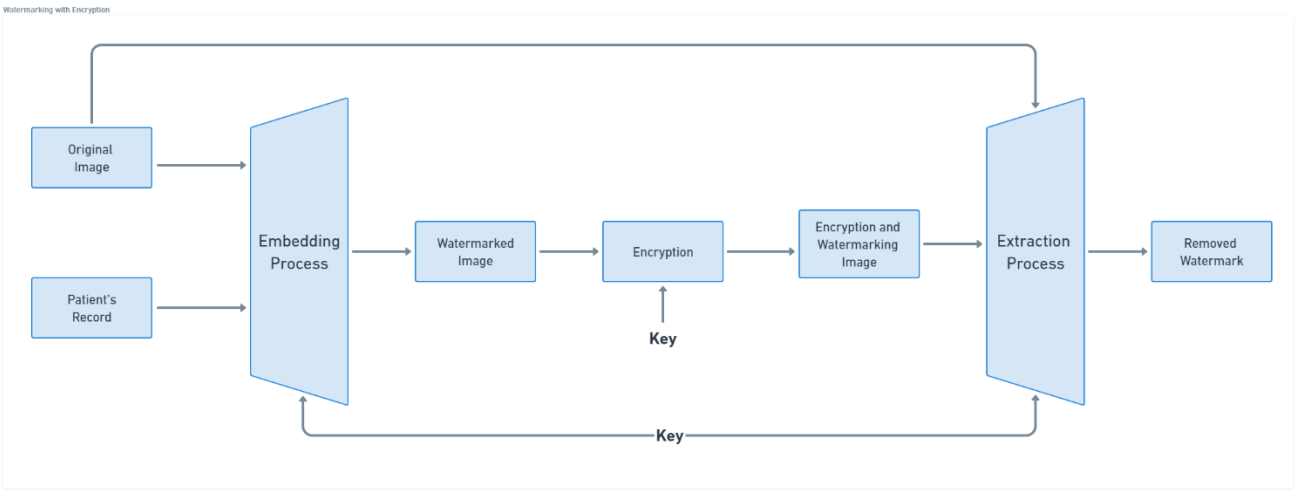

Figure 11. DCT with AES Encryption

Figure 11 explains the working of DCT and AES together. When it comes to securing medical images, a common approach is to use a combination of DCT (Discrete Cosine Transform) and AES (Advanced Encryption Standard) algorithms. By combining DCT and AES, medical images can be secured effectively. The DCT transformation provides a means of decorrelating and compacting the image data into frequency components. AES encryption adds an additional layer of security by ensuring that the transformed image data is encrypted and protected. The inverse process of decryption and inverse DCT allows the authorized recipient to retrieve the original image data.

CHAPTER- 5

RESULTS AND CONCLUSION

After many iterations we created a functional Graphical User Interface (GUI) for our project that is fully capable of encoding a text within a carrier image and also decode any encoded image and extract the text from within it.

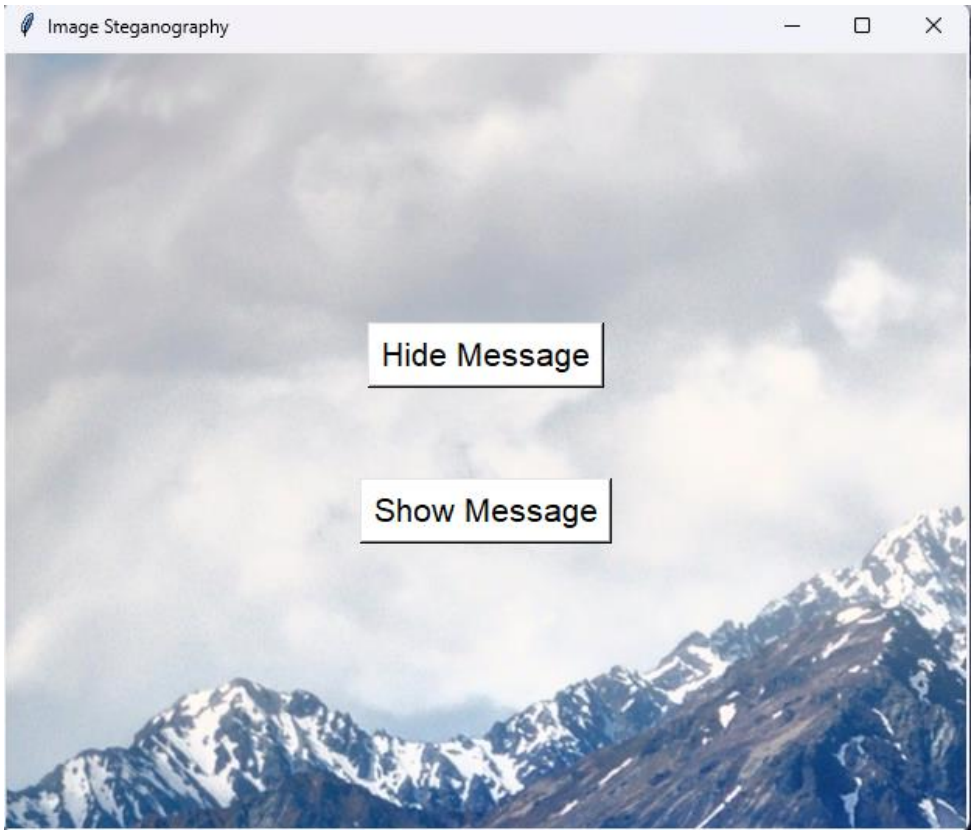

Figure 12. Home Page

Figure 12 represents the home page of our GUI that provides two different options which are either to hide message namely, Hide Message button, and Show Message button to extract the text which was hidden within an encoded image.

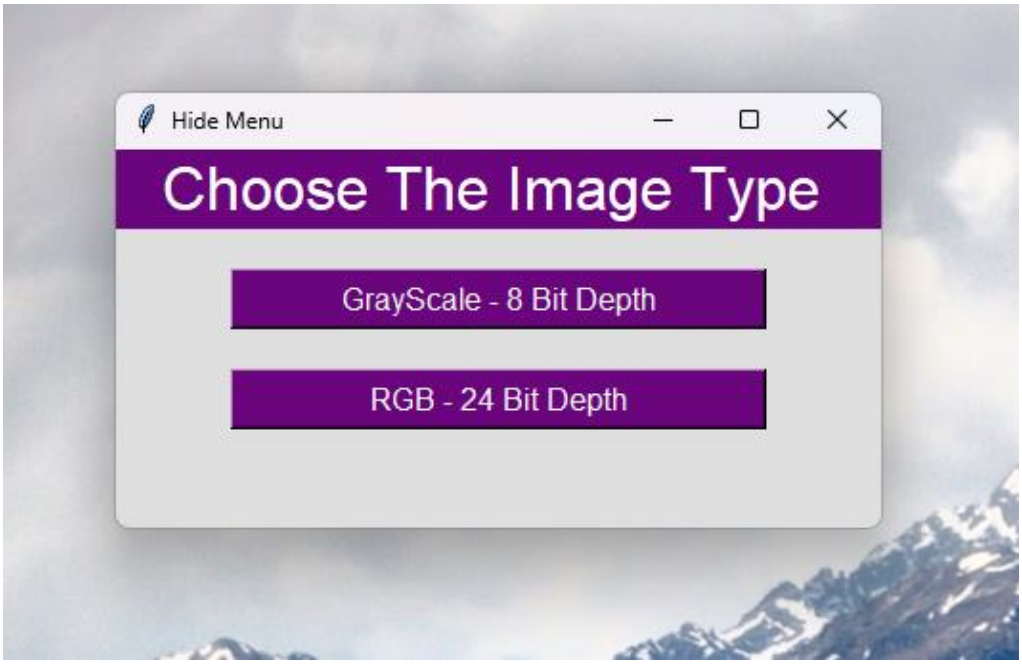

Figure 13. Choose Image Type Window

When we click on either of the button, we obtain a window as shown in Figure 13 above. The window provides us with two options either to select a Grayscale 8-bit image as carrier or encoded image to be decode or RGB 24-bit image.

Figure 14. Hide Image Window

If you have opted for Hide Message option in home page then after the choosing the image type, you will encounter a window like Figure 14 where you can add target image which will act as a carrier image and also enter the text you wish to hide within the carrier image. This carrier image could be either be a grayscale one or a RGB one as per the software requirements and specifications. After the text is successfully hidden within the image it is stored within a specific directory for easy retrieval and sharing it via various channels.

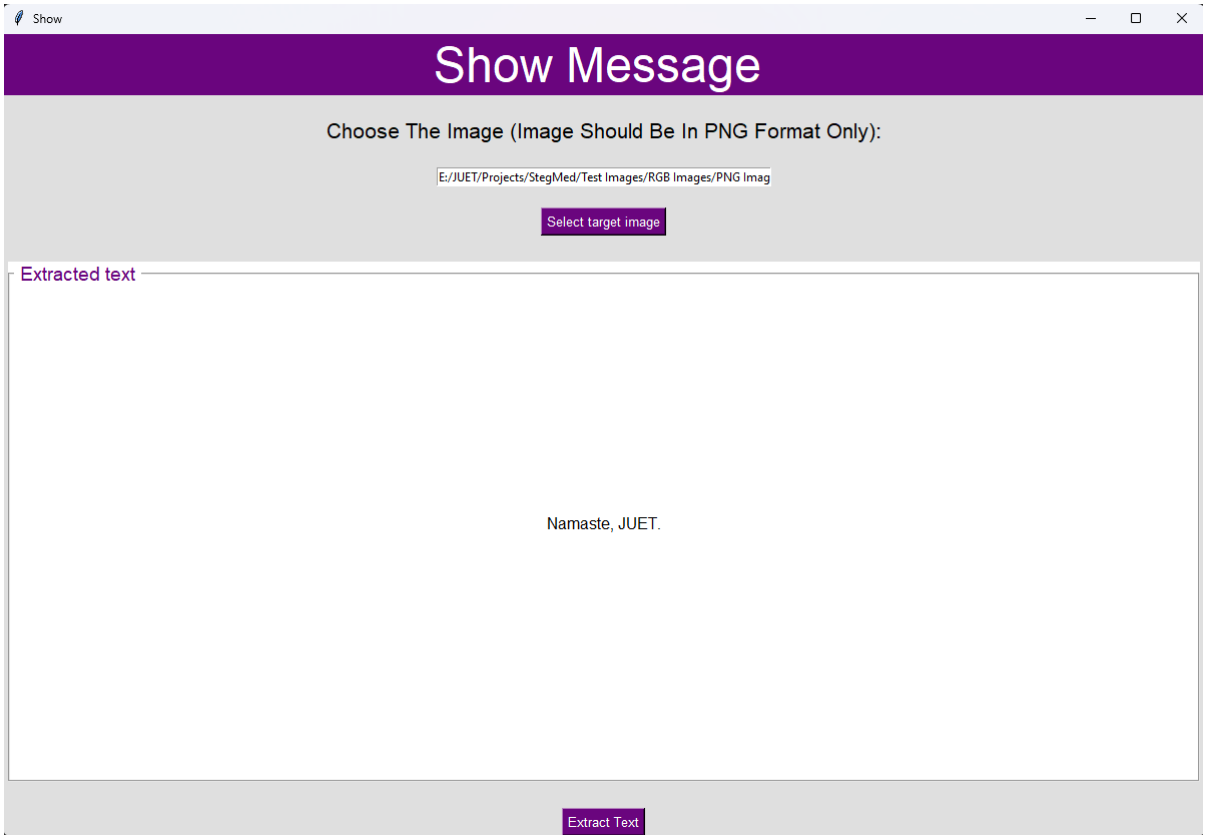

Figure 15. Show Message Window

If you have opted for Show Message option in home page then after the choosing the image type, you will encounter a window similar to Figure 15 where you can add target image and extract the hidden text within the image.

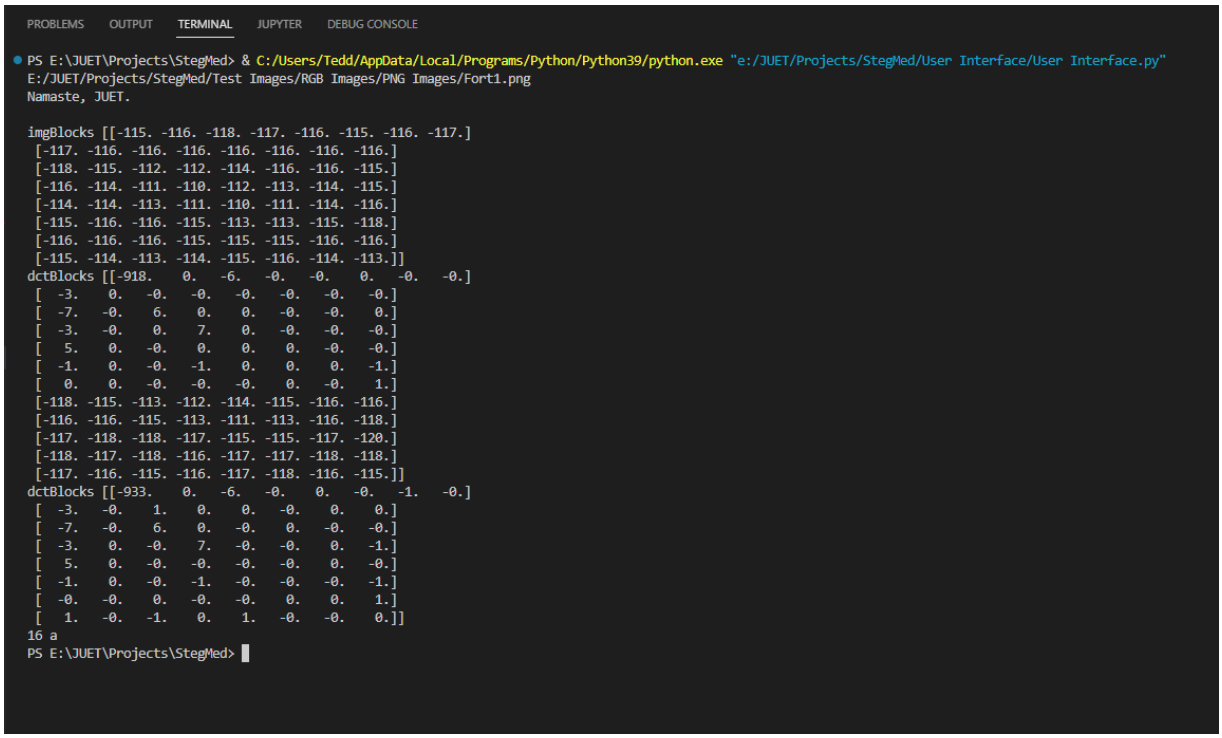

Figure 16. Terminal onsuccessful execution of programme.

In Figure 16 we can clearly see the state of terminal on successful execution of the programme which depicts Carrier Image Matrix, DCT transformation matrix, and hidden text message. Also, Figure 17 shows the project structure. This was the overall result of the project we built to hide sensitive medical information within the medical images with the help of concepts of steganography to hide message in plain sight or any format which can be shared publicly without the fear of information leak.
The concept cryptography was used to encrypt the image To add an extra layer of protection. Finally, the idea of Watermarking for authentication purposes.

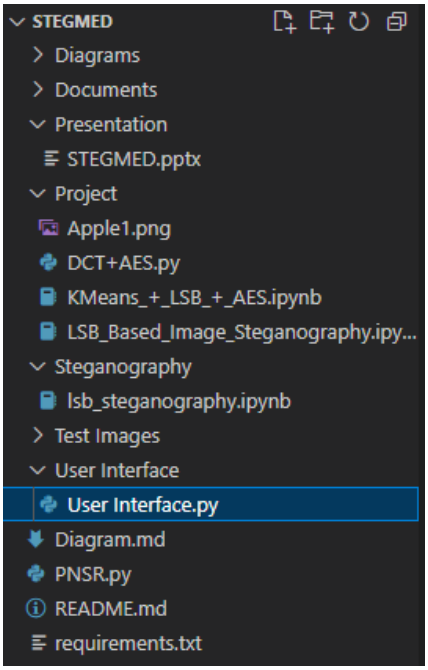

Figure 17. Project Structure

CHAPTER- 6
FUTURE WORK

Our project focuses on addressing the security concerns related to electronic health records (EHRs) by combining the technologies of steganography and cryptography. For that we were able to develop a secure and user-friendly system for transferring sensitive medical documents.

With blockchain breaking the market, it can be used to explore and enhance the security and integrity of EHRs. Blockchain provides a decentralized and tamper-proof ledger that can ensure data immutability, traceability, and secure access control. Using blockchain, multiple smart sensors collect the user's health recording, and then encrypted health data will be stored in the nodes of the Ethereum blockchain, thus protecting the privacy of users. Blockchain can also be used to enable patients to see every time their medical records are updated and to give explicit consent every time, they are shared with healthcare providers or others.

Artificial Intelligence is another field which can be explored when it comes to EHRs. We can utilize artificial intelligence and machine learning techniques to detect anomalies and potential security breaches in EHR systems. This can help in early detection and prevention of unauthorized access or data breaches.

CHAPTER - 7
REFERENCES

[1] A Secure and Efficient Scheme for Electronic Medical Record Transmission Based on Steganography and Cryptography, Xiaolong Li, Yang Xiang, Wanlei Zhou, 2016, Journal of Medical Systems, 10.1007/s10916-016-0564-3

[2] A Novel Secure Medical Image Transmission using Cryptography and Steganography, Priyanka Sharma, Savita Gandhi, 2020, International Journal of Advanced Research in Computer Science, 10.26483/ijarcs.v11i9.7262

[3] A Review on Image Steganography Techniques, Nisreen I. Yassin, Maen M. Al Assaf, Ghazali Sulong, A. Manaf, 2016, International Journal of Advanced Computer Science and Applications, 10.14569/IJACSA.2016.070751

[4]https://www.learnforensic.com/blog-details/How-Steganography-can-Lead-Digital-Forensic-Investigation/7

[5] Stallings, W. (2013). Cryptography and network security: Principles and practice (6th ed.). Pearson Education

[6] Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering: Design principles and practical applications. Wiley.

[7] Samavi, S., Karimi, N., & Soroushmehr, S. M. R. (2018). A review on medical image encryption techniques. Journal of Medical Systems, 42(7), 118.

[8] Mamatha, T., Rajan, C., & Gopinathan, M. (2015). Secure and efficient medical image transmission using steganography. In 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS) (pp. 1-5). IEEE. 10.1109/ICIIECS.2015.7192880

[9] Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3.4), 313-336.

[10] Podilchuk, C. I., & Delp, E. J. (2001). Digital watermarking: Algorithms and applications. IEEE Signal Processing Magazine, 18(4), 33-46, DOI: 10.1109/79.939780

[11] Wayner, P. (2002). Disappearing cryptography: Information hiding: Steganography & watermarking. Morgan Kaufmann.

https://www.sciencedirect.com/book/9781558607696/disappearing-cryptography-information-hiding-steganography-and-watermarking

[12] Fridrich, J. (2009). Steganography in digital media: Principles, algorithms, and applications (2nd ed.). Cambridge University Press.

[13] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

[14] Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES - The Advanced Encryption Standard. Springer.

[15] Ahmed, N., Natarajan, T., & Rao, K. R. (1974). Discrete cosine transforms. IEEE Transactions on Computers, 23(1), 90-93. DOI: 10.1109/T-C.1974.223784

CHAPTER – 8

AUTHORS

1. **Vani Seth**

   Email: 201b299@juetguna.in

   Contact: +91 7906966199

2. **Tanish Khandelwal**

   Email: 201b283@juetguna.in

   Contact: +91 7378427998

3. **Shreyash Shukla**

   Email: 201b259@juetguna.in

   Contact: +91 7007728174