Image Steganography Algorithm for Medical and E-Health care system

3rd Semester

MASTER OF TECHNOLOGY

By

Shreya Gupta

Department of Computer Science and Engineering

JAYPEE INSTITUE OF INFORMATION TECHNOLOGY
(Declared Deemed to be University U/S 3 of UGC Act)
A-10, SECTOR-62, NOIDA, INDIA

December 2022

TABLE OF CONTENT

ACKNOWLEDGEMENT

First and foremost, I would like to express our gratitude to my Mentor, Dr. Amanpreet Kaur, who were a continual source of inspiration. She pushed us to think imaginatively and urged me to do this dissertation without hesitation. Her vast knowledge, extensive experience, and professional competence enabled me to successfully accomplish this dissertation. This endeavour would not have been possible without her help and supervision. I could not have asked for a finer mentor in my studies. This initiative would not have been a success without the contributions of each and every individual.

I would like to thank Jaypee Institute of Information and Technology for providing me with the opportunity to work on the dissertation “Image steganography algorithm for medical and e-health care system”. Last but not least, I would like to express my gratitude to my family, siblings, and friends for their invaluable assistance, and I am deeply grateful to everyone who has contributed to the successful completion of this project.

DECLARATION

I hereby declare that the dissertation, titled **"Image steganography algorithm for medical and e-health care system"** is a record of original research work undertaken by me for the award of the degree of Master of Technology in Computer Science submitted at **Jaypee Institute of Information and Technology**. I have completed this study under the supervision of **Dr. Amanpreet Kaur**, Department of Computer Science.

I also declare that this dissertation has not been submitted for the award of any degree, diploma, associate ship, fellowship or other title. It has not been sent for any publication or presentation purpose.

I am fully responsible for the contents of my M. Tech Theses.

…….
(Signature)

Shreya Gupta

Department of Computer Science
Jaypee Institute of Information Technology, Noida, UP, India
Date: 09 December 2022

SUPERVISOR'S CERTIFICATE

This is to certify that the work reported in the M. Tech Dissertation entitled **"Image Steganography Algorithm for Medical and E-Health Care System"** submitted by **Shreya Gupta** at **Jaypee Institute of Information Technology, Noida**, **UP**, **India,** is a record of research work done by her during the academic year 2022-2023 under my supervision in partial fulfilments for the award of Master of Technology in Computer Science.

This dissertation has not been submitted for the award of any degree, diploma, associate ship, fellowship or other title. It has not been sent for any publication or presentation purpose.

…….
(Signature of Supervisor)

Dr. Amanpreet Kaur

Department of Computer Science
Jaypee Institute of Information Technology, Noida, UP, India
Date: 09 December 2022

PREFACE AND ACKNOWLEDGEMENT

This report has been prepared as a part of my dissertation as a part of MTech. The report is prepared with the view to include all the details regarding the thesis that I carried out.
The initial portion is the description and study of Image steganography and cryptography for health care system, its previous and current scenario. Next the second portion is regarding the core, how the secure and preserve the medical images using steganography and cryptography techniques. The expected outcome is to develop an algorithm which will be a hybridization of cryptography and steganography techniques and to apply it in health care domain for preserving security and information privacy of confidential data without much affecting the quality of medical image.

Currently, there are several methods that employ steganography, cryptography, or both to send information securely while masking the contents of keeping the content and its presence hidden. Modern protocols for steganography and cryptography are used to ensure the confidentiality and integrity of information. Thus, as you go ahead the report will reveal every detail of the work that I have done in this thesis.

ABSTRACT

Compared to traditional methods, significant improvements in internet infrastructure have an impact on e-healthcare services. Therefore, strong encryption methods are required for data security while transmitting data over any type of communication channel. The Internet of Things (IoT) combines the virtual and physical worlds to create an integrated communication environment of interconnected platforms and devices. The security and integrity of the medical data become major concerns for healthcare services applications as a result of the IoT's substantial growth in the healthcare industry. For the purpose of protecting the diagnostic text data in medical images, this thesis suggests a hybrid security strategy.

The proposed model is created by fusing a proposed hybrid encryption system with the 2D Discrete Wavelet Transform 2 Level (2D-DWT-2L) steganography technology. The Rivest, Shamir, and Adleman (RSA) and Advanced Encryption Standard (AES) algorithms are combined to create the proposed hybrid encryption scheme. The suggested model begins by encrypting the secret data and then uses 2D-DWT-2L to conceal the outcome in a cover image. Pictures in both colour and grayscale are used as cover images to hide various text sizes. The performance of the proposed system was evaluated based on six statistical parameters - the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Similarity (SSIM) and Correlation. The suggested model demonstrated its ability to conceal the patient’s confidential information into a cover image with high imperceptibility, capacity, and little degradation in the received stego-image when compared to state-of-the-art approaches.

LIST OF ACRONYMS AND ABBREVIATIONS

AES	Advance encryption standard
BER	Bit Error Rate
BIS	Bit Invert System
CC	Correlation Coefficient
DWT	Discrete Wavelet Transform
HMF	Henon Map Function
HH	High-High Band of DWT
HL	High-Low Band of DWT
HWT	Haar Wavelet Transform
IRD	Image Region Decomposition
LH	Low-High Band of DWT
LL	Low-Low Band of DWT
LSB	Least Significant Bit
MRI	Magnetic Resonance Imaging
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
RSA	Rivest, Shamir and Adleman
SC	Structural Content
SSIM	Structured Similarity
WT	wavelet transformation
2D-DWT-2L	2D Discrete Wavelet Transform

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

Computer networks have had to quickly expand due to the information technology industry's rapid and ongoing development. This has the effect of greatly easing the transport of electronic data. The rapid development of electronic data transmission methods and the widespread use of images have created enormous potentials for security and the protection of private information from unauthorised access. Therefore, it is imperative to establish security solutions to ensure data protection while being transferred over the internet.

One of the methods that is most frequently used to ensure the security of data is cryptography. Technology for data encryption has advanced significantly in recent years [16]. Currently, a variety of data encryption techniques are used, particularly for the protection of digital images. On the other hand, with the massive and rapid development of the Internet and network infrastructure, is a common way of using image steganography methods to hide confidential data in different image modalities. Steganography is the science and art of concealing information in a carrier so that no one other than the intended recipient is aware of its presence. The name "steganography" comes from the Greek terms "stegano," which means "covered," and "graphic," which means "writing." The cover, or another piece of information that appears to be normal in this process, conceals a secret message [1]. This procedure seeks to conceal the secret information without raising any viewer suspicions.

Many different algorithms are currently utilised to encrypt data in various ways. A technique that combines many codes of various sorts is known as a hybrid encryption [19]. One popular technique is to create a secret key to encrypt a random symmetric, and then use the recipient's asymmetric public key to encrypt this key cypher. The same symmetric cypher and secret key are then used to encrypt the message. The message is then encrypted and delivered to the recipient using the secret key.

The security of data transit was improved in this study by integrating encryption techniques based on Advanced Encryption Standard (AES) and Rivest, Shamir, Adleman (RSA). Due to the Advanced Encryption Standard algorithm's high effectiveness in the encryption block, it is used for data transfer [11]. The cover picture is merely a piece of unimportant information used to conceal the secret information in concealed communication techniques. However, in copyright protection strategies, the crucial information that has to be protected is the cover image, and the buried message could contain a copyright mark.

A stego key is used throughout the embedding procedure to make it challenging to extract the embedded message without passing this key. The result of the message embedding procedure is represented by the stego image. The original image with the secret message is also included in this picture. The embedded message is extracted from the stego image at the recipient's end, either to confirm the image's copyright or to finish the covert communication process. The stego key is used while embedding and must also be utilised during extraction. To stay up with the quick evolution and advancement of technology used for networking and hiding information, researchers are still looking more sophisticated methods of information concealment.

1.1 AIM

This thesis aims to improve the security of medical data transmission based on the integration between a steganography technique and a hybrid encryption scheme to get a highly secured healthcare system and to create an algorithm to securely insert sensitive information into the cover picture.

1.2 OBJECTIVE

The objective is to develop an algorithm that combines cryptography and steganography techniques and use it in the healthcare industry to protect the confidentiality and privacy of sensitive data without significantly compromising patient's safety the level of medical imaging quality. In order to create a highly secure healthcare system, this work intends to increase the security of medical data transmission via the combination of a steganography approach with a hybrid encryption strategy.

The objective of this dissertation is to combine steganography with cryptography algorithms to create a new hybrid approach for data security. With the help of this technology, a secret message may be encrypted and embedded into a cover picture to achieve maximum imperceptibility, longevity, and little degradation of the received stego image. The major goals of this study were to:

- Create a security framework for steganographic concealing text data in images utilising LSB and DWT separately.
- Create a hybrid security solution that combines steganography (LSB and DWT) with data encryption (AES and RSA) to improve stego picture performance and data imperceptibility.
- Determine how well the created system secures and retrieves the original data.

1.3 BACKGROUND

The organisation, processing, and preservation of medical data have all been transformed by information technology. It also focuses on the importance of information security and the steps that should be done to stop an attack. In steganography, choosing an image is the most important consideration since it establishes the foundation for security because it serves as the cover picture for embedding either text or an image. Due to its great picture quality and because it works well with images and paintings, the JPEG image format is widely used in data transfer via the internet.

1.4 MOTIVATION

Steganography serves the dual purposes of dispelling both the suspicion of having hidden information and preventing others from discovering the information. The unique aspect of information-hiding strategies is that they must keep up with new technology and make advantage of it across all computing media (texts, image, audio, video and network packets). The message is a secret document that has to be sent and is disguised in the carrier to make it hard to find.

Any steganography system has two key components: imperceptibility and steganography capacity. However, there is confusion between these two qualities. This is due to the difficulty of increasing capacity while retaining a steganography system's imperceptibility.

Additionally, there are still a few odd but effective ways of information concealment for usage with data transfer communication protocols.

- Increasing the peak signal to noise ratio (PSNR) is one of the most essential reasons for our present research, along with reducing the main squared error (MSE), average difference, and increasing the embedding capacity of the stego image.
- One of the key difficulties is the requirement that the communication content be protected from both (perceptual attacks or statistical). The ability to conceal information is a crucial need for the design of algorithms since there is a stronger special interest due to the existence of an ongoing, hostile assault.

1.5 AN OVERVIEW

1.5.1 Need of Security in Healthcare domain

Growth and strength of an organisation always depends on maintaining strong relationship and satisfaction of customers. Customers are patients in the healthcare industry, and each patient's medical records must be kept safe. The foundation of the healthcare industry has always been the patient-doctor relationship of trust. When it comes to treating a condition that is classified, security has a significant impact. One area of the health care industry where the patient's revelation of information about the ailment may have a detrimental effect on the patient's physical and emotional well-being is classified diseases. Here, confidentiality, security, and privacy of information are important considerations. All of these essential elements must be carefully and securely kept in the event of an illness.

1.5.2 Need of Information sharing in healthcare domain

Medical personnel must share data in order to provide treatment at a level that meets best practises, whether it be through an organization's intranet or the internet. This raises the issue of security.

1.5.3 Steganography

Steganography and watermarking are two information-hiding techniques that have lately drawn a lot of interest. This is due, at least in part, to the desire to safeguard digital copyrights (audio, image and video). Other uses include clandestine illicit communication, information gathering, and securing different forms of communication from spies. Along with new and improved methods for concealing information, the scene will also provide methods for finding and (perhaps erasing) such information. Data hiding is the technique of covertly incorporating information into a data source without affecting its integrity. Writing secret messages in a way that neither the sender nor the intended receiver is aware of their existence is both a science and an art. The technique of data concealing involves converting the real data into a different multimedia file that is equal to it in terms of photos, videos, or audios rather than keeping it in its original format.

1.5.3.1 Define Steganography

Steganography is the science and art of concealing information in a carrier so that no one other than the intended recipient is aware that it is there. The phrase literally means "covered writing" and derives from the Greek words "steganos" (covered) and "graphic" (writing). a method of secret communication in which a piece of information (a secret message) is buried within

another piece of seemingly harmless information, sometimes referred to as a cover, in order to prevent the viewer from developing any doubts about the secrecy of the secret information.

1.5.3.2 The Steganography S-Element

Steganography requires two pieces of information, the cover and the information to be concealed:

1.5.3.2.1 The Cover

The medium into which the data will be placed is referred to as the "cover." The best cover should be chosen if you want the steganography process to work well. The cover serves as a vehicle for the conveyed message as well. Steganography relies on concealing the data beneath a cover in order to prevent it from being seen as safe and to avoid encryption. As a result, once the embedding is detected, the embedded data may be accessed. Secret messages can be inserted into image, video, audio, and other file forms.

1.5.3.2.2 The Data

To be gradually inserted into the cover, the data that must be buried must be seriously reliable. To fit all the data within, the size of the data shouldn't be larger than the cover size. Images may contain the same number of pixels in both the cover and the data, but the cover will have more colour information per pixel than the concealed data. Figure illustrates the basic steganography method.

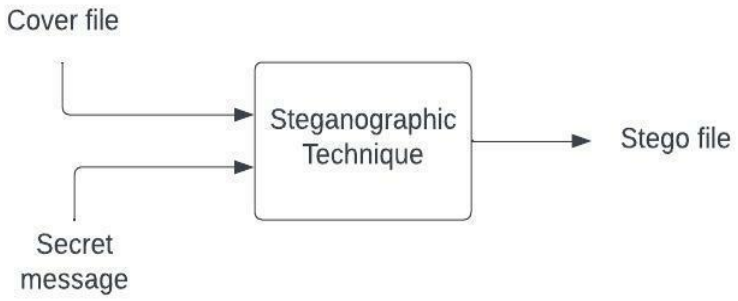


Figure 1.5.3.1 *Fundamental approach of steganographic process*

1.5.4 Cryptography

The two main divisions of cryptology are as follows:

- Cryptography: It is the study of secret writing, and its primary objective is to conceal the real meaning of the message being utilised. When sending data via an insecure channel, cryptography is highly helpful. Cryptography has a significant value in terms of security when it comes to data exchange, which covers almost every network, especially when it is done online. There are certain unique security needs for data exchange, including:
    a. Authentication is the process of establishing one's identification.
    b. Confidentiality - Assures that only the intended recipient may read the communication.

c. Integrity: Assures the recipient that the message they have received has not been altered in any way from the original.
d. Non-repudiation is a technique to confirm that the communication was transmitted by the intended recipient.

- Cryptoanalysis is the study or practise of breaking down coding systems. You could occasionally believe that a break is available and shouldn't be categorised as a serious scientific subject. Although nowadays the majority of cryptanalysis is conducted by academic scholars and is crucial to contemporary coding schemes. Whether they are secure or not will never be known. The only method to ensure that a cryptosystem is safe is through cryptanalysis, which is why it is regarded as a fundamental component of cryptology.

The function of cryptography may be explained by a straightforward example of cryptography, as shown in Figure. The fundamental concept of encryption is to change the message's content in a certain way and only let the message's lawful receiver to reconstruct it. You may characterise the discrete valued cryptosystem as follows:

P: It represents a collection of potential plain texts.

C: It represents a collection of potential cypher texts.

K: It is a symbol for a range of potential encryption keys.

E, D: A collection of potential encryption and decryption transformations.

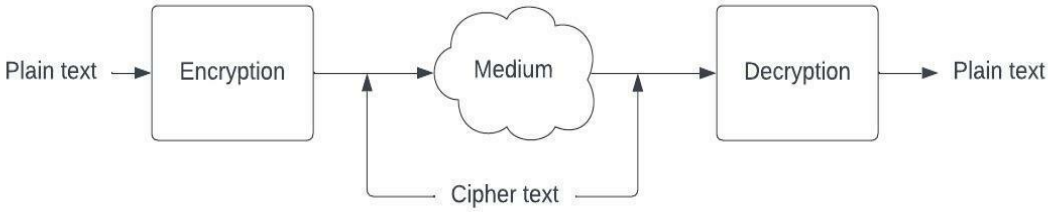


Figure 1.5.4.1 *Cryptography*

1.5.4.1 Basic Terminology in cryptography

- Plain text: The original message sender who wishes to speak with another person is referred to in plain text.
- Cipher Text: It refers to a message that is unintelligible to everyone. In other words, it is a meaningless communication, and before the message is really transferred, an encoder will convert the original message (plain text) into something that cannot be read or understood.
- Encryption: It explains that this term refers to the process of turning plain text into cypher text. Secret messages are sent using encryption techniques across secure, private

channels. Two essential components—a key and the fundamentals of each encryption algorithm—are required for the encryption process.

- Decryption: This procedure undoes the encryption. To put it another way, any procedure to change (cypher text) to (plain text). To get the assistance of the original method, we apply the decryption technique side in the second method (receiver) (cipher text message). To ensure that the message is transmitted in this situation, the decryption technique and key must also be used.
- Key: It alludes to a specific letter, alphanumeric text, or a number. And throughout the first two stages of encryption (plain text) and the second stage of decryption, this key is used (cipher text). The choice is crucial for the cryptography key since it directly affects how secure the encryption technique is. Symmetric key cryptography is employed when the same key is used for encryption and decryption. However, when using several keys in a cryptographic system, it is necessary to utilise a unique encryption key for one, a second for another, and a third key for decryption.

1.5.5 Advanced Encryption Standard (AES) algorithm

The National Institute for Standards and Technology (NIST) in the United States has established the Advanced Encryption Standard (AES) as a cryptographic standard. It is the outcome of a 1997 competition. The NIST has urged current parties across the world to submit suggestions for new standards. He was expected to support a block size of at least 128 bits in all submitted ideas, and the three primary volumes must be made up of 128, 192, and 256 bits. The Rijndael Algorithm, created by Joan Daemen and Vincent Rijmen, was selected as the winner three years later. In 2001, the AES standard's final version was unveiled [3]. The Rijndael algorithm's simplicity and ease of use were key factors in its success to implement at the hardware and software levels.

The initial round key is added in order to encrypt data using the AES (Rijndael) method. The round function and a small (mod I round with (a = Nal) come next, followed by this application function round of the function (Nr - 1) times.

The (sub_bytes, shift_rows, and mix_columns) steps make up the round suction, which also includes the round key. In the (Nal) round, the Mix Columns step is careless. The following provide justification for describing an advanced AES (Rijndael) algorithm:

The blocks AES (Rijndael) technique requires all inputs and outputs to be organised into chains of bytes. The state will first create a matrix with a plain text block before working on the filled matrix (column by column). After the final round, the encrypted text of the matrix state is obtained. The note will now be read by a matrix (column by column). Each phase works continuously (sub_bytes, shift_rows, mix_columns and Add_key).

1.5.5.1 Evaluation Criteria for AES

The primary requirement of the Advanced Encryption Standard (AES) algorithm submission is that you must use a block cypher that supports blocks longer than 128 bits and has keys longer than (128, 192, and 256) bits [4]. The request for proposals was assessed using the following assessment criteria:

Security: Is one of the most crucial aspects of assessment in terms of: "Are compared to the real security algorithm for other algorithms offered. " It's critical to guarantee the integrity of the mathematical foundations underlying the algorithmic security.

The additional security elements that are known to the general public and that are found out throughout the review process.

Cost: The following is included in this section:

- The licencing conditions, as the AES algorithm ought to be accessible and not exclusive.
- Excellent computational performance and memory capacity requirements must also be met.
- The algorithm and implementation characteristics: The following are included in this:
- Flexibility, which aims to offer the essential tools like: (PRNG, MAC generator, retail, stream cipher).
- It is necessary to provide a conducive environment for the usage of both hardware and software.

1.5.5.2 Hardwired electronics using AES

The same key is used on both sides of the symmetric encryption known as AES, making it suitable for hardwired electronics. It features keys that are either 128, 192, or 256 bits long and a set message block size of 128 bits of text (plain or encrypted). Longer messages are split into 128-bit chunks before being transmitted. Naturally, longer keys demand a lengthier encrypt and decrypt procedure while also making the encryption harder to crack. A two-dimensional, 44-byte array may be used to conceptualise the structure of a 128-bit message block. The four fundamental processes of AES encryption operate on the bytes, rows, and columns of this array many times each.

1.5.6 Rivest- Shamir- Adleman (RSA) algorithm

The Rivest- Shamir-Adelman (RSA) public key and that of its creators make up the origin, which is known as the asymmetric cypher. Because they were all students at the Massachusetts Institute of Technology (MIT), and because RSA has been chosen because to its widespread use and in-depth analysis [11]. The public key algorithm is being utilised commercially and will be heavily publicised across all industries (business and personal communications). RSA currently has the benefit of having flexible key sizes that vary from 2 to 2048 bits. The key size that the user or programmer selects will have the most impact on the security of this technique.

Although many applications still utilise keys with 512 bits, this approach is employed and the length of the key size (1024) bit representation.

A symmetric key is frequently used to encrypt data using private or secret keys. It is a class of algorithms that, in general, uses a single key to (encrypt or decrypt) communications. The method in which personal information is utilised is crucial, thus the parties concerned want to talk openly and honestly about everything. The best security measures involve giving each correspondent pair their own key. Therefore, it is crucial for both parties to preserve the user key's secrecy. Prior to the message being delivered to the receiver, the sender must first work to encrypt the message using the secret key. On the other side, the recipient will encrypt the

message he receives using the same key. He is used here as a secret key ratification service for the message. Additionally, it sets the missionaries apart from other harmful sources.

Public Key

If the key is known, the integrity of the message being sent is compromised. Therefore, it is essential to develop a secure method of key exchange between the correspondents. The accomplishment of his operation depends completely on the encryption of a Private Key. Through the use of keys and certificates, public key encryption provides secure electronic business communication, as shown in Figure. It demonstrates how a message is encrypted, making it only capable of being decrypted by the intended receiver. As a result, Alice uses Bob's public key to encrypt a message before sending it to him. Bob used his private key to decipher the ciphertext.

Implementation:

1. Key will be generated.

2. Encryption process

3. Decryption process

1.5.7 Transform Domain Technique

Wavelet transformation (WT) What we currently refer to as a "wavelet," one of the crucial and practical computation tools for a range of signal and image processing applications, appears to have been first mentioned in writing in 1909. [14] The ability to distinguish the minute features in a signal is a benefit of the wavelet transform. While extremely small wavelets may be used to extract very fine features in a signal, very big wavelets can be utilised to detect coarse details. Image steganography models frequently involve the conversion of spatial domain information into frequency domain information wavelet. This is due to the wavelet transform's pixel-by-pixel division of the high frequency and low frequency information. Due to its many benefits, the wavelet transform domain is recommended for many steganography applications.

In a wide range of statistical applications, including data compression, signal processing, picture smoothing and denoising, computer graphics, fingerprint authentication, and multiracial analysis, wavelets are a potent tool. The transform-based strategies leverage the image's domain-specific properties to both embed and carry out data. The picture is first translated into the appropriate domain, such as the wavelet domain (DWT), frequency domain (DCT, DFT), or another domain. Instead of using actual pixels, the data in these approaches is contained in the altered image. The picture is then converted again into the spatial domain. The advantage of this approach is that it embeds data in the image that is less susceptible to compression, image processing, and cropping. Additionally, the information covers more pixels or the entire image.

1.5.8 Discrete Wavelet Transform (DWT)

Any wavelet transforms for which the wavelets are discretely sampled is known as a discrete wavelet transform (DWT). [14] One of the frequency domains where steganography can be used is represented by it. A coding mistake results in discontinuity between blocks when using the Discrete Cosine Transform (DCT) approach, which results in unappealing blocking

artefacts. Because DWT is applied to the entire image, this shortcoming of DCT is lessened when employing it. Without any blocking artefacts, DWT offers superior energy compaction than the DCT. In the DWT, the picture signal is filtered using two different types of filters.

1.5.9 Haar Wavelet Transform (HWT)

Since Alfred, a Hungarian mathematician, originally presented the HWT in 1910, it has been in use. A straightforward method of data compression known as the Haar Wavelet Transformation (HWT) entails averaging and differencing terms, data removal, storing detail coefficients, and matrix reconstruction. Simple input value pairing using the HWT, transmitting the sum and saving the difference. Recursively repeating this procedure produces the next scale by pairing together the sums, which ultimately produces differences and one final sum.

1.5.9.1 Haar Function

Wavelets are mathematical operations that were created for frequency-based data sorting. A certain vector space's orthogonal basis is referred to as a "wavelet" in this context. Using a wavelet transformation, data is transformed from the spatial to the frequency domain and then each component is stored with the corresponding resolution scale.

When doing a 2D wavelet transformation, the transformation method is initially performed to the rows and columns. The Haar DWT does exceptionally well at identifying features like corners and edges. The inverse Haar DWT is used to construct the stego picture when the embedding procedure is finished. The following is how the vertical and horizontal operations are carried out:

$$\varphi = \begin{cases} 1, & t \in [0,1/2) \\ -1, & t \in [\frac{1}{2}, 0) \\ 0, & t \in [0,1) \end{cases}$$

Eq 1.5.9.1 Vertical and horizontal operations

a) Operation on the horizontal plane:

A picture will be split into two bands, one for low frequencies and the other for high frequencies. From left to right, horizontally, pixels are scanned. The surrounding pixels are subjected to addition and subtraction processes. The left side, which symbolises the low frequency band, is where the results of the addition operation are kept.

b) Operation on Vertical plane:

Low low (LL), low high (LH), high low (HL), and high high (HH) frequencies are further differentiated from the low and high frequencies acquired from the horizontal operation. For the addition and subtraction operations, every pixel will be scanned over, but in the vertical direction. The nearby pixels' addition will be held in the top.

1.5.9.2 Properties of Haar:

The characteristics of the Haar Transform are as follows:

i. Orthogonally: Low and high frequencies are separated in the original signal. These filters are said to as orthogonal since they allow for splitting without repeating unnecessary information.
ii. Compact support: Outside of the transform frequency range, the filter's magnitude response should be zero. The transform is energy invariant when this property is true.
iii. Linear Phase: To produce a linear phase, symmetric filters must be utilised.
iv. The energy compaction for pictures of the Haar Transform is low.
v. The orthogonal, genuine, and very quick Haar transform.
vi. The Haar matrix's basis vectors are arranged sequentially.
vii. The speed of computation is fast.
viii. HWT is a powerful compression technique.
ix. Ease of use.
x. The quickest computation performance.
xi. Since it can be computed directly without using
xii. A temporary array, it is memory efficient.

1.5.10 Image type

The information in an image can be encoded in a number of different ways:

1.5.10.1 Binary picture
1.5.10.2 A grayscale pictures
1.5.10.3 An index images
1.5.10.4 A RGB or true colour image

1.5.10.1 The binary image

Pixels only come in black or white. We just need one bit per pixel because there are only two potential values for each pixel (0, 1).

1.5.10.2 Grayscale icon

The typical range of grayscale values for pixels is 0 (black) to 255. (white). A pixel can be represented by eight bits, or exactly one byte, within this range. There are other grayscale ranges used, although they are often powers of 2.

1.5.10.3 Indexed picture

An array plus a colour map matrix makes up an index image. Direct indices into a colour map make up the pixel values in the array. By convention, this documentation refers to the array in this document as the variable name X and the colour map in this document as map.

1.5.10.4 RGB or TRUE COLOR IMAGE?

Each pixel has a unique hue, which is determined by the proportions of red, green, and blue in the pixel. A totally of 2563 different colours are conceivable if the range of values for each of these components is 0-255. The red, green, and blue values for each pixel are represented by a "stack" of three matrices in such an image. This indicates that there are 3 values that correlate to each pixel.

1.6 CONCLUSION

Data transmission and storage have become more dependent on information security. The security backgrounds presented in this chapter make use of several encryption methods and steganography methods. The extensive usage of images and the quick growth of electronic data interchange have increased the need for data security and the protection of sensitive information from unwanted access.

One of the most popular strategies for guaranteeing good data security is encryption. A significant advancement in encryption technology has been made recently, and a variety of encryption techniques are being employed for picture security. These techniques generate random encryption keys, but the material itself is hidden. To ensure safe transport of picture data, both the encryption and decryption methods are created and implemented.

On the other hand, we worked on steganography method. Steganography and watermarking are two information-hiding techniques that have lately drawn a lot of interest. This is due, at least in part, to the desire to safeguard digital copyrights (audio, image and video). Image Steganography is the process of hiding information which can be text, image or video inside a cover image. The secret information is hidden in a way that it not visible to the human eyes. Deep learning technology, which has emerged as a powerful tool in various applications including image steganography, has received increased attention recently.

CHAPTER 2

LITERATURE REVIEW

The current literature review included is divided into four-part exploration of correlated areas:

2.1 Literature Review of 20 papers
2.2 Integrated Summary
2.3 Research gap
2.4 Objective

2.1LITERATURE REVIEW

G.F. Siddiqui, [1] proposed the Image Region Decomposition (IRD) method that contain more secret information in patient medical photos with higher imperceptibility. The algorithm divides the grayscale magnetic resonance imaging (MRI) images into low-intensity, medium-intensity, and high-intensity zones, each of which is distinct. Each region consists of k pixels, and we operate a block of n least significant bits (LSBs) in each pixel. For embedding, four kinds of MRI pictures in various dimensions are used. Images are tested for imperceptibility using data of varying quantities, and their veracity is confirmed by quality factors. Peak signal-to-noise ratio (PSNR) index are used to evaluate the performance of the proposed IRD algorithm on the set of brain MRI images. By altering the 2nd and 1st LSBs in the low-intensity region, the findings demonstrated that the MRI stego image is undetectable, just like the original cover image. Compared to other approaches of a similar kind, our suggested steganography technique offers a superior average PSNR (49:27). The empirical findings demonstrate that, when compared to current state-of-the-art approaches, the proposed IRD algorithm greatly enhances imperceptibility and data embedding capability.

Dr. Bhavani R, [2] Proposed a multi-secure and robustness of medical image-based steganography scheme. For the preservation of digital medical photos, the suggested method offers an effective storage security mechanism. In order to secure the MRI medical image into a single container image, we suggested a workable steganography technique using the Integer Wavelet Transform (IWT). After applying a flip to the left on the container picture, the dummy container image was produced. The hidden image of the patient's medical diagnosis was then retrieved, transformed using Arnold, and then jumbled. In the first instance, a dummy secret picture was created while the scrambled secret image was integrated into the dummy container image. In the second instance, the container image was captured, the dummy secret image was combined with it, and a stego image was produced. The medical image that was recovered has satisfactory visual quality.

[3] Medical picture tampering is possible when the medical image is transferred over an insecure public network. Therefore, it is essential to verify the accuracy of medical photographs in order to guard against any unlawful alterations. We compute the ROI (Region Of Interest) cryptographic hash function using the SHA method to verify the integrity. The discrete wavelet transform will be used to incorporate the hash value (H1) in the RONI. We can verify the integrity of a medical image by comparing the hash value at the receiver side. The hash function does not match if any alteration takes place. This study postulates a fresh approach to enhancing

security. By using spatial reversible steganography, the altered medical image is concealed within a regular-looking image. It facilitates in hiding the existence of sensitive medical information. It makes sure that anyone listening in won't suspect that a hidden medical image is present in the image.

M. M. Hashim, [4] proposed the new steganography method which uses three control random parameters and is based on the Bit Invert System (BIS). Henon Map Function is used to guide the random selection process (HMF). Affine cypher and the Huffman technique are used to limit the amount of data that needs to be encrypted before being embedded for high payload capability and to boost security. This integration works well for two primary reasons: first, segmenting the secret data to track and map every bit in the stego picture during embedding, and second, verifying and mapping to determine the 0- and 1-bits during embedding. The findings demonstrated that the proposed approach may guarantee medical data security and confidentiality while retaining image quality.

Yeshwanth Srinivasan, [5] proposes the idea of concealing the very existence of these records via image steganography is examined in this study, despite the availability of several security solutions that encrypt data and prohibit unwanted access to it. The usefulness of Bit-Plane Complexity Segmentation (BPCS) steganography, an improved high-capacity data hiding technique, is explained, and it is shown that it can successfully conceal medical records in color cervical pictures. To address the drawbacks of the conventional Least Significant Bit (LSB) manipulation approaches of data concealing, Bit Plane Complexity Segmentation (BPCS) was developed. It is based on the notion that information can be concealed even in higher bit-planes if it is concealed in blocks that appear to be complex. This technique breaks down each color plane in an RGB image into its 8 individual bit-planes, resulting in a total of 24 bit-planes (8-bit grayscale images will have just 8 bit-planes). Pursuing the bit-plane decomposition, the 8-bit intensity values (also known as Pure Binary Code, or PBC) are first converted to Canonical Gray Code for the reasons indicated in (CGC). The distribution of 1s and 0s for each 8x8 block in each of the 24 bit-planes, a complexity value α is calculated. The α measure specifies the distribution of 1s and 0s in the 8×8 block. If α is high, this indicates that the 1s and 0s are evenly distributed across the block, therefore switching out the complex block will not significantly alter the image.

R. Bala Krishnan, [6] describes a biomedical data concealing method that uses a Queen Traversal pattern to locate the pels over the DICOM picture and a Sudoku-based scrambling on the biomedical DICOM image. It conceals the private medical information in the cover images that have been encrypted or scrambled. The effectiveness of the system in relation to the many parameters of relevance is established by experimental results. In this expected work, the authors of the suggested model present and discuss a novel method for encapsulating hidden content in scrambled DICOM pictures. The chess game's Queen Traversal pattern is used to identify the pels. As a result, massive complexity and a larger payload were required for the unlawful material extraction. The cover DICOM image has been split up into an equal number of smaller blocks and subjected to the Sudoku pattern-based scrambling technique. The tour patterns have been put into practice to locate the Image's pels during the hidden medical data embedding exercise. The secret material is embedded by the LSB substitution algorithm, and the DICOM stego image is produced after the final descrambling. The stego DICOM pictures produced by this suggested method have the lowest Means Square Error (MSE) and highest

Peak Signal to Noise Ratio (PSNR) values. The key (secret) for content extraction is the optimal traversal method for locating the pels and Image scrambling and descrambling patterns.

Muhammad Arslan Usmana, [7] proposed a novel picture steganography technique is put forth that not only satisfies the three criteria for a successful steganography approach but also provides various levels of data encryption for medical images. The study's objectives are to:

- I provide imperceptibility by only using the edge regions of the cover picture for data embedding.
- provide high capacity by applying lossless compression to the secret images and
- encrypt and protect the compressed data by employing swapped Huffman tree encoding (SHT).

While briefly explaining the Canny algorithm that we utilized in our method and edge recognition in photos.

Additionally, it describes encryption, starting with the most fundamental kind of Huffman coding, and switched Huffman tree coding (SHT). The suggested image steganography method's data embedding and extraction processes are also thoroughly detailed.

This paper proposes, [8] E-Health Security Using Images Steganography is a combination of various techniques that have been put forth. The suggested system offers many levels of protection to assist the user in sending data securely. These safeguards make it challenging for an intrusive party to obtain or open the file. As a result, robustness is increased because the intruder cannot grasp what is transmitted. Using MATLAB 2021 and a random pixel generator to encrypt the hidden image, the cover image is turned into a steganography image, which is then validated with credentials such a user ID, password, and OTP verification using a program called Pega. The major goal of this work is to ensure adequate and secure transmission of the image while maintaining full encryption. This paper also suggests that in order to validate identification, the sender and receiver should be authenticated more than once. In the encryption process, the secret image is encrypted by randomly rearranging the pixels according to a random pixel generator method. Only the sender and receiver are aware of the random key that is used. The Pega Database, which sends emails, was used to extract the user ID and password. The Pega tool sends the OTP to the authenticated sender's mobile phone number. The receiver end also uses the same two-level authentications. Thus, the suggested paper aids in the secure and safe transmission of images from sender to receiver. Using email authentication and an OTP, the authenticated user proves his identity on the transmitter side. Using the Pega tool, email authentication is carried out by sending the authorized user's login information to the sender's email address. Sending the OTP to the sender's mobile number completes the OTP verification process. The sender will be able to send the secret image following successful authentication. The encryption and steganography processes are implemented in the backend using MATLAB. The transmitter end handles both encryption and steganography completely. Here, the secret image is first encrypted using the XOR Cipher Encryption principle, followed by image steganography using the LSB approach, and lastly a stego image is produced using MATLAB.

Jing Liu [9], suggested a steganographic technique that can offer very secure protection for sensitive data in medical systems. In our method, a cover picture is first translated into a sequence of 1D pixels using a Hilbert filling curve, and then it is separated into embedding units with three consecutive pixels that are not overlapping. The base of the embedded digits depends on the differences between the three pixels, and we utilize the adaptive pixel pair match (APPM) approach to embed numbers in the pixel value differences (PVD) of the three pixels. Minimal distortion of the pixel ternaries brought on by data embedding can be achieved by addressing an optimization issue. We provide an APPM-based approach that takes HVS into account. Comparing Hong et al APPM. to other embedding techniques as k-bits LSB replacement, LSBMR, and DE, it exhibits the least distortion at the same embedding rate. Additionally, APPM permits the embedding of digits in several bases, which is a crucial condition for an embedding method when taking HVS into account. However, when a big base is used, APPM exhibits significant distortion. The suggested methodology uses APPM to embed data in PVD. To convert a 2D image's pixel matrix into a 1D pixels sequence, a Hilbert filling curve is utilized.

In order to guarantee the integrity of user multimedia image information processed through specialized medical equipment employing VR, Jeong Yoon-su, [10] suggest a steganography-based digital healthcare approach. The suggested model attempts to prohibit the medical team from using VR to illegally access multimedia picture data obtained by specialized medical equipment without the user's consent. The suggested model encrypts multimedia health care information with a hybrid cypher using the user's credentials and signature. Without compromising the user's multimedia image quality captured using specialized medical equipment, the suggested model incorporates elements that guarantee the integrity and confidentiality of the user's medical image information. In addition, because the user's signature information was encrypted using steganography-based cryptography-based ciphering techniques, multimedia medical information viewed through VR is not exploited without the users' agreement. In order to improve the administration of medical image information for users in hospitals, the suggested model in particular offers real-time guidance related to users' health status and first-aid care in connection with the hospital health service. The suggested model includes the following attributes: For the confidentiality of data:

- It first secures the integrity of encryption and decryption.
- Second, the certification is guaranteed by the medical imaging system without compromising the integrity of the medical images produced by specialized medical tools.
- Third, medical image information is safely communicated via steganography techniques.

In this paper Mamta Jain, Anil kumar, [11] suggest the idea of indefinite quality is used to suggest a fresh mystery transmission method, which is a compelling choice for conveying mystery therapeutic patient information combined with the appropriate medicinal carrier image. The sender distributes the secret information blocks arbitrarily to the transporter using a decision tree, which improves security standards and has a strong impact on the computation that is displayed. The proposed conspiracy makes use of the RSA cryptosystem to provide information privacy at the server farm. LSB replacements are used in steganography, together with a decision tree, to secure medical data. A decision tree shows a perfect division between

corresponding groups to provide options. By analyzing the results and histograms, it is discovered that the PSNR, MSE values, and rate of largest concealment limit are superior to other existing plans, and that subtlety bending cannot be evaluated from the associated mystery therapy stego images.

In this paper, Xia Liao and Jiaojiao Yin [12] suggest a brand-new steganographic method for JPEG medical images that is based on the inter-block coefficients' interdependence. The fundamental approach is to keep as many of the variations between consecutive DCT blocks' DCT coefficients at the same place. During the embedding phase, the cost values are dynamically distributed in accordance with changes in inter-block neighbors. According to experimental findings, the suggested methodology outperforms the most advanced steganographic technique and can cluster inter-block embedding changes.

In this paper, S.Durgadevi and S.Jayasrilakshmi [13] a substitute secure communication model is presented that combines cryptography with steganography techniques to provide a second layer of security, preventing a stenographer from deciphering the ciphertext without the key. The key images were first encrypted with the Secure Force-AES algorithmic programme, and then the encrypted images were concealed in the cowl picture using JSTEG and LSB techniques. This combination allows the key image to transmit over an open channel because the cypher image does not appear nonsensical but is concealed by the use of steganography to hide it between the cover photos. PSNR and MSE, two parameters, are computed.

In order to conceal the EPR data in the integer wavelet coefficients of RONI, a novel and effective medical image steganography is suggested by Hayat Al-Dmour and Ahmed Al-Ani [14]. In order to locate and conceal the hidden data in the sharp areas of the image, it uses an edge detection algorithm that makes use of overlapping blocks. Utilizing overlapping blocks is done in order to increase the embedding payload by minimizing the number of unwanted pixels. Applying an XOR operation, which only modifies one bit at most, reduces the difference between the cover and stego images by encoding two secret bits into three-pixel bits. In comparison to one of the already available EPR concealment techniques, the experimental results show improvements in the embedding capacity and imperceptibility.

A model is proposed and presented in this paper by merging the two approaches of elliptical curve cryptography and two types of steganography, as suggested by Eshraq S. Bin Hureib and Adnan A. Gutub [15] (i.e.,1 LSB and 2 LSB). The private and secret information will be encrypted then hidden in a much better method than before with the help of two procedures [1, 18, 21]. Additionally, when employing or applying 2 LSB with an appropriate level of security, there was a discernible shift in the number of empty bits in the picture capacity. This enables the secret information recorder and receiver to send more information while keeping anyone who is not permitted to see or obtain this information at a distance [14, 16, 17]. No unauthorised individual even learns that any information is present.

In this system, Mei Ling Phang and Swee Huay Heng [16] suggested few techniques, including a secure and reliable method using hybrid feature detection to extract edge and smooth areas from an image, two-component LSB substitution to randomly embed secret messages in edge areas, adaptive LSB substitution to randomly embed secret messages in smooth areas, and the widely used AES encryption technique to encrypt messages before embedding. They also demonstrated how this approach resists the two types of steganalysis attacks: visual and statistical. Therefore, this crypto-steganographic system for healthcare was able to meet the

fundamental requirements of steganography, as well as the main objectives of cryptography, which protect the message confidentiality.

In order to secure patient information, Ahmed Al-Ani and Hung Nguyen [17] suggested a steganography method for biomedical photos in this study. With PSNR values of more than 50 dB, this technique produces a stego image with a high payload and good quality. The suggested method's very effective performance is attained by employing PVD to choose sharp sections for embedding that are less susceptible to alterations by the HVS. The distortion is additionally lessened by utilising a hamming code to hide sensitive information, which also increases the security of the embedded message.

In order to improve anonymity in the event of a remote diagnosis, Hussah N. AlEisa [18] suggest image steganography to safely and covertly incorporate the patient's personal information in their medical photographs. The approximation coefficient of the integer wavelet transform's least significant bit is proposed. For both colour and grayscale images, this technique is examined. While IWT with R, B, and G component is used to conceal the secret picture in a colour image, IWT with LSB is used to conceal the hidden image in a grayscale image. By evaluating the mean square error and PSNR, one may determine the degree of distortion between the cover picture and stego-image, and one can estimate this degree of distortion using the normalized cross-correlation.

For a healthcare-based IoT environment, Mohamed Elhoseny and Gustavo Ramírez-González [19] has suggested a secure patient diagnostic data transfer model using both colour and grayscale photographs as a cover carrier. The suggested model used a hybrid of AES and RSA cryptographic methods with either 2D-DWT-1L or 2D-DWT-2L steganography. Different font sizes were used in the experiment, along with colour and grayscale graphics. The six statistical measures (PSNR, MSE, BER, SSIM, SC, and correlation) were used to evaluate the performance. The suggested model demonstrated its ability to conceal the private patient information into a sent cover image and little degradation in the received stego-image when compared to state-of-the-art approaches.

The grouped block approach is used in this paper, SVD-based fragile watermarking system to increase security and give an additional mechanism for identifying the attacked regions inside various medical pictures. To resist the vector quantization attack, two authentication bits—block authentication and self-recovery bits—were utilised. By recovering the compromised region from nearby blocks using the Arnold transform, the restored host's NCC and PSNR are finally improved. Abdulahziz Shehbab's [20] experimental findings demonstrated the suggested scheme's excellent reliability and ability to precisely pinpoint the attacked blocks. The suggested methodology significantly increases the PSNR of the self-recovered picture and the tamper localization accuracy as compared to state-of-the-art methods. Despite the fact that our suggested solution handled fragile tampered photos well, more testing is needed to assess how well it handles non-fragile altered images.
In their upcoming effort, they want to address this problem. Additionally, they will concentrate on identifying other tampering problems like image rotation, skewing, and resizing operations.

2.2INTEGRATED SUMMARY

The success of every business process depends on information and communication, which are two sides of the same coin. Computer networks are necessary in the rapidly expanding field of

health care for information exchange and communication. Internet or intranet, computer networks provide speedier communication options than other facilities. Risks associated with communication across a network are always present, including unauthorized access to the network.

In the healthcare industry, protecting patient confidentiality and information privacy are top priorities. Confidentiality, integrity, and availability are the three characteristics that must be maintained according to a traditional definition of security. Authenticity, responsibility, and non-repudiation qualities are also taken into account in several recent research. When focusing on patient information, all security terms and circumstances must be taken into account, particularly in cases of classified data when patients would like to keep their personal information private. However, in order to receive better care and treatment, individuals occasionally need to divulge details about their illness. In these circumstances, the appropriate person must be provided the appropriate information. To safeguard the privacy of patient information, different laws and regulations are in place in different nations.

Since transmitted medical data, such as private medical photographs and patient records, is typically enormous in size, steganographic systems protecting sensitive data should have a high embedding capacity while also being able to avoid detection. Medical data can be easily stolen or intercepted while being stored, sent over a network, or received online. By ensuring the security of medical data, these cybercrimes can be avoided. Researchers are increasingly using different media, such as images, audio signals, etc., to conceal sensitive or private information. Steganography is a technique for concealing secret information that can be used as an alternative to modern techniques for protecting medical data. By using a technique called image steganography, a secret image is embedded in a cover image. We employed steganographic methods to achieve the necessary authenticity and integrity. The inserted data should be undetectable thanks to steganographic technology. It is not visible to the naked eye. Integrity information for medical images is encoded in the RONI (Region of non interest). The addition or removal of lesions using image processing techniques can alter images. Lossy compression, such as JPEG, scale, rotation, and other factors could be at blame. Loss of diagnosis information in medical images will result. As a result, doctors occasionally misdiagnose patients. According to the tampering method, there can be unacceptable information loss. Integrity check is crucial in medical image communication as a result. We chose a common image to serve as our cover image to prevent deliberate attack. More protection is provided by the modified medical image that is integrated into the cover image.

In some papers, they presented a unique IRD approach in the image spatial domain to embed MRI host pictures with variable-sized patient secret data. The image is first divided into three parts based on intensities by the algorithm. Low, medium, and high intensity zones operate using the three least significant bits. Secret data bits are substituted on the third LSB with the 2nd and 1st LSB in the low-intensity area. Two LSBs are used in the region of medium intensity; the second LSB is used to replace secret data bits while the first LSB is adjusted. Only the first LSB is operated and replaced with secret data bits in the high-intensity region. A set of MRI pictures are used to evaluate the algorithm for both positive and negative cases. And on the other hand, they provide a pixel value differencing and APPM method-based adaptive steganographic scheme with low distortion and high capacity. We use the Hilbert filling curve to produce a 1D pixels sequence in order to better maintain the contents of the cover image. The APPM method is used adaptively to embed digits in multiple-base in pixel

value difference pairs of pixel ternaries using three pixels as the embedding unit. Their solution, as compared to the APPM scheme under the same base, achieves a significantly reduced distortion by addressing a smaller optimization issue.

2.3RESEARCH GAP

A multi-secure and reliable steganography technique based on medical images had previously been proposed. For the preservation of digital medical photos, the suggested method offers an effective storage security mechanism. The MRI medical image is protected using the Integer Wavelet Transform (IWT) in a practical steganography technique that creates a single container image [2]. However, the most recent research shows further development in image steganography, offering a means to boost stego images' potential for data concealment and imperceptibility. The Image Region Decomposition (IRD) method that has been proposed embeds more secret information in patient medical photos with higher imperceptibility. The algorithm divides the grayscale magnetic resonance imaging (MRI) images into low-intensity, medium-intensity, and high-intensity zones, each of which is distinct [1].

In the past, image steganography was used to safeguard medical images or data to increase imperceptibility [3], but as technology has advanced, a new steganography technique based on the Bit Invert System (BIS) with three control random parameters has been proposed. Henon Map Function is used to guide the random selection process (HMF). Affine cypher and the Huffman technique are used to limit the amount of data that needs to be encrypted before being embedded for high payload capability and to boost security [4].

Originally, medical data was secured via image steganography. Before integrating the payload into the cover image, lossless compression and many levels of encryption are applied to it using swapped Huffman tree coding. Secondly, the secret data is exclusively embedded in the cover image's edge regions, offering strong imperceptibility. The findings demonstrate that the suggested strategy assures patient information confidentiality and secrecy while retaining imperceptibility [7]. However, during the past few years, the practice of data masking has acquired significant support as a substitute for ensuring information security. This new study examines a biomedical data concealing method that uses a Queen Traversal pattern to locate the pels over the DICOM picture and a Sudoku-based scrambling on the biomedical DICOM image. The encrypted or otherwise obscured medical data is used to conceal [6].

Earlier, the transmission of private data in the healthcare system required confidentiality protection. In [9] study, we suggest a steganographic technique that can offer highly secure security for confidential data in medical systems. In our method, a cover picture is first translated into a sequence of 1D pixels using a Hilbert filling curve, and then it is separated into embedding units with three consecutive pixels that are not overlapping. Minimal distortion of the pixel ternaries brought on by data embedding can be achieved by addressing an optimization issue. But over time, further levels of security were added to protect the medical records by assuring secure connection between sender and receiver. The approach used in Paper [8] combines steganography and encryption to give security first priority. Only the designated sender is able to communicate the receiver with the secret image. Undercover medical X-ray images that are confidential are processed in the first stage of an image steganography system. By altering the position of the pixel in the image to encrypt the image

on the transmitting side, the encryption method utilized is based on the Random Number Generator and the pixel indication. On the other hand, this project suggests a way for authenticating the receiver by using OTP Verification and Email Authentication to decrypt the encrypted image on the receiver side.

They described a steganography method in article [5] that may be utilized as a very effective substitute for encryption for sending secure medical information together with the relevant medical picture. Steganography leverages the redundancies in the image to excellent use and decreases the quantity of information to be communicated by incorporating the secure information into the redundancies of the image, in addition to obscuring the fact that patient medical records are even present. The medical picture itself may be concealed inside, for instance, commonplace papers that offer signature verification by employing the multilayer encoding technique given. Furthermore, both in terms of data concealing capacity and resilience of the encoding model, the improved BPCS technique provided here exceeds the existing state-of-the-art in large capacity steganography whereas to guarantee the integrity and security of user multimedia picture information transmitted through specialized medical equipment like VR, the clinical workforce developed a steganography-based digital healthcare information service model in [10] article. To protect the integrity of the user's multimedia picture data obtained by specialized medical equipment, such as VR, without the user's agreement, the suggested model ciphered the user's signature and credentials on a steganographic basis. By connecting directly to a hospital server, encrypted digital medical information may be delivered in real time, addressing issues with previous research and offering real-time advice on user health and first assistance. According to the performance evaluation, the user's accuracy in extracting multimedia medical information was on average 10.4% higher than that of the current approaches, and the suggested model managed multimedia medical information 13.1% more efficiently than the existing model. Using the findings from this work, a performance evaluation of hospitals proposing to use VR is proposed, taking into account the size of the institutions and the number of medical personnel.

In paper [12], they provide a brand-new inter-block coefficient-based medical JPEG picture steganographic system. In order to preserve the differences between DCT coefficients at the same position in adjacent DCT blocks as much as possible, they first investigate an adaptive strategy that synchronises the modification directions for adjacent DCT blocks at the same position. Then, in the embedding process, the cost values are adjusted dynamically according to the changes of inter-block neighbours. Based on maintaining the interdependence of inter-block DCT coefficients, a unique medical JPEG picture steganographic system is created. Comparative tests demonstrate the effectiveness of the suggested strategy in clustering inter-block embedding changes and in achieving greater anti-steganalysis performance. According to experimental findings, the proposed scheme outperforms the most advanced steganographic technique and can cluster inter-block embedding changes whereas, in [14] paper, the researchers provide a novel medical picture steganography method for securing patient information by embedding that information within the image itself while preserving excellent image quality and high embedding capacity. By using Otsu's approach, this methodology splits the cover picture into the Region of Interest (ROI) and the Region of Non-Interest (RONI), and then shapes the ROI pixels into a rectangle in accordance with the binary pixel intensities. The Electronic Patient Records (EPR) are incorporated in the high frequency sub-bands of the wavelet transform domain of the RONI pixels to increase security. A method for identifying

and categorising edge areas using overlapping blocks is provided. Then, in order to reduce the difference between the cover and stego pictures, two secret bits are embedded into three coefficient bits via an XOR operation. Applying reduces the disparity between the cover and stego photos an XOR procedure, which may incorporate two secret bits by changing no more than one bit. The results of the experiments show that the suggested approach offers a decent balance between security, embedding capability, and aesthetic quality of the stego pictures into three bits for pixels.

In order to secure patient information, this [17] research offered a steganography technique for biological images and suggested a brand-new steganography algorithm. It uses a Hamming method to encrypt three secret message bits into four bits of the cover picture and Pixel Value Differencing (PVD) to identify contrast regions in the image. Excellent payload and high quality are both attained by this technique shows a stego picture with PSNR readings over 50 dB. The suggested method's very effective performance is attained by employing PVD to choose sharp sections for embedding that are less susceptible to alterations by the HVS. The distortion is also lessened by utilising a hamming code to hide sensitive information, which also increases the security of the embedded message as we compare to paper [18] in order to increase secrecy in the event of a remote medical examination, we employed image steganography to safely and covertly encode the patient's personal information in their medical images' diagnosis. The approximation coefficient of the integer wavelet transform's least significant bit is proposed. For both colour and grayscale images, this approach is examined. While IWT with R, B, and G component is used to conceal the secret picture in a colour image, IWT with LSB is used to conceal the hidden image in a grayscale image. By evaluating the mean square error and PSNR, one may determine the degree of distortion between the cover picture and stego-image, and one can quantify this degree of distortion using the normalised cross-correlation. The outcome demonstrates that the IWT-LSB approach can cover up long secret data with superior MSE, PSNR, and NCC.

A secure patient diagnostic data transfer approach combining both colour and grayscale photographs as a cover carrier for a healthcare-based IoT environment has been suggested in article [19]. The suggested model used a hybrid of AES and RSA cryptographic methods plus either 2D-DWT-1L or 2D-DWT-2L steganography. Different font sizes were used in the experiment, along with colour and grayscale graphics. On the basis of the six statistical indicators, the performance was evaluated (PSNR, MSE, BER, SSIM, SC, and correlation). The suggested model demonstrated its capability to conceal sensitive patient information into a sent cover image with high imperceptibility, capacity, and little degradation in the received stego-image when compared to state-of-the-art approaches. An SVD-based fragile watermarking approach employing the grouped block method is presented in this research [20] to increase security and offer an additional tool to identify the attacked regions inside various medical images. To resist the vector quantization attack, two authentication bits—block authentication and self-recovery bits—were utilised. By recovering the compromised region from nearby blocks using the Arnold transform, the recovered host's NCC and PSNR are finally improved. Our experimental findings demonstrated the suggested scheme's excellent reliability and ability to precisely locate the attacked blocks. Copy and paste attacks, content removal attacks, text addition attacks, and VQ attacks are all successfully avoided by the suggested technique. The suggested methodology significantly increases the PSNR of the self-recovered image and the tamper localization accuracy as compared to state-of-the-art methods. Additional testing is necessary to determine the effectiveness of our suggested solution with non-fragile

tampered photographs, despite the fact that it performed well when handling fragile tampered images.

Using the concept of indefinite quality and a decision tree with LSB's substitution, a novel mystery transmission technique is proposed in this [11] study alternative for sending the appropriate image of the medicine bearer combined with the secret therapeutic patient information. The sender distributes the secret information blocks arbitrarily to the transporter using a decision tree, which improves security standards and has a strong impact on the computation that is displayed. The proposed conspiracy makes use of the RSA cryptosystem to provide information privacy at the server farm. LSB replacements are used in steganography, together with a decision tree, to safeguard medical data. A decision tree shows a perfect division between corresponding groups to provide options. Results and histogram analysis show that PSNR, MSE values, and rate of highest concealment limit are superior to other existing plans, and that subtlety bending cannot be evaluated from the associated mystery therapy stego images. As opposed to paper [15], which proposes and introduces a model by integrating the two methods of elliptical curve cryptography and two different types of steganography (i.e.,1 LSB and 2 LSB). The private and secret information will be encrypted then hidden in a much better method than before with the help of two procedures [1, 18, 21]. Additionally, when employing or applying 2 LSB with an appropriate level of security, there was a discernible shift in the number of empty bits in the picture capacity. This benefits the receiver as well as the recorder to transfer more information and of the confidential information Keep anyone who isn't permitted to see or obtain this in your custody avoiding information [14, 16, 17] any unapproved person is not even made aware of the existence of any information.

An alternative secure communication model has been presented in this paper [13] that combines cryptography with steganography techniques to add an additional degree of security, preventing people from accessing plaintext while lacking the key to decrypt the ciphertext. The key images were first encrypted with the Secure Force-AES algorithmic program, and then the encrypted images were concealed in the cowl picture using JSTEG and LSB techniques. This combination allows the key image to transmit over an open channel because the cipher image does not appear nonsensical but is concealed by the use of steganography to hide it between the cover photos. PSNR and MSE, two parameters, are computed. We have a tendency to try and apply the anticipated methodology to audio and video at various points of the long run effort. Additionally, we are working to advance the predicted methodology's strength in order to develop the capability over it while maintaining a similar PSNR or greater whereas in [16] Paper. They provided a summary of the crypto-steganographic techniques now in use along with their advantages and disadvantages. We also emphasized the parallels and discrepancies among the crypto-steganographic techniques. The chosen strategy suggested by Juneja and Sandhu is then implemented, leading to the creation of a secure crypto-steganographic system for the healthcare industry. Several techniques have been used in this system, including a secure and reliable method that extracts edge and smooth areas from an image using hybrid feature detection, two-component LSB substitution to randomly embed secret messages in edge areas, adaptive LSB substitution to randomly embed secret messages in smooth areas, and the widely used AES encryption technique to encrypt messages before embedding. We also demonstrated how this approach resists the two types of steganalysis attacks: visual and statistical. Therefore, this crypto-steganographic system for healthcare was able to meet the fundamental requirements of steganography, such as imperceptibility, robustness, and capacity of hidden message, as well as the main objectives of cryptography, which protect the message confidentiality, integrity, and availability.

2.4OBJECTIVE OF THIS DISSERTATION

The objective is to develop an algorithm that combines cryptography and steganography techniques and use it in the healthcare industry to protect the confidentiality and privacy of sensitive data without significantly compromising patient's safety the level of medical imaging quality. In order to create a highly secure healthcare system, this work intends to increase the security of medical data transmission via the combination of a steganography approach with a hybrid encryption strategy.

The objective of this dissertation is to combine steganography with cryptography algorithms to create a new hybrid approach for data security. With the help of this technology, a secret message may be encrypted and embedded into a cover picture to achieve maximum imperceptibility, longevity, and little degradation of the received stego image. The major goals of this study were to:

- Create a security framework for steganographic concealing text data in images utilising LSB and DWT separately.
- Create a hybrid security solution that combines steganography (LSB and DWT) with data encryption (AES and RSA) to improve stego picture performance and data imperceptibility.
- Determine how well the created system secures and retrieves the original data.

CHAPTER 3

ANALYSIS, DESIGN AND MODELLING

3.1DETAILED DESCRIPTION

3.1.1 Proposed model

For the purpose of safeguarding the transmission of medical data in IoT contexts, this article suggests a healthcare security paradigm. The suggested model is made up of four ongoing processes:

- A suggested hybrid encryption technique that incorporates both the AES and RSA encryption algorithms is used to encrypt the private patient data.
- Using 2D-DWT-2L, the encrypted data is hidden under a cover picture, creating a stego-image.
- Extracting the embedded data.
- To get the original data, the extracted data is decrypted.

Cryptography is the process of converting messages into unmeaningful form order to ensure confidentiality it includes encryption and decryption. The Rivest-Shamir-Adleman (RSA) and Advanced Encryption Standard (AES) algorithms are primarily employed for data encryption. The same key is used on both sides of the symmetric encryption AES. It features keys that are either 128, 192, or 256 bits long and a set message block size of 128 bits of text (plain or encrypted). Longer messages are split into 128-bit pieces before transmission. Evidently, longer keys demand a lengthier encrypt and decrypt operation while simultaneously making the cipher harder to crack. The RSA, on the other hand, is a public key algorithm that is extensively used in both corporate and private communication. It benefits from a configurable key size that ranges from (2–2048) bits.

This study employs DWT steganography methods that work in the frequency domain at the 1, 2, and 3-level levels. It divided the picture into sections with high and low iterations. While the low iteration section is typically split into high and low iteration parts, the high iteration part contains edge information. The recommended approach employs an image cover as a data-hiding approach (colour and grayscale). To expose the message, the intended recipient merely needs to complete the necessary procedures; otherwise, the existence of the hidden information is essentially unnoticeable. The suggested technique differs from conventional data concealing algorithms in that it may hide information of a substantial quality.

3.1.2 Block diagram of Proposed system

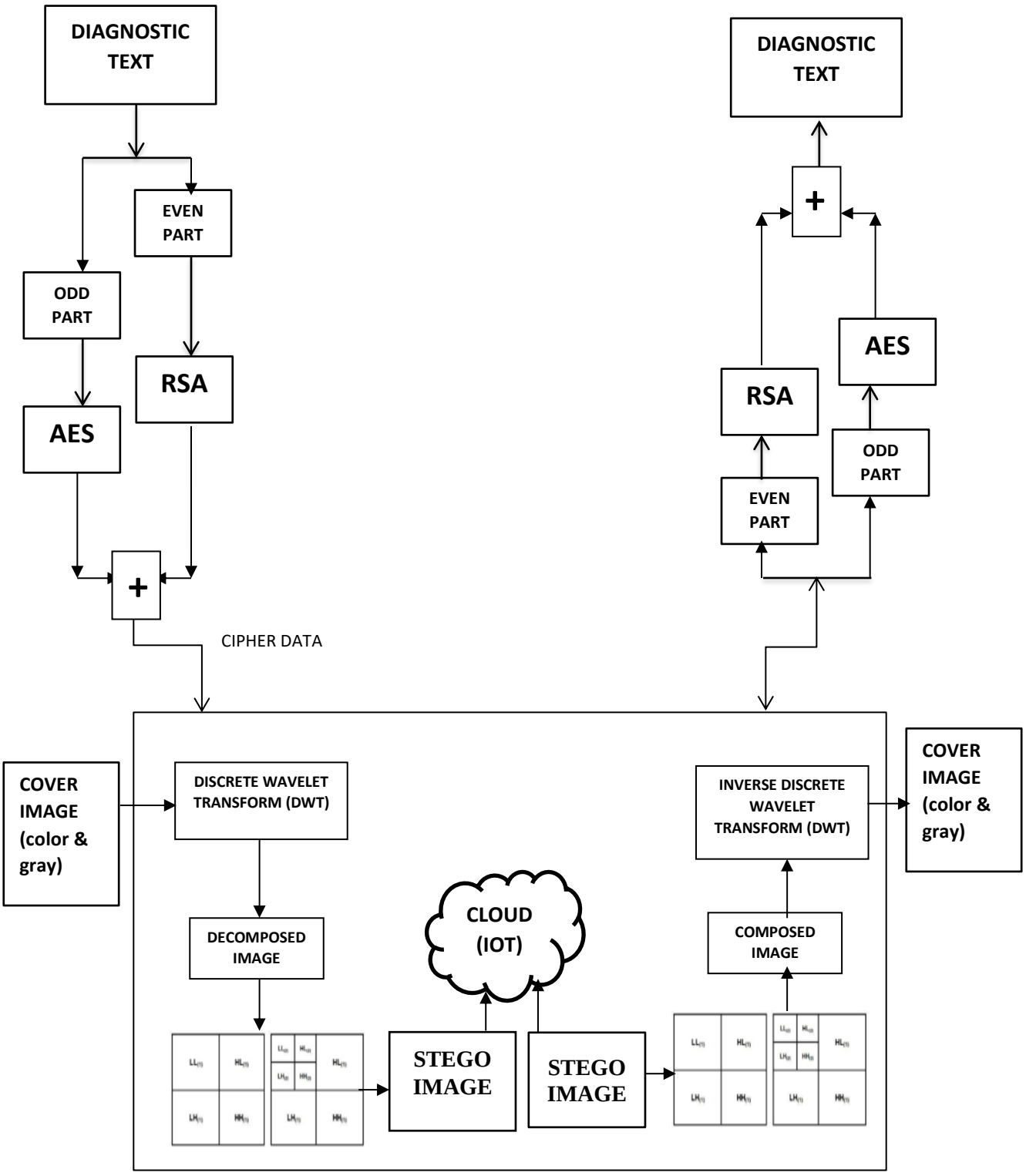


Figure 3.1.2.1 *Block diagram*

3.1.3 Flow chart

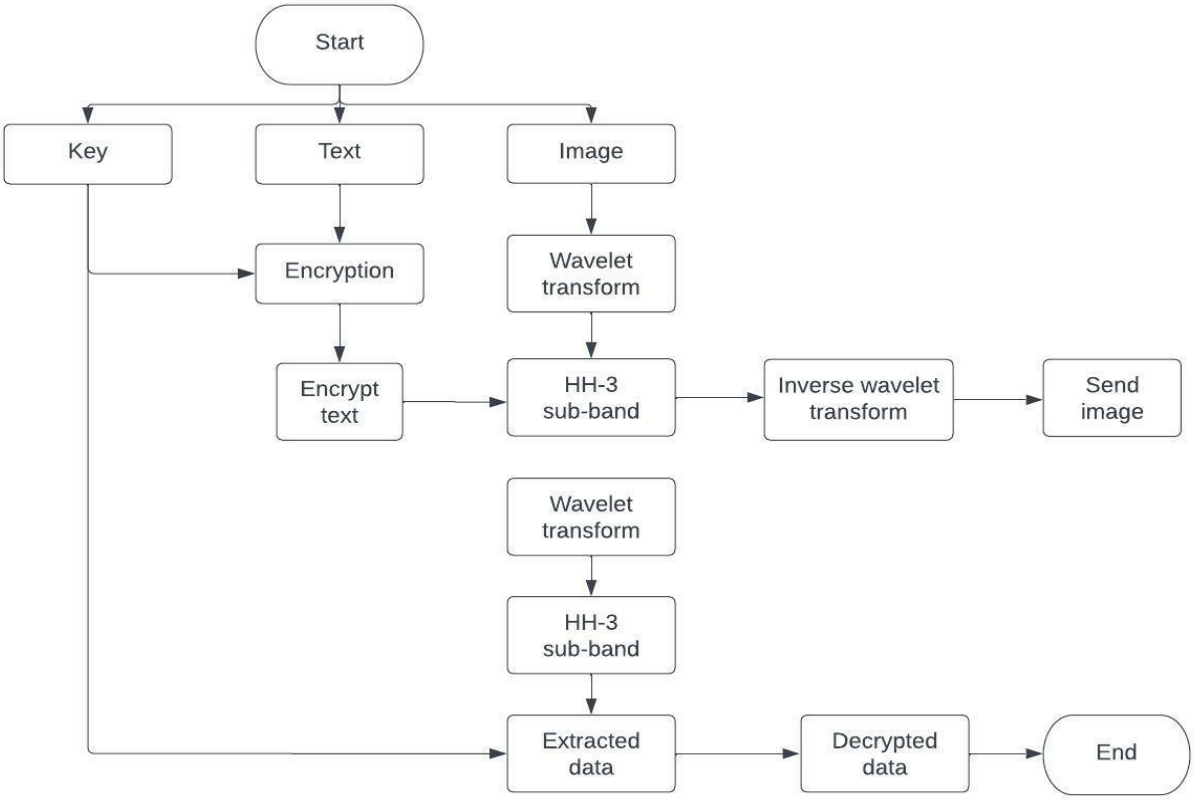


Figure 3.1.3.1 *Flow diagram of proposed system*

3.2DATASET

Select any image file, behind which the user wants to hide data. The image which is selected should have fixed height and width. Now save the image file as in jpeg extension and the image appears as an original image file.

3.3TOOLS

3.3.1 MATLAB

3.3.1.1 Introduction to MATLAB

The numerical computing environment and fourth-generation programming language is called MATLAB (matrix laboratory). Matrix manipulation, function and data visualization, algorithm implementation, user interface design, and interface interaction with programs written in other languages, such as C, C++, Java, and Fortran, are all possible with MATLAB, a tool created by Math Works.

The MuPAD symbolic engine is used by an optional toolbox in MATLAB, which is primarily designed for numerical computing but also has access to symbolic computing capabilities. Graphical multi-domain simulation and Model-Based Design for dynamic and embedded systems are added by an extra program called Simulink.

In 2004 there were about a million users using MATLAB in both business and academia. Users of MATLAB come from a variety of engineering, scientific, and economic backgrounds. Both academic and research institutions, as well as commercial businesses, frequently utilize MATLAB. Control engineering, Little's area of expertise, was where researchers and practitioners first began using MATLAB, but it swiftly expanded to many other fields. It is increasingly widely used in academia, particularly for the instruction of linear algebra and numerical analysis, and is well-liked by researchers who work on image processing. The MATLAB language is the foundation of the MATLAB program. Typing MATLAB code into the Command Window, one of the components of the MATLAB Desktop, is the easiest way to run it. MATLAB may be utilized as an interactive mathematical shell when code is input in the Command Window. In order to expand the available commands, sequences of instructions can be stored in a text file using the MATLAB Editor as a script or included within a function. A variety of tools are available in MATLAB for recording and sharing your work. You may distribute your MATLAB algorithms and applications as well as combine your MATLAB code with other languages and software.

- Toolbox for Image Processing:

The image processing toolbox enables the execution of picture enhancement, image deblurring, characteristic identification, noise reduction, image segmentation, arithmetical alteration, and image registration.

- Both fundamental import and export operations:

Basic import and export functions allow for the import and export of images from a variety of image acquisition systems, including digital cameras, telescopes, microscopes, satellite and airborne sensors, CT and MRI scanners, and other scientific instruments. Therefore, such images can be viewed, analysed, and processed into a variety of data formats, including single-accuracy, double-accuracy, and 8-bit, 16-bit, and 32-bit integers that can be signed or unsigned. Image read-write operations are commonly carried out through import and export routines.

- Display capability

The photos that are understood by the import purpose are typically illustrated for display purposes. This function enables the creation of presentations using text and graphics, images in a specific window, and specialised displays like an outline plot, a histogram, and so on.

- Thresholding

A straightforward approach for segmenting images is thresholding. Thresholding can be used to create binary images just like a grayscale image. The input image's intensity that is less than the threshold value will be displayed as black (intensity is zero) in the thresholding section, and the remaining intensities will be converted to white (intensity is one) and then displayed. The goal of this process is to produce the segmented image.

3.3.1.2 Features of MATLAB

- High-level language for technical computing.
- A development environment for controlling files, data, and code.
- Interactive resources for iterative design, exploration, and problem-solving.

- Mathematical operations for numerical integration, filtering, optimization, Fourier analysis, statistics, and linear algebra.
- Graphics tools for data visualization in 2-D and 3-D.
- Instruments for creating unique graphical user interfaces.
- Integration functions for MATLAB-based algorithms with third-party software and coding languages, including C, C++, Fortran, JavaTM, COM, and Microsoft Excel.

Signal and image processing, communications, control design, test and measurement, financial modelling and analysis, and computing are just a few of the many fields in which MATLAB is employed. The MATLAB environment is extended by add-on toolboxes (collections of specialized MATLAB functions) to address specific kinds of issues in certain application areas.

Personal PCs, sophisticated server systems, and the Cheaha computing cluster can all run MATLAB. The language may be expanded with parallel implementations for usual computational operations, such as for-loop unrolling, with the addition of the Parallel Computing Toolbox. This toolkit also enables the offloading of computationally demanding jobs to the campus compute cluster Cheaha. One of the few programming languages where each variable is a matrix (in the broadest sense) and "knows" how big it is is MATLAB. Additionally, where necessary, the basic operators (such as addition and multiplication) have been coded to cope with matrices. And much of the tedious housekeeping that makes all this possible is handled by the MATLAB environment. Because matrices are used in so many of the Macro-Investment Analysis techniques, MATLAB is a very effective language for both communication and execution.

3.3.1.3 Interfacing with other languages

Functions and subroutines developed in the C programming language or FORTRAN can be called by MATLAB. The creation of a wrapper function enables the passing and returning of MATLAB data types. "MEX-files" are dynamically loadable object files produced by such functions (for MATLAB executable).

Direct library calls from MATLAB are possible for libraries written in Java, ActiveX, or.NET, and many MATLAB libraries (such as XML or SQL support) are developed as wrappers over Java or ActiveX libraries. It is more difficult to call MATLAB from Java, although it is possible via Math Works' MATLAB extension or a less-documented technique dubbed JMI (Java-to-Mat lab Interface), which should not be mistaken with the unrelated Java that also goes by the same name. MATLAB may be linked to Maple or Mathematica as an alternative to Math Works' MuPAD-based Symbolic Math Toolbox.

To import and export MathML, libraries are also available.

- Development Environment

Start-up Accelerator for network installations and speedier start-up of MATLAB on Windows, particularly Windows XP. A spreadsheet import tool with greater selection and loading options for mixed text and numeric data. Automatic variable and function renaming in the MATLAB Editor. Readability and navigational enhancements for warning and error messages in the MATLAB command window.

- Creating Applications and Algorithms

Your algorithms and applications may be developed and analysed fast with the help of MATLAB's high-level language and development tools.

- Development Devices

You may efficiently implement your method using the development tools provided by MATLAB. They consist of the following:

- MATLAB studio

Setting breakpoints and single stepping are only a couple of the usual editing and debugging options offered by the MATLAB.

- Code Analyst

checks your code for issues and makes suggestions for changes to improve performance and maintainability.

- MATLAB Tester

The time taken to execute each line of code is recorded by MATLAB PROFILER.

- Database Reports

Report on code effectiveness, file differences, file dependencies, and code coverage after scanning every file in a directory.

3.3.1.4 Designing Graphical user interfaces

By laying out, designing, and editing user interfaces using the interactive GUIDE (Graphical User Interface Development Environment) tool. With GUIDE, you may add MATLAB plots, Microsoft ActiveX controls, list boxes, pull-down menus, push buttons, radio buttons, and sliders. As an alternative, you may use MATLAB routines to programmatically generate GUIs.

3.3.1.5 Environment for Development

You may utilise MATLAB functions and files with the aid of this group of tools and resources. The user interfaces for many of these programmes are graphical. It has browsers for reading help, the workspace, files, and the search path in addition to the MATLAB desktop and Command Window, a command history, and these features.

- The Mathematical Function Library for MATLAB

There are many different types of computational algorithms included in this, from simple ones like sum, sine, and cosine to more complicated ones like matrix inverse, eigenvalues, Bessel functions, and rapid Fourier transformations.

- The language of MATLAB.

This is a high-level matrix/array language with features for object-oriented programming, control flow statements, functions, data structures, input/output, and input/output. It enables "programming in the tiny" to quickly produce shoddy throw-away programmes as well as "programming in the huge" to fully develop substantial, intricate application applications.

- Work with graphics.

instructions for image processing, animation, two- and three-dimensional data visualisation, and presentation graphics. Additionally, it has low-level instructions that enable you to create completely functional graphical user interfaces for your MATLAB programmes as well as fully alter the appearance of visuals.

3.3.1.6 The Application Program Interface for MATLAB (API)

This library enables you to create FORTRAN and C applications that communicate with MATLAB. It includes tools for reading and writing MAT-files, invoking MATLAB as a computational engine, and dynamically connecting MATLAB functions.

- Command window

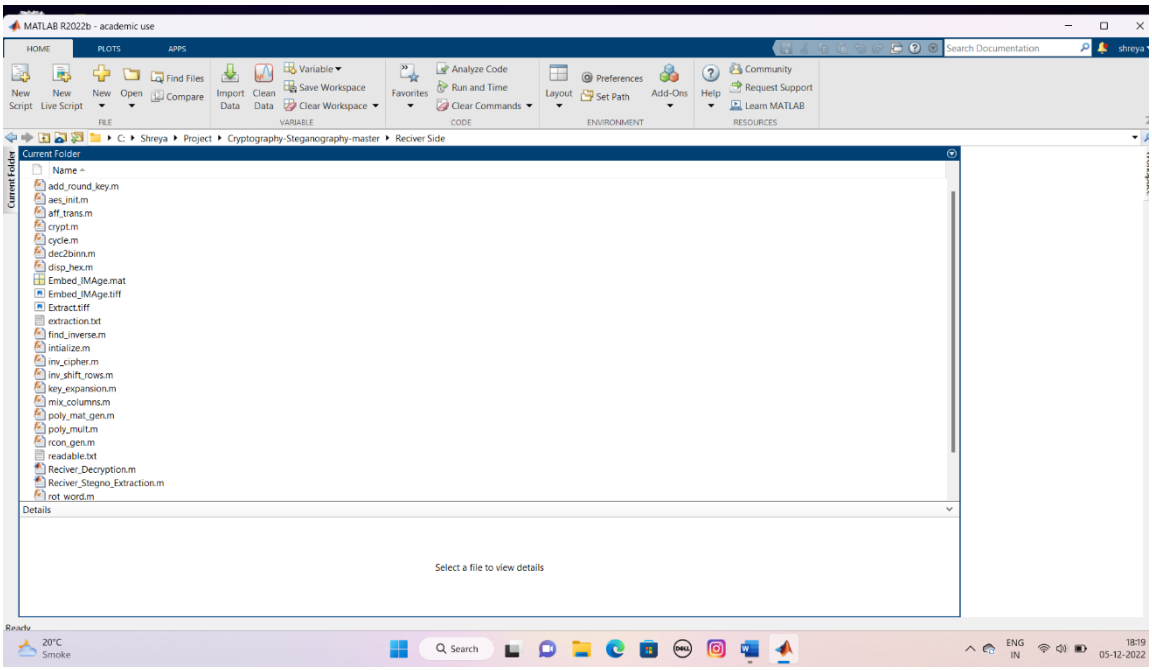


Figure 3.3.1.1 *Command window*

- Command Priority

The Command History window keeps track of the lines you type in the Command Window. You may inspect previously used functions as well as copy and run certain lines from the Command History. Use the diary function to record the input and output from a MATLAB session to a file.

- Run Third-Party Programs

From the MATLAB Command Window, external programmes may be launched. The exclamation point character! is a shell escape and tells the operating system that the remaining characters on the input line are commands. This is helpful for starting other applications or

utilities without closing MATLAB. The operating system regains control to MATLAB when you end the external software.

- Launch Pad

The Launch Pad in MATLAB makes resources, presentations, and documents available.

- Browser Support

To search for and access documentation for all of your Mat Works products, use the Help browser. The MATLAB desktop includes a built-in Web browser called the Help browser that shows HTML documents.

Click the help button in the toolbar or enter help browser in the Command Window to launch the Help browser. The Help Navigator, which you use to discover information, and the display pane, which shows the information, are the two panes that make up the Help browser.

- Navigator Help

Use Navigator to Help to discover information. It contains:

- Filtering by product

Make sure the filter is set to only display documentation for the goods you choose.

- Tab for contents

View the documentation for your items' titles and tables of contents.

- Page Index

Find particular index entries (chosen keywords) for your items in the MathWorks documentation.

- Tab for Search

Look in the documentation for a certain word or phrase. Set the Search type to Function Name to access help for a specific function.

- Bookmarks tab

View a list of the papers you have marked as favourites in the past.

- Display Window

View the documentation on the display window after discovering it using the Help Navigator. You can: View the documentation while it is open.

- Visit other pages

Use the toolbar's back and advance buttons or the arrows at the top and bottom of the pages to navigate.

- Save webpages

In the toolbar, select the Add to Favourites button.

- Print out pages

The toolbar's print button should be clicked.

- Look for a phrase on the page

In the toolbar's Find in page field, enter a keyword, then click Go. The display pane also has options for copying data, analysing a selection, and visiting websites.

3.3.1.7 Desktop tools

The desktop tools of MATLAB are introduced in this section. The majority of the capabilities present in desktop programmes may also be accomplished using MATLAB functions. The following tools are available:

- Current Directory Browser
- Workspace Browser
- Array Editor
- Editor/Debugger
- Command Window
- Command History
- Launch Pad and
- Help Browser

i. Request Path

MATLAB employs a search path to locate M-files and other MATLAB-related files, which are arranged in directories on your file system, to figure out how to execute functions you call. The current directory or a directory on the search path must contain any file you wish to launch in MATLAB. The files included with the MATLAB and MathWorks toolboxes are automatically added to the search path.

ii. Workspace Browser

The variables (named arrays) accumulated during a MATLAB session and kept in memory make up the MATLAB workspace. Using functions, executing M-files, and loading stored workspaces are all ways to add variables to the workspace. Use the workspace browser or the who and who's functions to explore the workspace and details about each variable.

Select the variable, then choose Delete from the Edit menu to remove it from the workspace. Use the clear function instead.

When the MATLAB session is over, the workspace is not kept up to date. Choose Save Workspace as from the File menu or use the save function to save the workspace to a file that can be accessed during a subsequent MATLAB session. By doing this, the workspace is saved to a binary file with the Mat extension known as a MAT-file. Options exist for saving in several formats. Choose Import Data from the File menu or use the load function to read in a MAT-file.

iii. Editor for Arrays

To view a variable in the Array Editor, double-click on it in the Workspace browser. In the workspace, strings, cell arrays of strings, and one- or two-dimensional numeric arrays may all be viewed and edited visually using the Array Editor.

iv. Editor/Debugger

Create and debug M-files, which are programmes you build to run MATLAB functions, using the Editor/Debugger. The Editor/Debugger offers a graphical user interface for M-file debugging in addition to simple text editing. Any text editor, such as Emacs, may be used to produce M-files, and settings (found in the desktop File menu) can be used to choose that editor as the default. If you use another editor, you may still debug your code using the MATLAB Editor/Debugger or debugging tools like dbstop, which creates a breakpoint.

You can use the type function to show an M-contents files in the Command Window if all you need to do is look at them.

3.3.1.8 Data Analysis and Access

The whole data analysis process is supported by MATLAB, including data collection from external devices and databases, pre-processing, visualisation, and numerical analysis, as well as the creation of output suitable for presentations.

i. Data anatomy

MATLAB offers command-line functions and interactive tools for data processing tasks like:

- Correlation,
- Fourier analysis
- Filtering
- 1-D peak, valley
- Zero discovery
- Basic statistics and curve fitting
- Thresholding and smoothing
- Extracting parts of data
- Scaling, and Averaging
- Matrix analysis

ii. Information access

Accessing data from files, other programmes, databases, and external devices is simple and effective using MATLAB. You can read data from common file types including Microsoft Excel, ASCII text or binary files, picture, music, and video files, as well as HDF and HDF5 scientific file types. You can work with data files in any format thanks to low-level binary file I/O methods. Additional features enable you to read data from XML and Web sites.

iii. Data visualization

In MATLAB, you may access every graphic element needed to visualise engineering and scientific data. These comprise tools for interactively building plots, 2-D and 3-D graphing, 3-D volume visualisation, and the ability to export outcomes in all widely used graphics formats.

Plots may be altered by adding additional axes, altering line and marker colours, adding commentary, Latex equations, and legends, as well as by sketching shapes and multiple axes.

Plotting in 2D

Using 2-D plotting tools to generate:

- line, area, bar, and pie charts from data vectors
- Plots of direction and speed.
- Histograms.
- Surfaces
- Polygons
- Bubble/scatter plots
- Animations.

Volume visualization and 3D plotting

3-D scalar and 3-D vector data, as well as 2-D matrices, may all be shown using MATLAB tools. These features may be used to display and comprehend vast, frequently complicated, multidimensional datasets. describing the plot's elements, such as the camera's perspective, the lighting effect, the placement of the light sources, and transparency. There are various types of 3-D charting functions:

- Surface
- Contour
- Mesh.
- Picture plots
- Conical
- Slice
- Stream

3.4FUNCTIONAL / NON- FUNCTIONAL REQUIREMENTS

In order to develop the system, the necessary information was extracted to create the system requirement specifications. The system needs to achieve the elaborative criteria. Additionally, the SRS provides a thorough understanding of the system, enabling users to comprehend the project's intended outcomes without being constrained by any specific methods. While hiding the strategy, this SRS withholds information from other parties.

3.4.1 Hardware Requirements

The required hardware for a personal computer includes the following configuration:

1. Processor: Intel core i5.
2. Disk capability: 1GB for MATLAB only.
3. RAM: 4GB.

3.4.2 Software Requirements

The programme required for a personal computer with the following configuration:

1. Windows 11 (64-bit) operating system.

2. MATLAB 9.13.0.2049777 (R2022b)

3.5 RISK ANALYSIS

3.5.1 Choosing right kind software

The research trials are an important activity because picking the wrong software might lead the research in the wrong direction and have a significant negative impact on the research job. As a result, great care is made to select the proper software. Windows 11 is the utilized operating system.

3.5.2 Choosing right kind of images

The first and most important stage in steganography is selecting the appropriate pictures since even a slight change in an image after embedding might draw the notice of hackers, which could lead to data destruction or modification.

CHAPTER 4

IMPLEMENTATIONS AND RESULTS

4.1 IMPLEMENTATION

4.1.1 Data Encryption Scheme

The presented method carries out the cryptographic system. Encryption and decryption procedures make up the cryptographic system. The plain text T is separated into odd and even portions throughout the encryption process. Using a secret public key, odd component is encrypted using the AES algorithm. Even sections are encrypted using the RSA algorithm and a secret public key called m. the receiver side's usage of private key x during the decryption procedure. The Advanced Encryption Standard (AES) is a symmetric encryption method in which both the sender and the receiver can use the same key for encryption and decryption. We can employ AES with lengths of 128, 192, or 259 bits, each of which has 2128, 192, or 2256 combinations. The key itself maintains authentication while safeguarding the confidentiality that it maintains. Both keys in this have to be kept a secret. But it is difficult to decipher the encrypted text without knowing the private key or at least additional information. Finding the secret key with the aid of the public key and algorithm must be impossible. One key, the private key for encryption, is all that is required to provide the secrecy and authenticity we need. DES and AES are two cryptographic systems that offer security, but from the perspective of cryptography, they vary in that one is symmetric and the other is asymmetric.

AES keys are more difficult to crack than DES keys, yet both need more key distribution between sender and recipient. The National Institute for Standards and Technology (NIST) in the United States has established the Advanced Encryption Standard (AES) as a cryptographic standard. It is the outcome of a 1997 competition. The NIST has urged current parties across the world to submit suggestions for new standards. He was expected to support a block size of at least 128 bits in all submitted ideas, and the three primary volumes must be made up of 128, 192, and 256 bits. The Rijndael Algorithm, created by Joan Daemen and Vincent Rijmen, was selected as the winner three years later. AES's final standard was introduced in 2001. shows how the block cypher operation works. The Rijndael algorithm's simplicity and ease of hardware and software implementation were key factors in its success. Asymmetric cryptography uses the RSA algorithm. Asymmetric really implies that it utilizes both the public and private keys, which are two separate keys. As implied by the name, the private key is kept secret while the public key is distributed to everyone.

Asymmetric cryptography illustration:

1. A client (such as a browser) contacts the server and requests certain data while sending the server its public key.
2. The server uses the client's public key to encrypt the data before sending it.
3. The data is delivered to the client, who decrypts it.

The concept of RSA is based on the fact that big integers are hard to factor. The public key is made up of two numbers, one of which is the product of two enormous prime numbers. The same two prime numbers are also used to create the private key. Therefore, the private key is compromised if someone is able to factorize the huge integer. As a result, the key size completely determines how strong an encryption is, and doubling or tripling the key size

significantly boosts encryption strength. RSA keys may normally be 1024 or 2048 bits long, however experts think that keys with 1024 bits could be decoded soon.

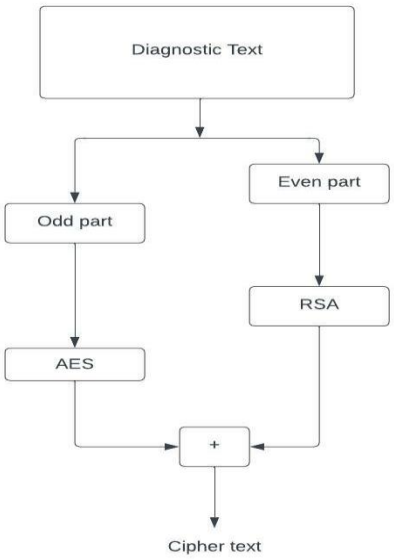


Figure 4.1.1.1 *Data encryption scheme*

4.1.2 Embedding Procedure

The A Haar-DWT was used in this procedure. With regard to Haar-DWT, 2D-DWT-3L may be formulated as a sequential transformation that applies low-pass and high-pass filters along the image's rows before the outcome is deconstructed along the image's columns. A high-high (HH), a high-low (HL), a low-high (LH), and a low-low (LL) frequency band are used as examples of the elemental breakdown process for a cover picture of a size N * M.
The stenographic system is used in the suggested model. The operations of embedding and extraction think up the stenographic scheme. A cover picture C and a secret text message T are inputs into the embedding process, which produces a stego-image S. While the embedded message is conversely extracted throughout the extraction procedure. The secret text is converted to ASCII during the embedding procedure and then cloaked in diagonal coefficients determined by HH3. The algorithm that evolved 2D-DWT-3L is employed in the embedding process.

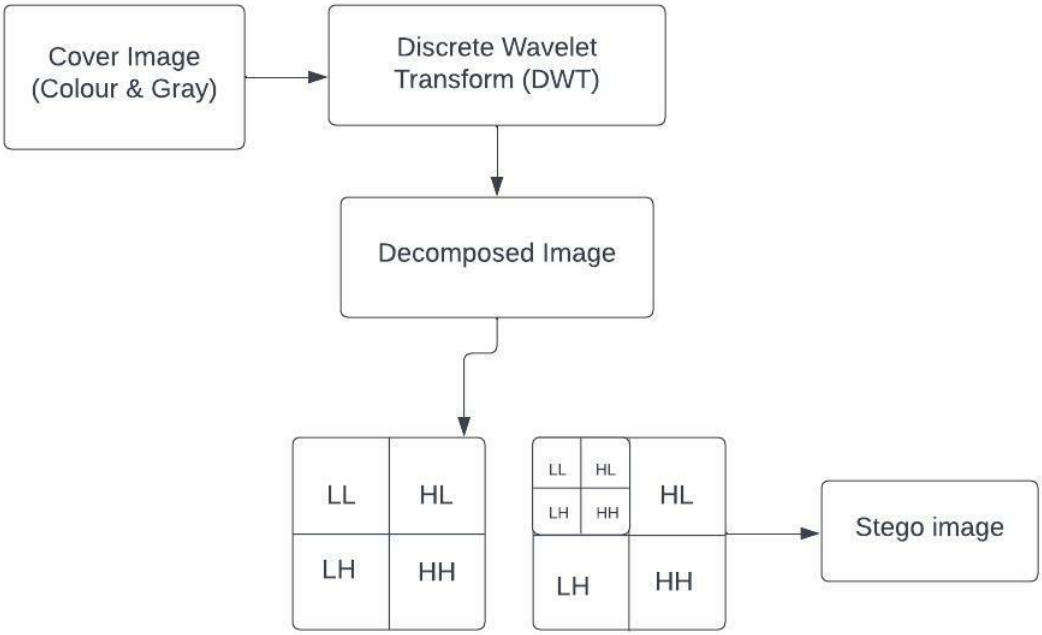


Figure 4.1.2.1 *Steganography scheme*

4.1.3 Extraction Procedure

The 2DDWT-3L approach is used to extract the secret message and retrieve the cover image after the text has been included into the cover image. The cover picture is created from the approximate reconstruction after the secret text message has been retrieved by first calling the idwt2 for the first level and then for the second level.

4.1.3.1 Discrete Wavelet Transform

Any wavelet transforms for which the wavelets are uniformly sampled is known as a discrete wavelet transform (DWT). One of the frequency domains where steganography can be used is represented by it. A coding error results in discontinuity between blocks when using the Discrete Cosine Transform (DCT) approach, which results in unappealing blocking artefacts. Because DWT is applied to the entire image, this shortcoming of DCT is lessened when employing it. Without any blocking artefacts, DWT offers superior energy compaction than the DCT. the following filters:

1. High pass filter (H): Loss of low frequency information results in the retention of high frequency information in the pixel.
2. Low pass filter (L): In contrast to a high pass filter, a low pass filter retains pixels with low frequency information.

In order to effectively deconstruct the signal, it is split into two parts: a detailed part (high frequency) and an approximation part (low frequency), as shown in The visual signals are divided into four sub band images (LL, LH, HL, and HH) at Level 1 Detail, which represent the average horizontal and vertical information. Each sub band at level 2 is thus split into four further sub bands.

The secret message can be concealed in the other three sections without changing the LL sub band since human eyes are more sensitive to the low frequency part (LL sub band). Because the other three sub bands are high frequency sub bands and consequently include insignificant data, hiding secret data in them doesn't significantly reduce the quality of the image. As a result, when computing with a cascade of filters and factor 2 subsampling, multiple methods can be used to enhance the features in different frequency domains.

4.1.4 Data Decryption scheme

Decryption is the process of returning encrypted data to the user in a format that is familiar to them; it is the opposite of the encryption process. Throughout the encryption procedure, the cipher-text must be protected with the same key that was used by the sender.

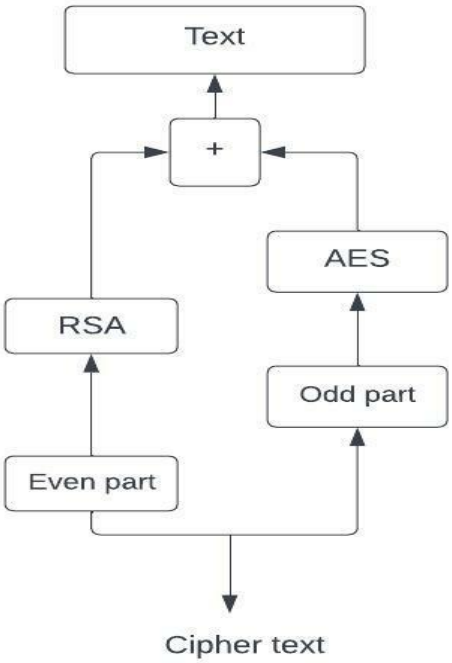


Figure 4.1.4.1 *Decryption scheme*

4.1.5 Proposed Algorithm

Algorithm 1: AES and RSA algorithm

The plain text T is separated into even and odd sections throughout the encryption process, respectively. T-ODD is encrypted with the AES utilising a set of private public keys. T-EVEN is encrypted with the RSA using the secret public key m.

Algorithm 2: 2D-DWT-2L Algorithm

1. HAAR-DWT: Low-pass and high-pass filters can be used to create the consecutive transformation known as 2D-DWT-2L.
2. Least significant bit:
    a) Determine the pixel's value.
    b) Transform it into its corresponding binary form.
    c) Correctly adjust the least significant bit.

4.1.5.1 Convert plain text to cipher text

A block cypher is AES. It processes a block of bits in plain text and outputs encrypted text of the same size. This algorithm has been run through 10/12/14 rounds. The byte substation, mixed columns, shifted rows, and add round key are all included. Each byte is replaced using a 16x16 byte table that has a permutation of all the supplied values. The byte indexed with row and column replaces each state byte. Circular bytes are utilised in shift rows. Shift in each row, keeping the first row intact while shifting the second row by one byte to the left and the third row by two bytes to the left. It can also process and decrypt inverts by shifting each row one byte to the right. Each column in the mix columns is broken down and analysed, and each byte is replaced with a value that depends on every byte in the column. Additionally, the round key is an XOR state with a key length of 128 bits that is processed by column and inverse for decryption. Since the steps are carried out in reverse order, AES decryption is not the same as encryption, but it is defined as an equivalent inverse cypher with the same steps as encryption by using the opposite of each step with a different key.

1. Choosing a file for an image:

Choose an image file that the user wishes to conceal data behind first. The chosen picture should have a set height and width. When you save the picture file as a jpeg, it becomes an authentic image file.

4.1.5.2 Image Steganography

1. Sender's Side

The sender will choose the JPEG extension-format original picture for this. The sender has since used the "imread" method to read the file. Additionally, use the "rgb2gray" function to convert the picture file from RGB to grey. The text should then be read and converted to binary format. The text is then converted to an encrypted format after the key has been read. while using a wavelet transformation. The picture may be divided into the LL, LH, HL, and HH sub bands. The LL Sub band must be used for the binary cypher. The image may be returned to its original size by using the inverse wavelet transformation function. And the recipient receives the image.

3 Stego Image file creation:

Utilizing digital watermarking, join the stegno text and stegno picture files to create the stegno image file. This creates the stego image text file on the transmitter side, which contains concealed content.

2. Receiving Side:

The text file is turned into an image when it is read by the receiver using "fread." Apply the wavelet transformation function for this receiver and split the picture into four sub bands as LL, LH, HL, and HH. Select the necessary LL sub band from the picture at this time. The code from the picture is extracted using extractionfun2 (), converted to hexadecimal format, and then stored in the variable "extra1". The code has now been decrypted.

4 Image Restoration:

The text file is opened with the fopen function and stored in the variable "fid," while the image file is read by the "imgread" function. It is saved into the variable "a" using the fread function. Now use matrix representation to transform the text file into an image file. Here, the matrix is put into the appropriate sub band, i.e., LL, LH, HL, HH, in order to conduct various additions and subtractions on it. The text can be used to restore the image.

4.2 RESULTS

4.2.1 Data Encryption

Even parts are encrypted using the RSA algorithm and a secret public key called m.

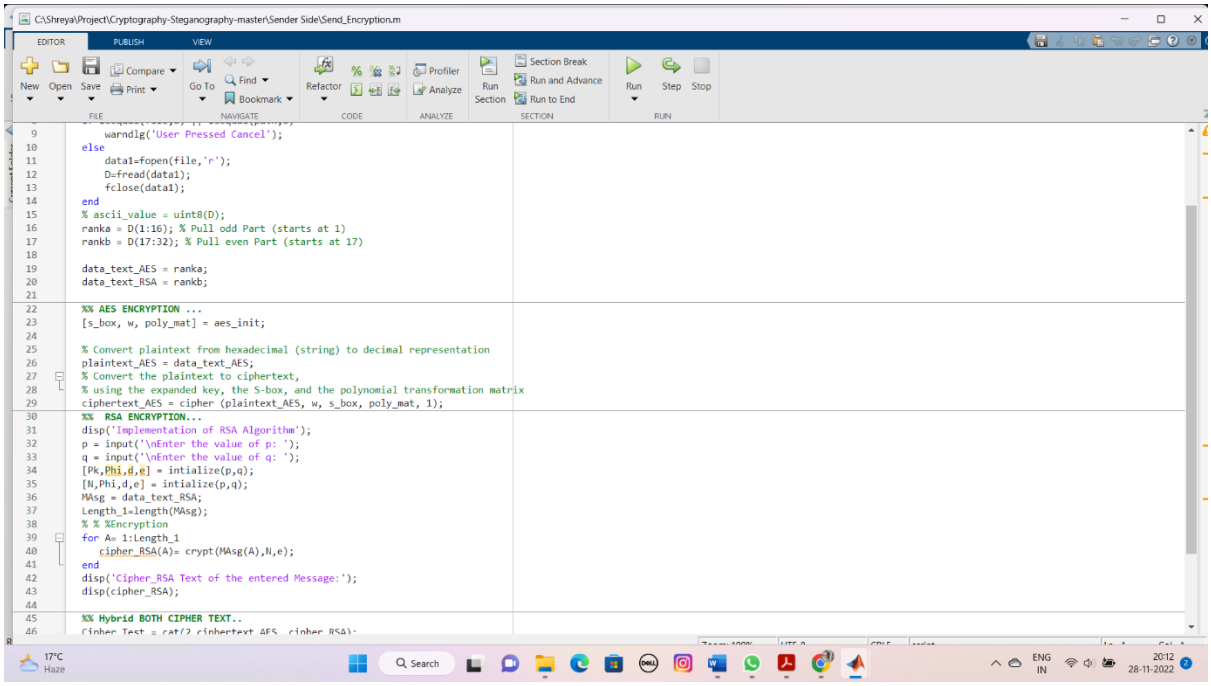


Figure 4.2.1.1 *Encryption code*

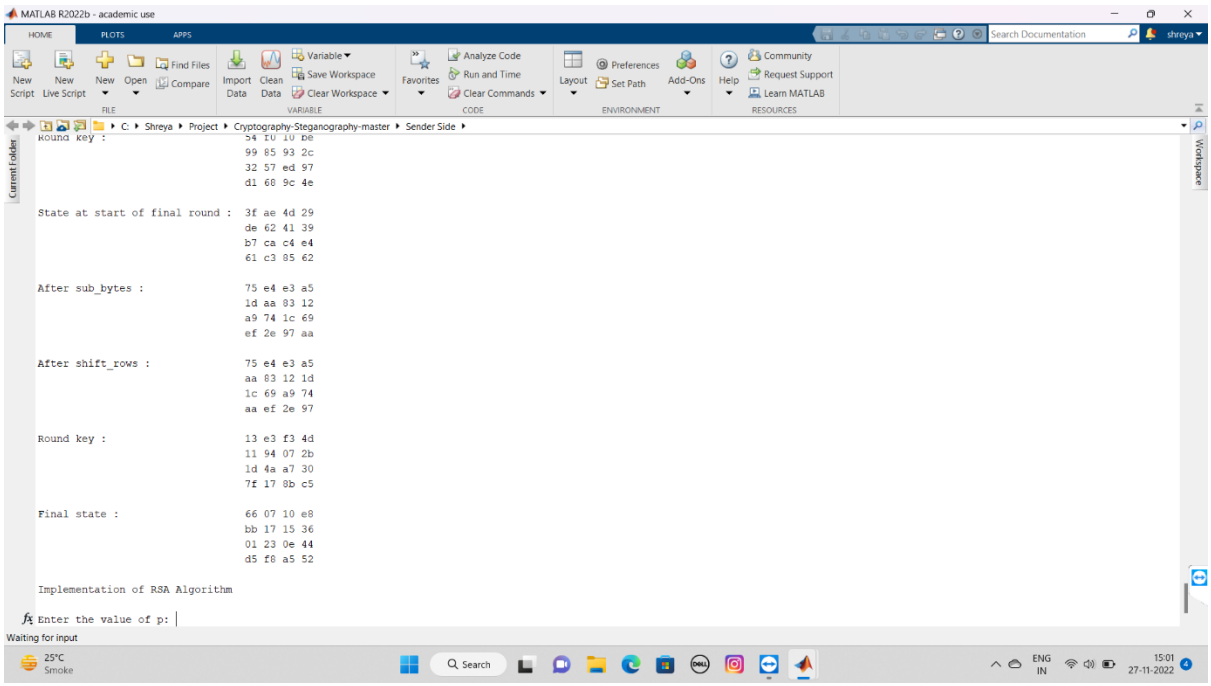


Figure 4.2.1.2 *Encryption process*

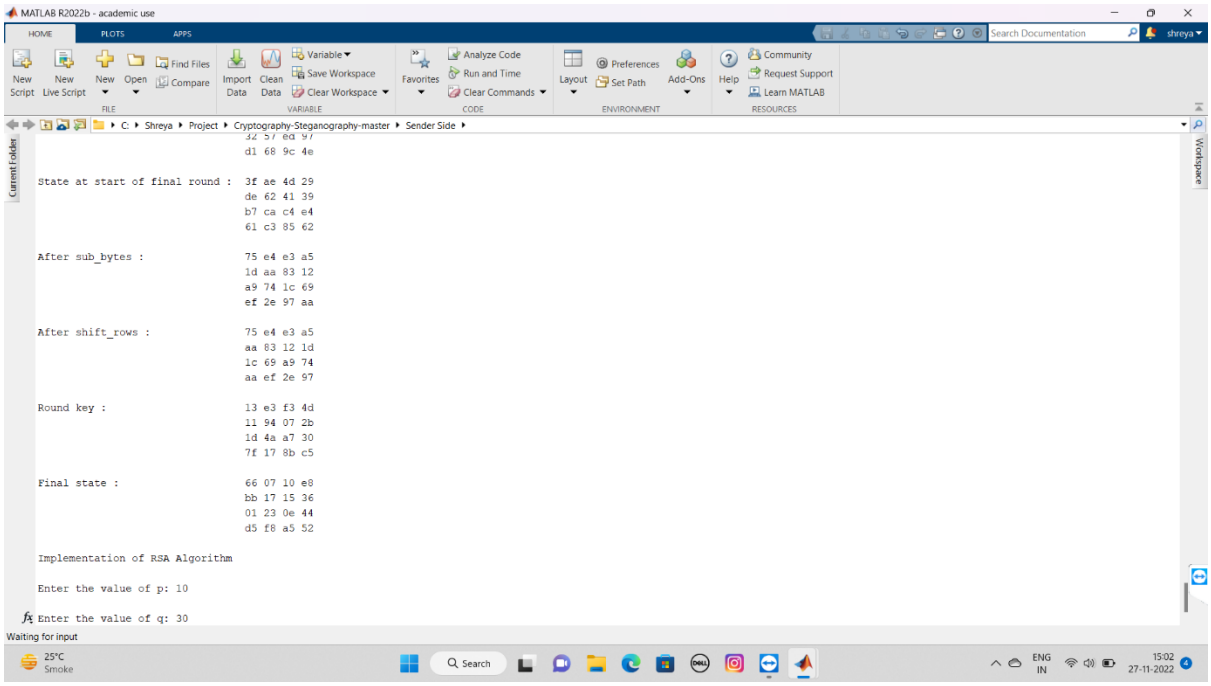


Figure 4.2.1.3 *Input key value*

Select Text to encrypt

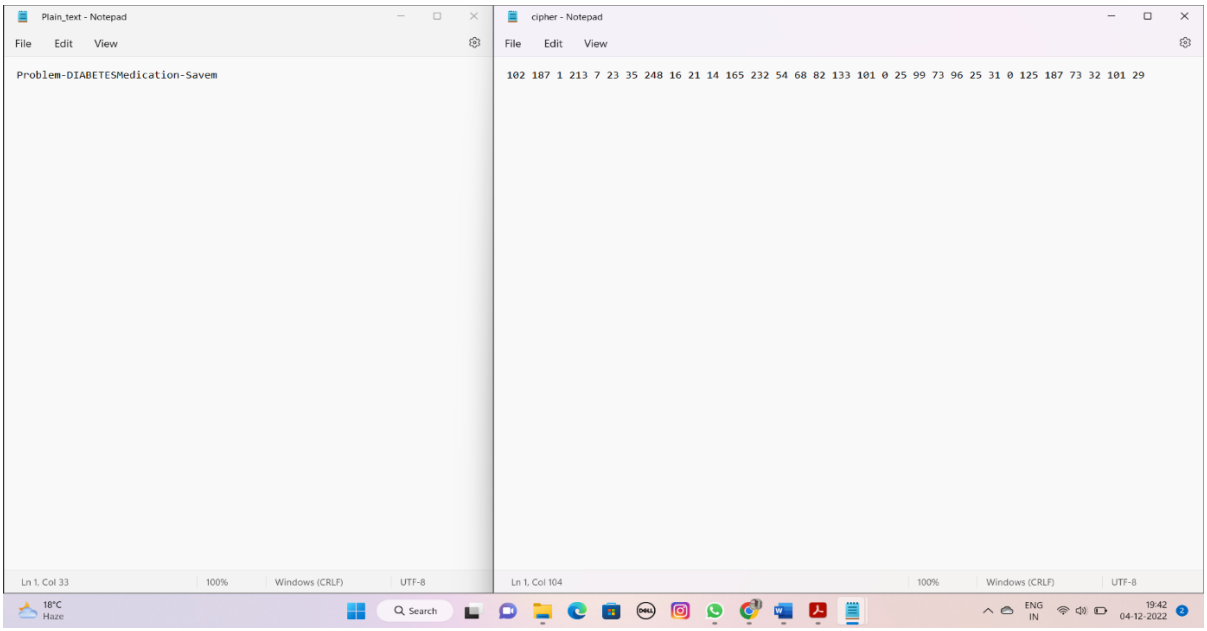


Figure 4.2.1.4 *Plain and cipher text*

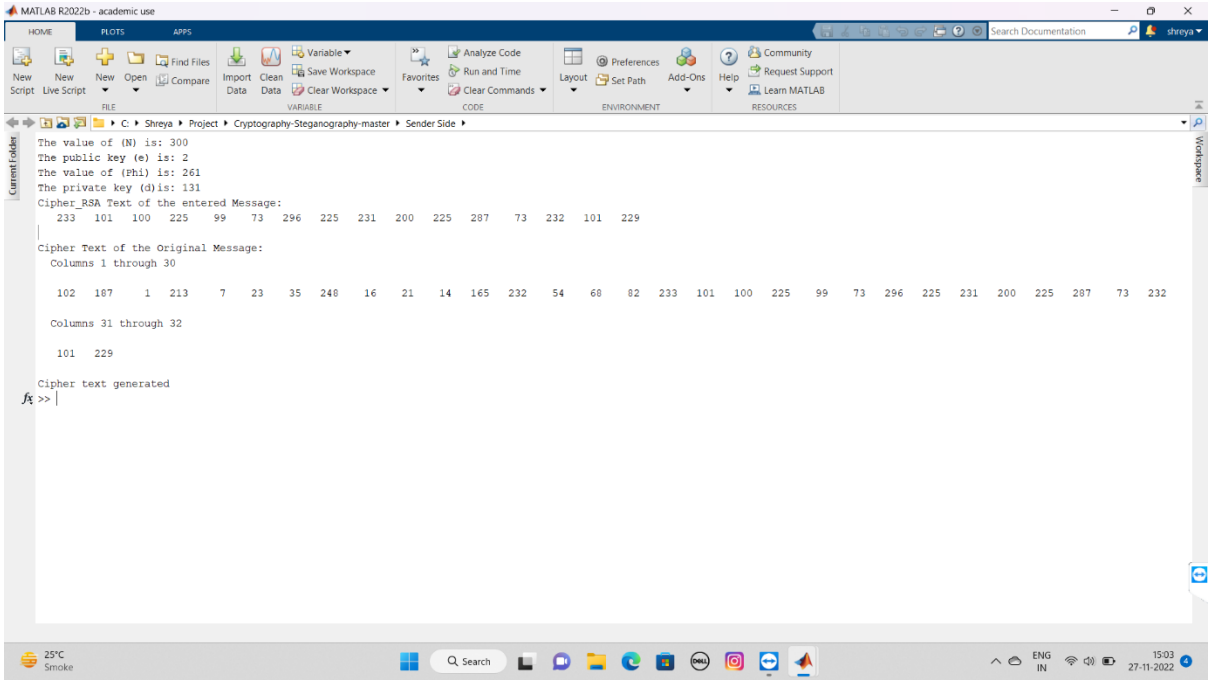


Figure 4.2.1.5 *Cipher text generated*

4.2.2 Image Steganography

The sender will choose the JPEG extension-format original picture for this. The sender has since used the "imread" method to read the file [7]. Additionally, use the "rgb2gray" function to convert the picture file from RGB to grey. The text should then be read and converted to binary format. The text is then converted to an encrypted format after the key has been read. while using a wavelet transformation. The picture may be divided into the LL, LH, HL, and HH sub bands. The LL Sub band must be used for the binary cypher. The image may be returned to its original size by using the inverse wavelet transformation function. And the recipient receives the image.

- Sender’s side:

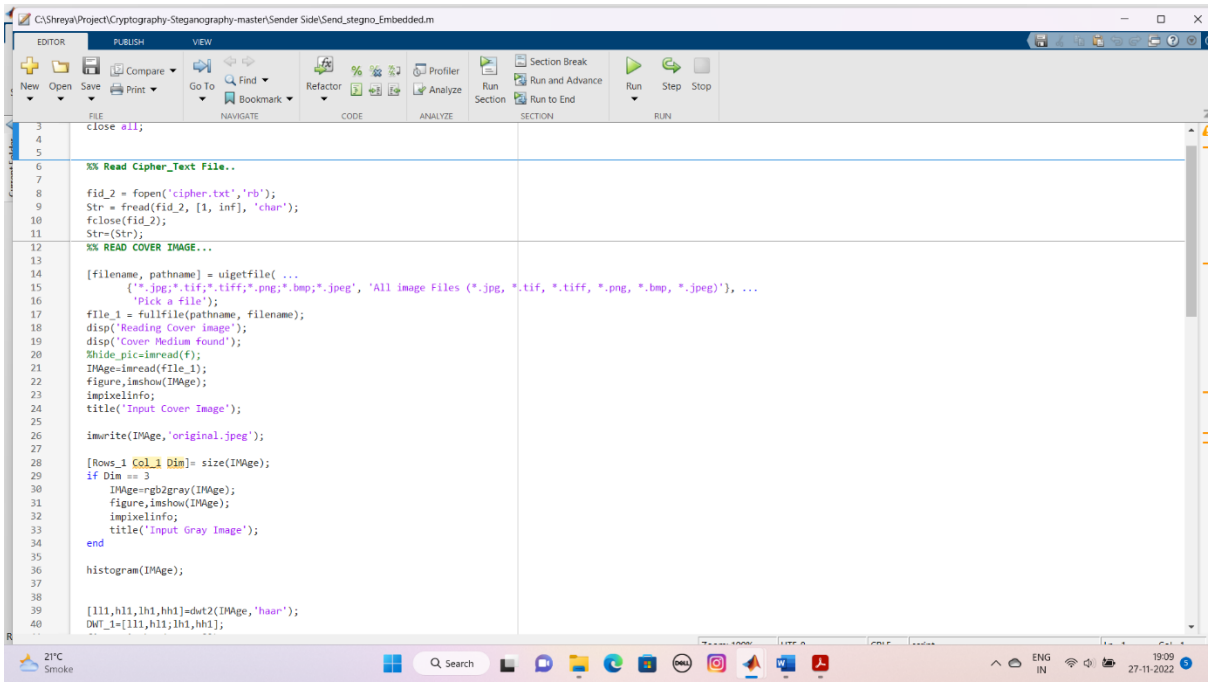


Figure 4.2.2.1 *Read cover image*

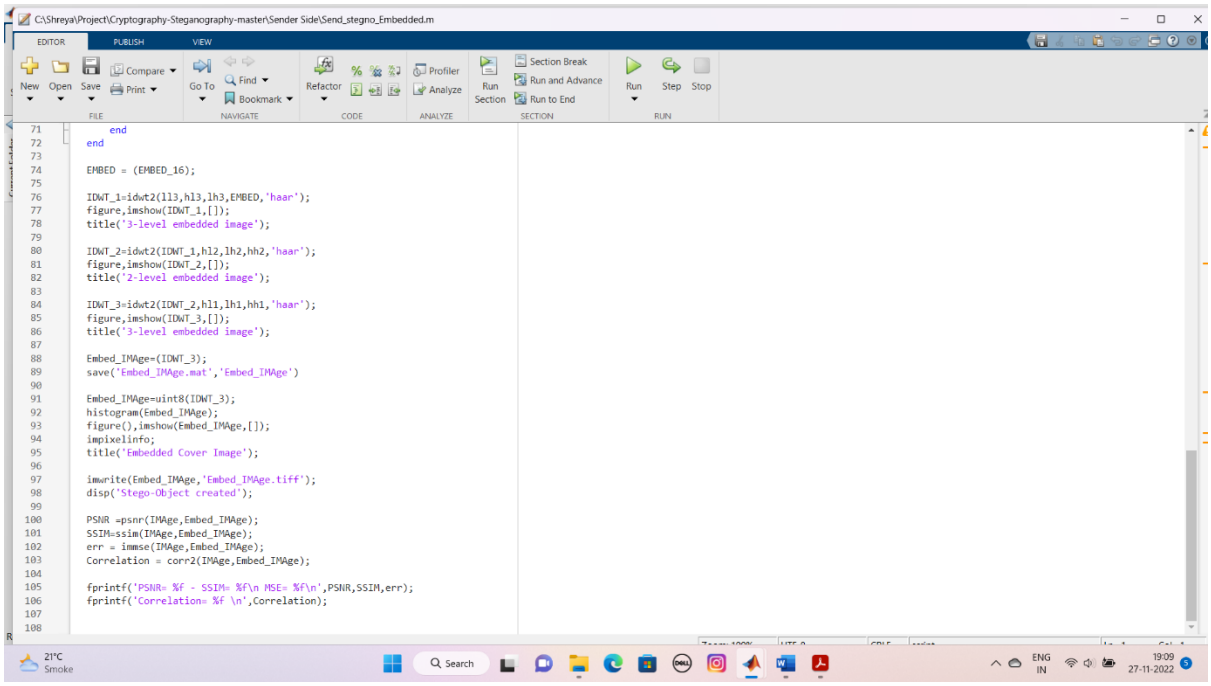


Figure 4.2.2.2 *Decomposed cover image*

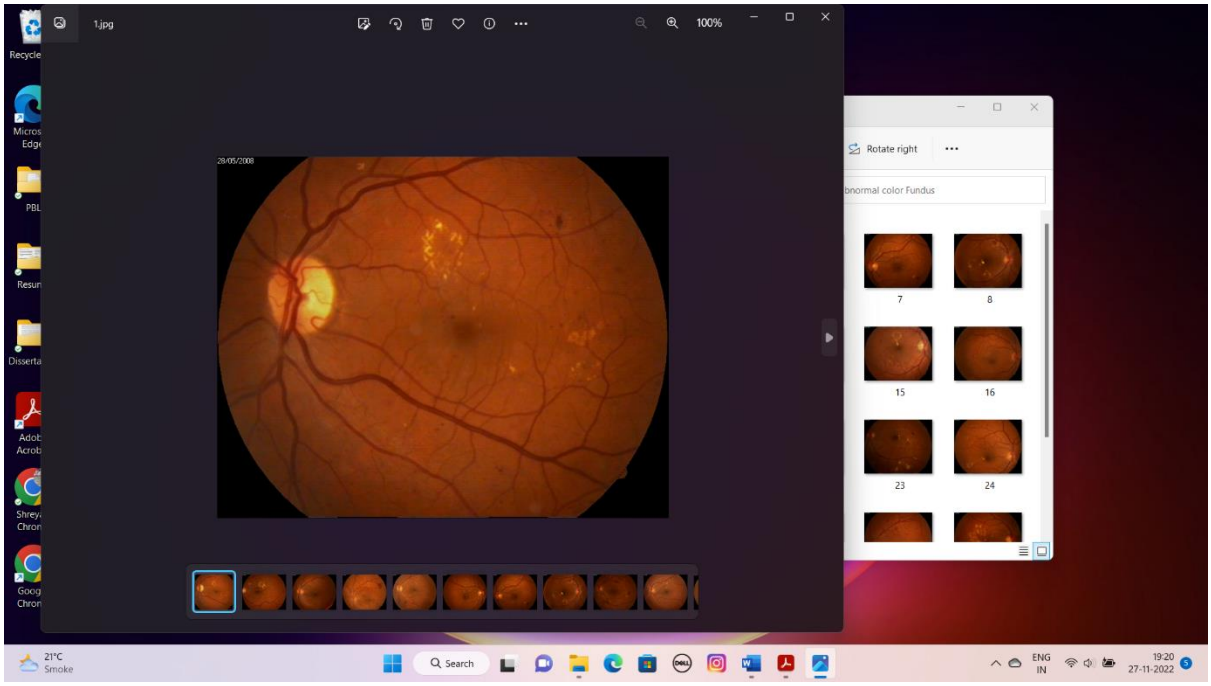


Figure 4.2.2.3 *Coloured image*

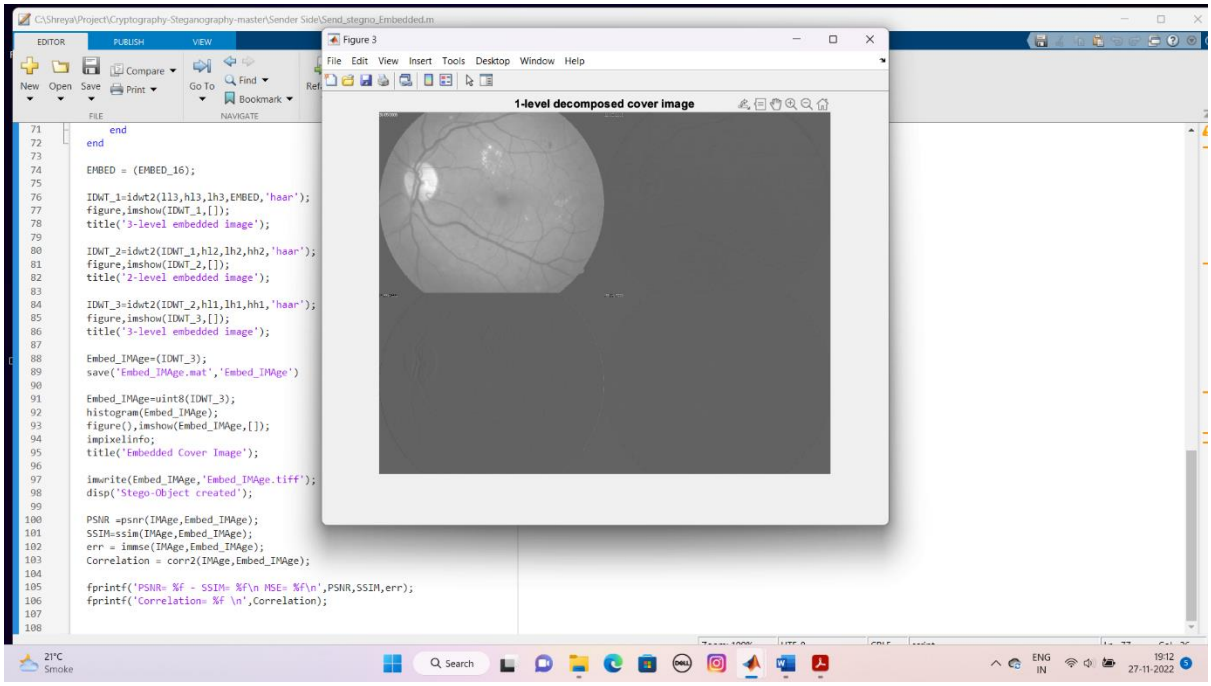


Figure 4.2.2.4 *1-level decomposed cover image*

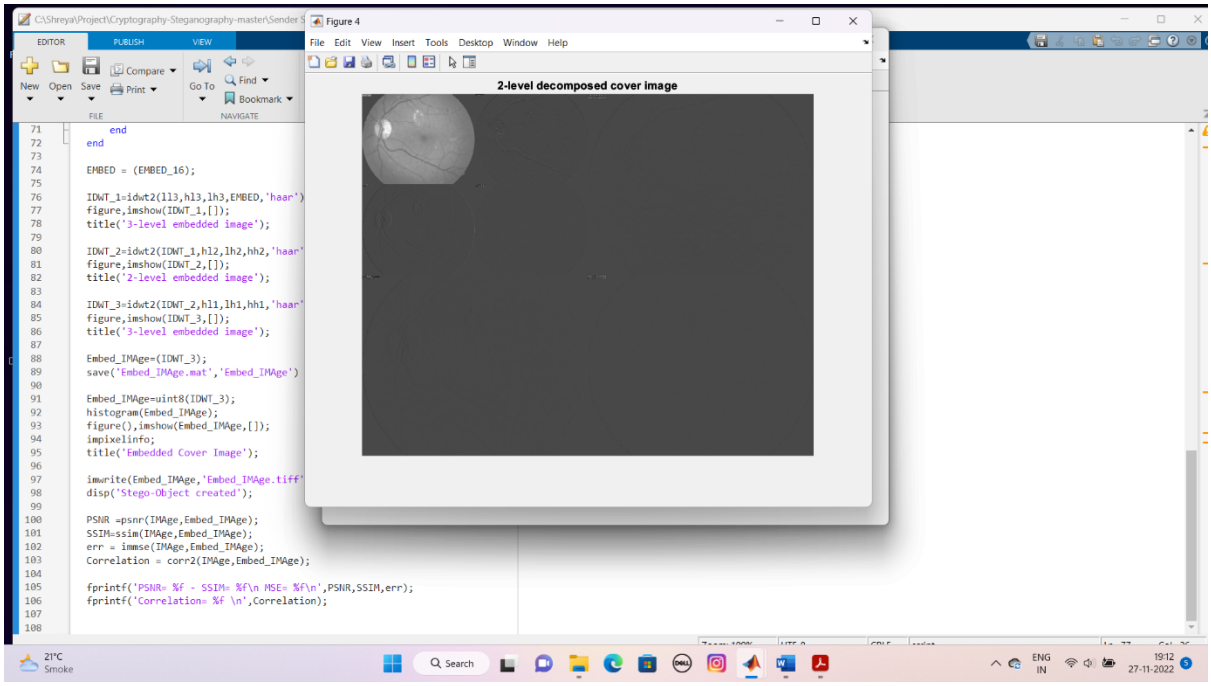


Figure 4.2.2.5 *2-level decomposed image*

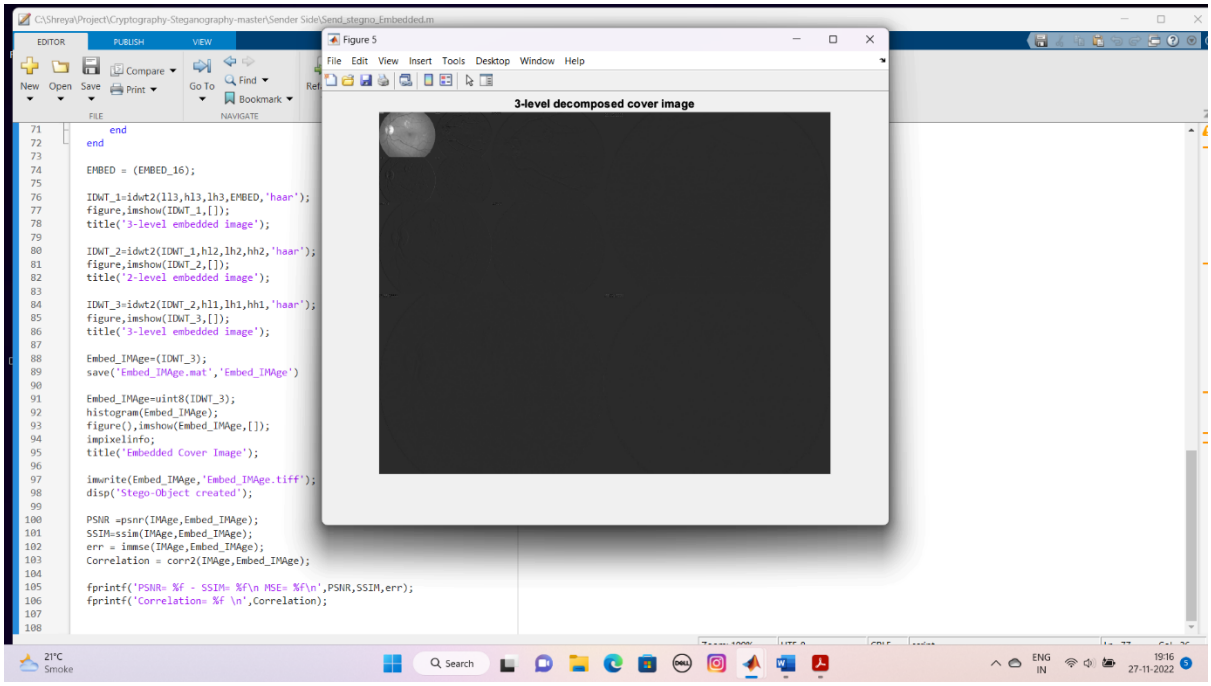


Figure 4.2.2.6 *3-level decomposed image*

4.2.3 Receiver's side

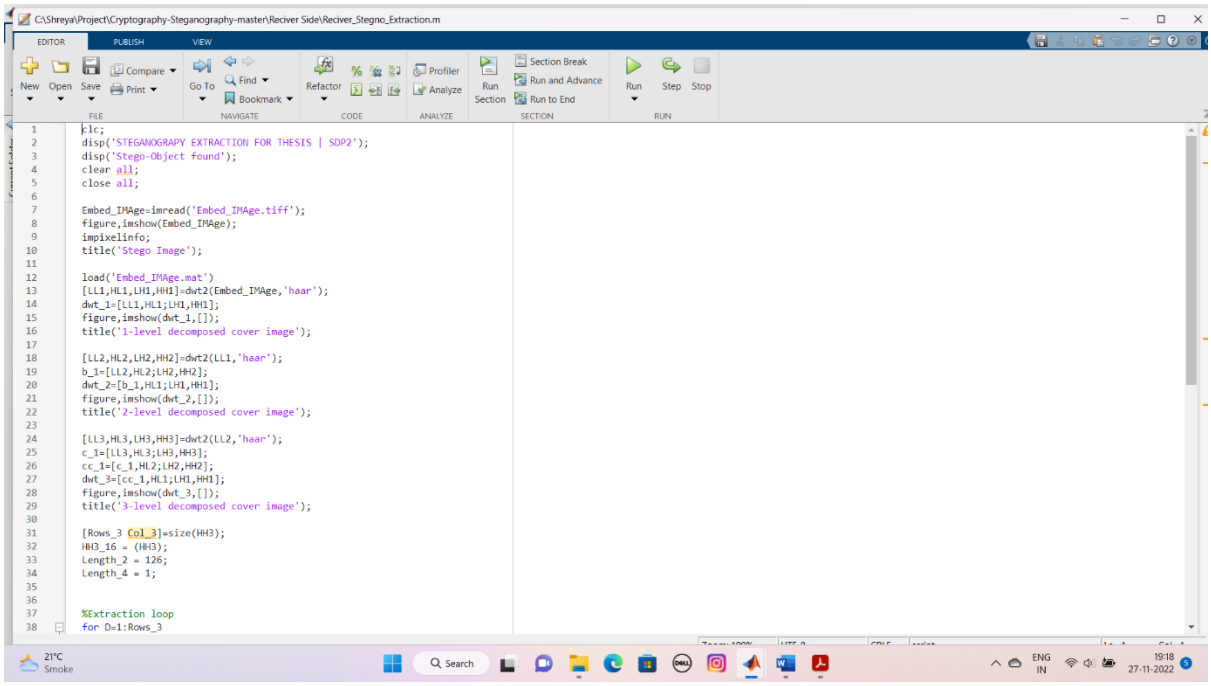


Figure 4.2.3.1 *Extraction code*

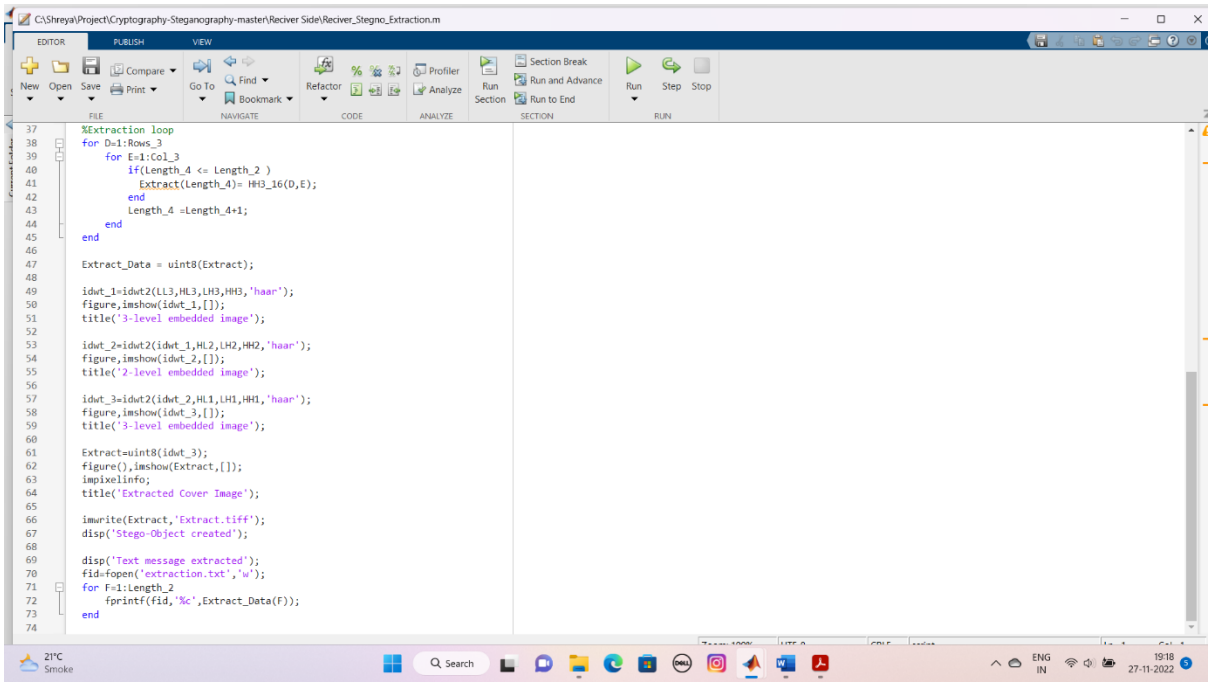


Figure 4.2.3.2 *Extract data*

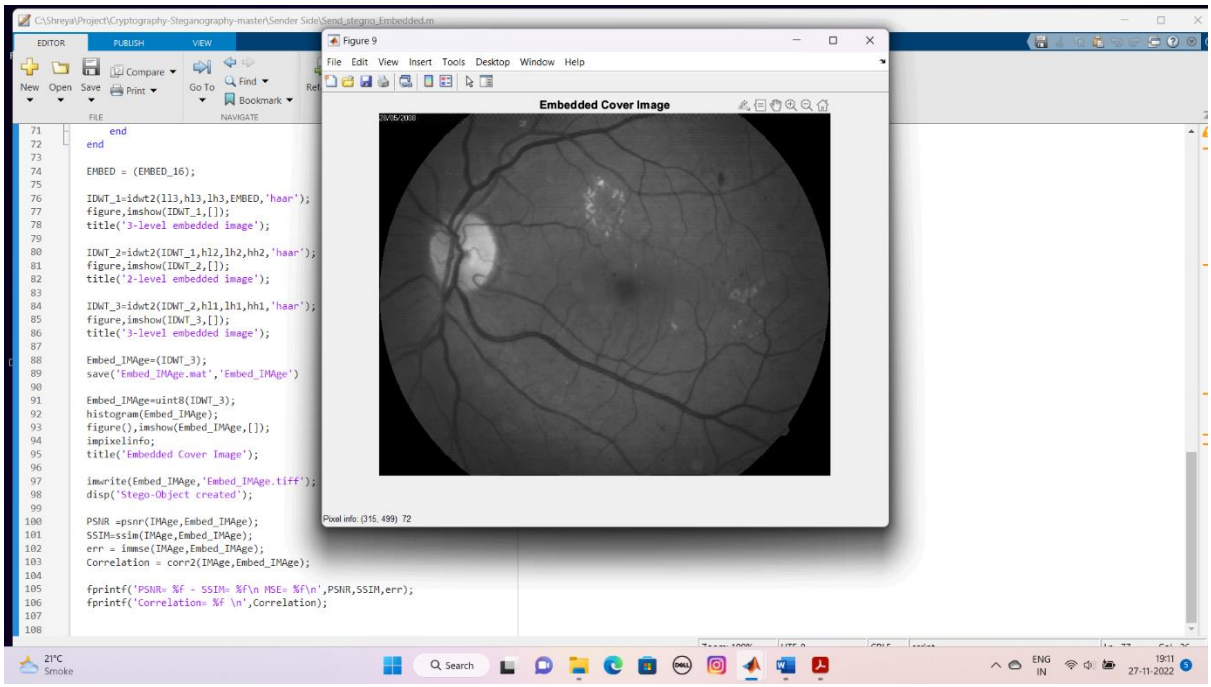
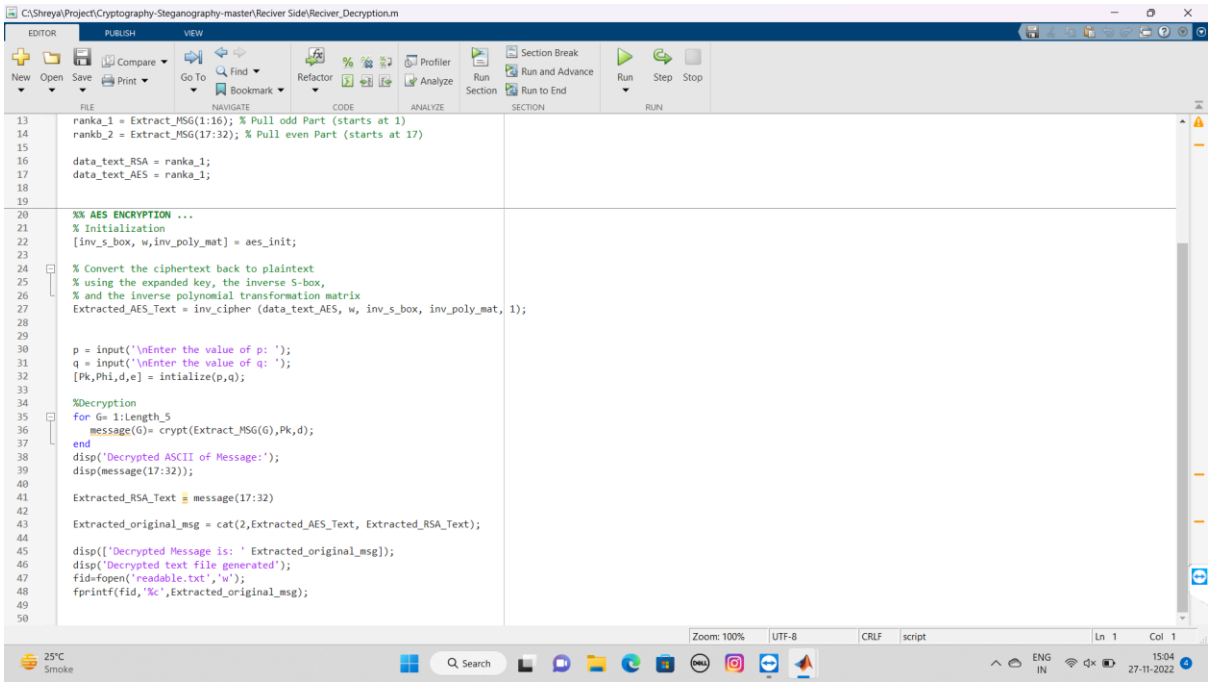


Figure 4.2.3.3 *Extracted grey image*

4.2.4 Decryption



```
ranka_1 = Extract_MSG(1:16); % Pull odd Part (starts at 1)
rankb_2 = Extract_MSG(17:32); % Pull even Part (starts at 17)

data_text_RSA = ranka_1;
data_text_AES = ranka_1;


%% AES ENCRYPTION ...
% Initialization
[inv_s_box, w,inv_poly_mat] = aes_init;

% Convert the ciphertext back to plaintext
% using the expanded key, the inverse S-box,
% and the inverse polynomial transformation matrix
Extracted_AES_Text = inv_cipher (data_text_AES, w, inv_s_box, inv_poly_mat, 1);


p = input('\nEnter the value of p: ');
q = input('\nEnter the value of q: ');
[Pk,Phi,d,e] = intialize(p,q);

%Decryption
for G= 1:Length_5
   message(G)= crypt(Extract_MSG(G),Pk,d);
end
disp('Decrypted ASCII of Message:');
disp(message(17:32));

Extracted_RSA_Text = message(17:32)

Extracted_original_msg = cat(2,Extracted_AES_Text, Extracted_RSA_Text);

disp(['Decrypted Message is: ' Extracted_original_msg]);
disp('Decrypted text file generated');
fid=fopen('readable.txt','w');
fprintf(fid,'%c',Extracted_original_msg);
```

Figure 4.2.4.1 *Decryption code*

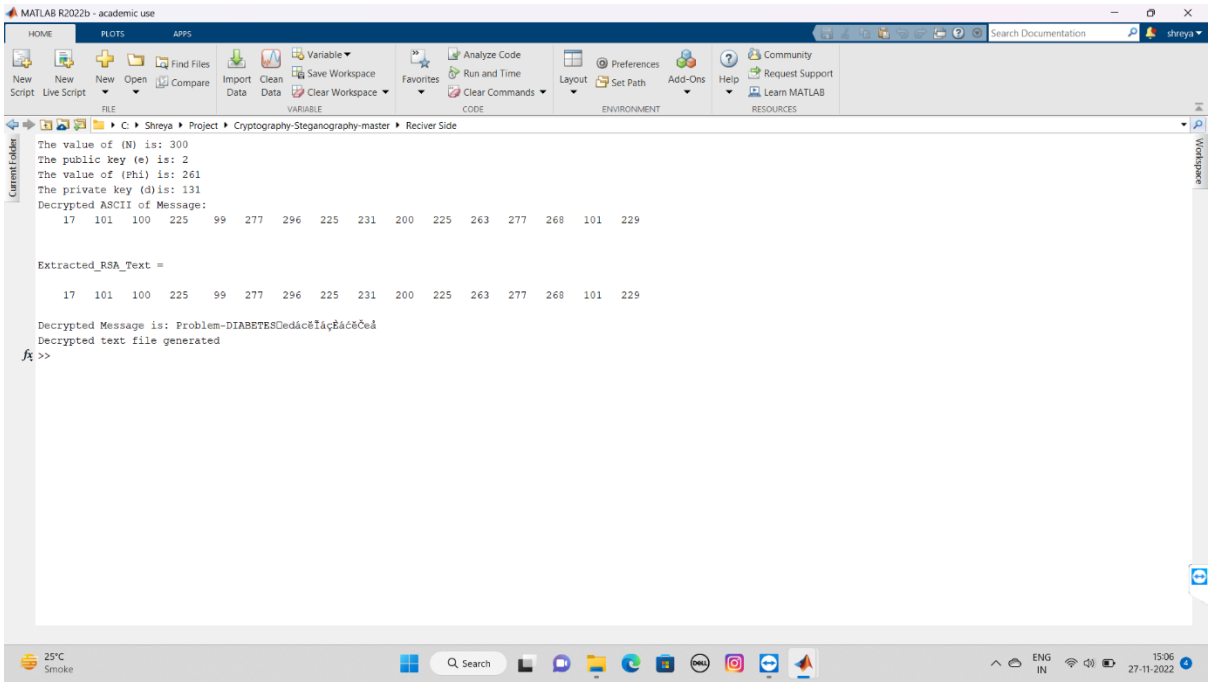


Figure 4.2.4.2 *Decrypted text*

CHAPTER-5

EVALUATION AND DISCUSSION

5.1 EVALUATION

5.1.1 Colored image

We compare our method with 90% of the host pictures payload capacity. Human eyes are unable to distinguish between the stego pictures because to their extreme imperceptibility, according to analysis of MSE, PSNR, SSIM, and Correlation. The average PSNR is 50.681 and SSIM is 0.9939 of coloured format of dataset, whereas for grey format of dataset the average PSNR is 49.311 and SSIM is 0.9951.

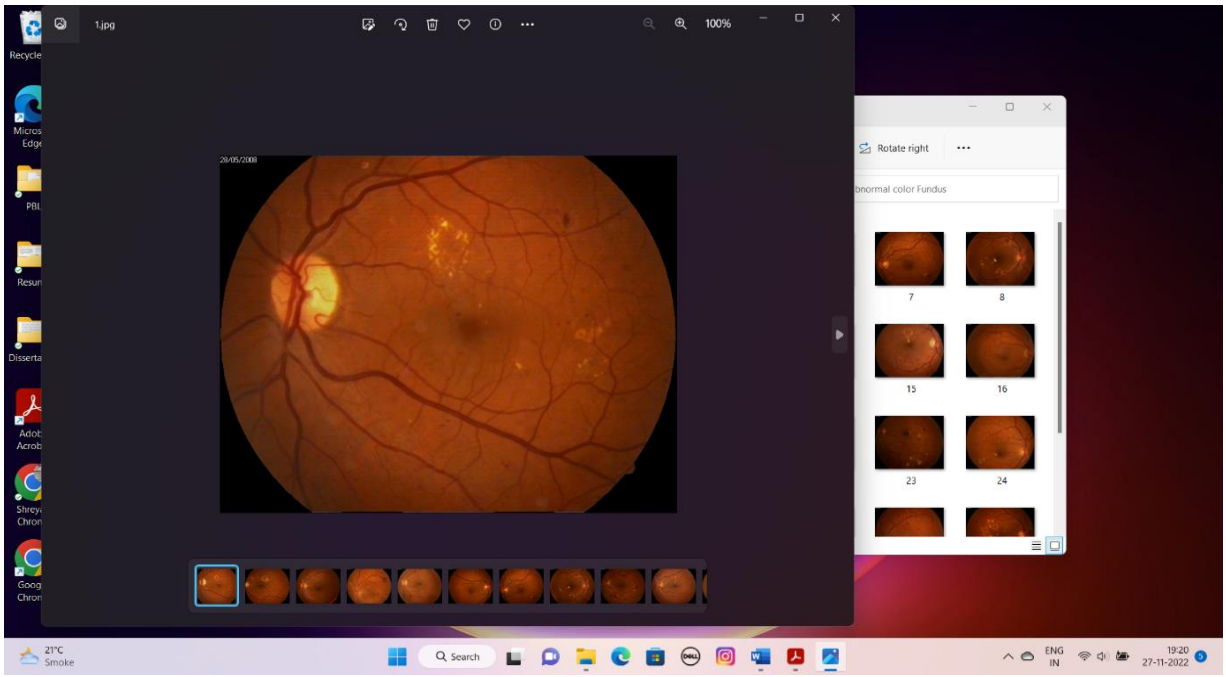


Figure 5.1.1.1 *Coloured image*

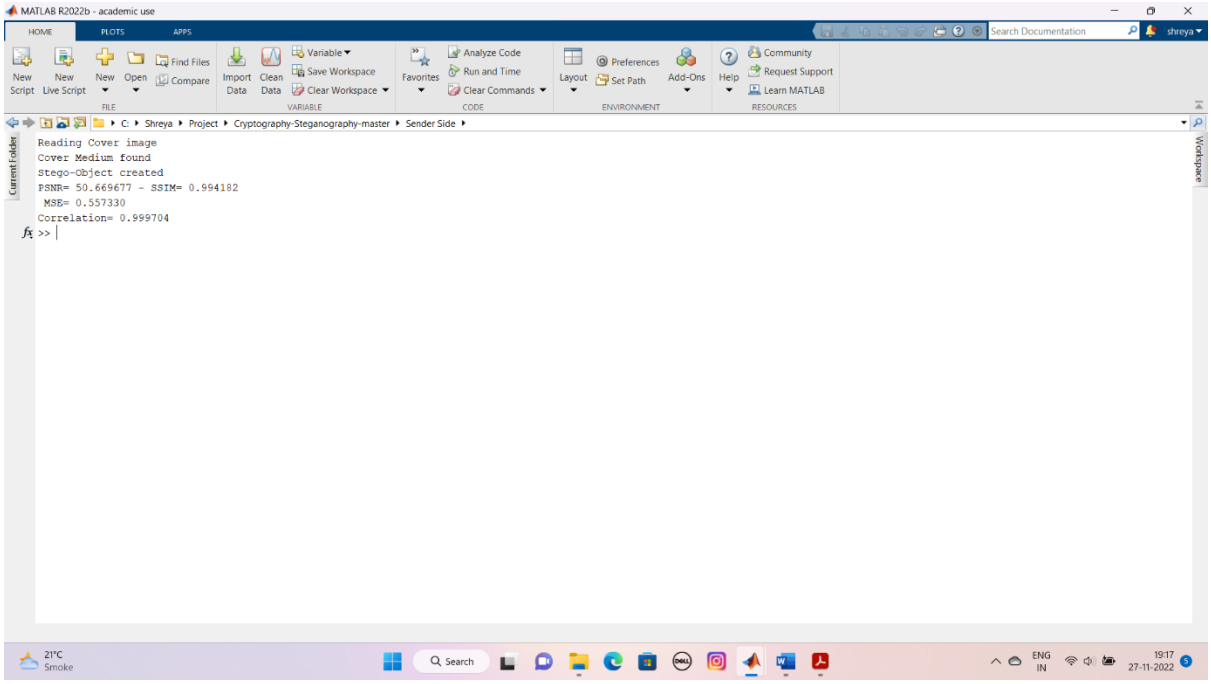


Figure 5.1.1.2 *PSNR and MSE Values*

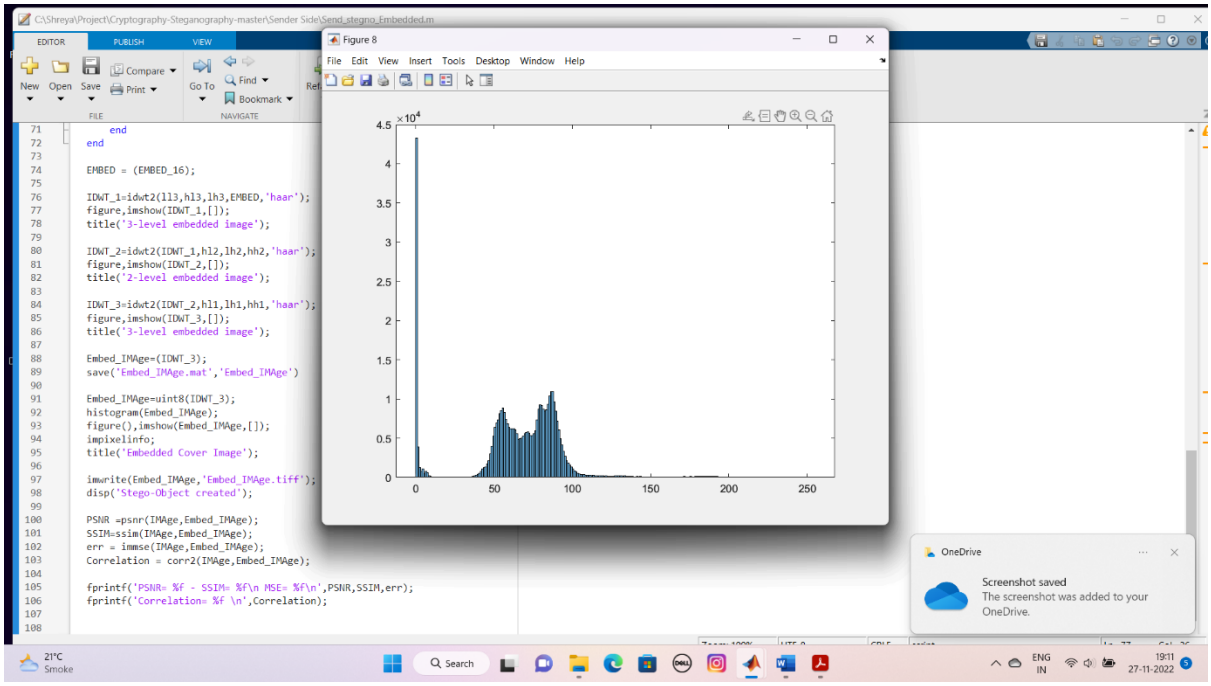


Figure 5.1.1.3 *Graph*

Table 5.1.1 *PSNR, MSE, SSIM and Correlation of 10 coloured image*

Image No.	PSNR	SSIM	MSE	Correlation
1	50.669	0.9941	0.5573	0.9997

2	50.788	0.9939	0.5423	0.9995
3	50.810	0.9938	0.5395	0.9995
4	50.587	0.9941	0.5679	0.9997
5	50.430	0.9942	0.5888	0.9997
6	50.802	0.9938	0.5405	0.9995
7	50.682	0.9940	0.5557	0.9995
8	50.763	0.9939	0.5454	0.9994
9	50.777	0.9937	0.5436	0.9990
10	50.504	0.9941	0.5788	0.9996

5.1.2 Grey image

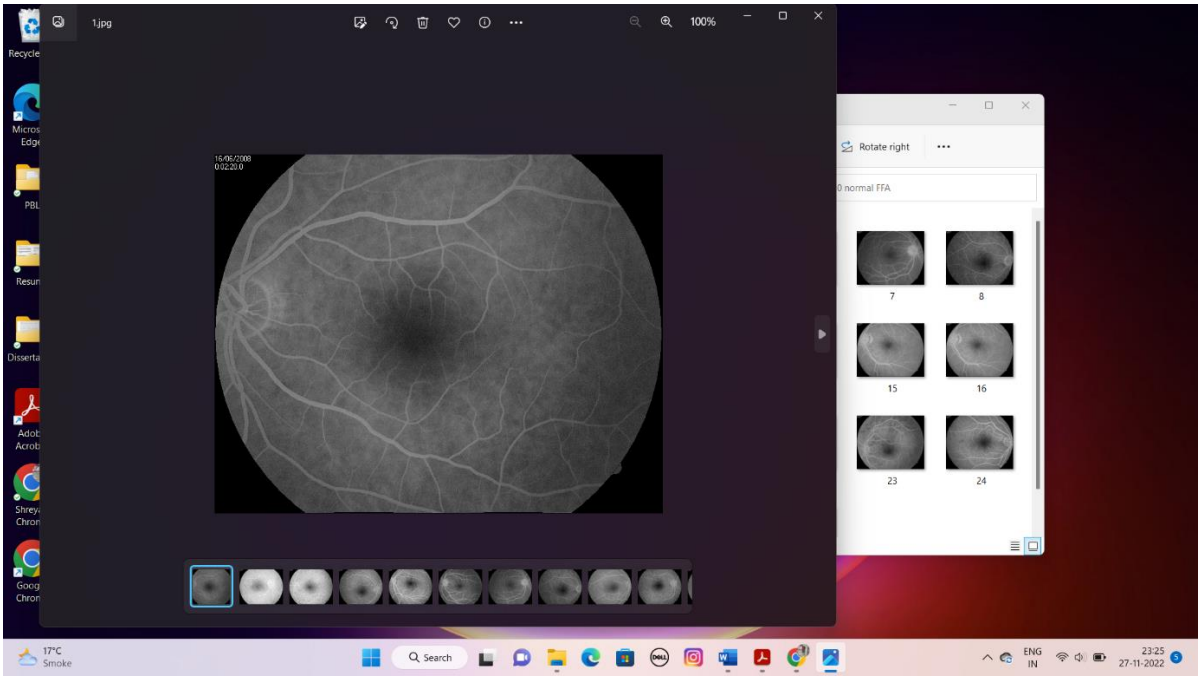


Figure 5.1.2.1 *Grey image*

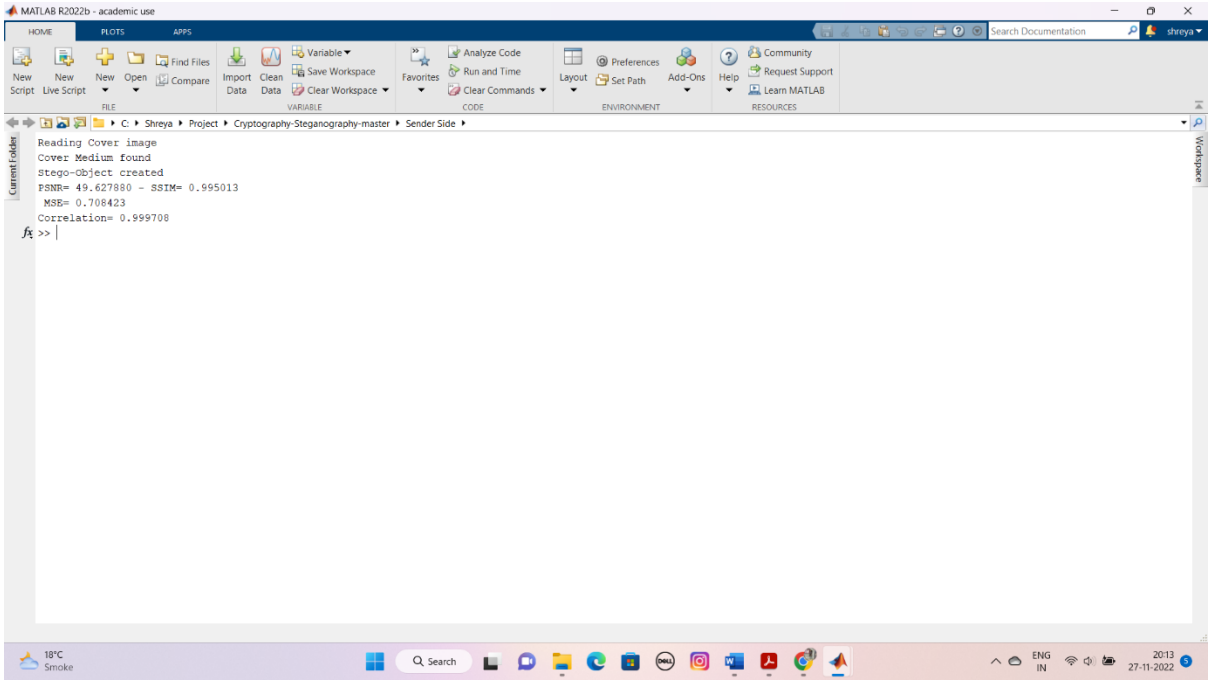


Figure 5.1.2.2 *Values of PSNR and MSE of grey image*

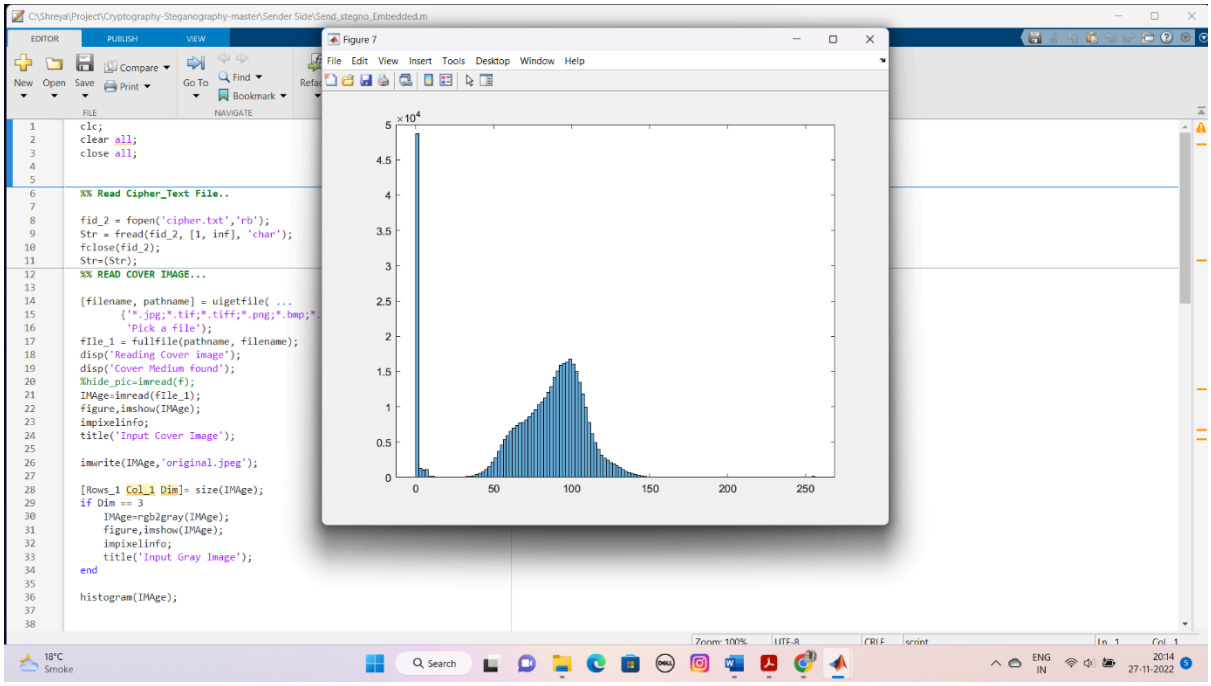


Figure 5.1.2.3 *Graph of grey image*

Table 5.1.2 *PSNR, MSE, SSIM and Correlation of 10 grey image*

Image No.	PSNR	SSIM	MSE	Correlation
1	49.627	0.9950	0.7084	0.9997

2	48.875	0.9949	0.8423	0.9999
3	48.583	0.9950	0.9009	0.9998
4	49.419	0.9951	0.7432	0.9998
5	48.745	0.9957	0.8681	0.9998
6	49.844	0.9954	0.6738	0.9997
7	49.547	0.9954	0.7216	0.9997
8	49.556	0.9951	0.7201	0.9997
9	49.391	0.9947	0.7480	0.9998
10	49.525	0.9952	0.7253	0.9997

5.2DISCUSSION

Comparing the results against another approach:

On a 720x576 pixel medical colour picture, the effectiveness of our model was compared with another method proposed by Ghazanfar Farooq Siddiqui [1]. Table compares the PSNR and SSIM values obtained by using our model to those obtained by [1]. the models' outcomes were applied to 720x576 colour medical photos. It was discovered that our suggested model performed better than others since it had a greater PSNR value and a SSIM value.

Table 5.2.1 *Comparison*

	PSNR	SSIM
Ghazanfar Siddiqui [1]	43.23	0.915
Proposed model	50.681	0.9939

CHAPTER 6

CONCLUSION

6.1CONCLUSION

Our system's key benefits include better embedding capability, more security, increased flexibility, and increased invisibility. In this study, a hybrid encryption technique that has been used was also employed. This hybrid system is seen as combining the RSA and AES algorithms [16]. When used on colour and grayscale pictures with various text sizes, all of the two suggested steganography approaches (LSB and 2D-DWT-3L) and their integration with encryption (AES and RSA) algorithms performed better. This is based on the eight statistical parameters that were examined (PSNR, MSE, SSIM, and Correlation). Only the PSNR and MSE, however, were able to discern the differences between the suggested approaches. With the suggested methodologies, there were no appreciable differences among the other statistical measures.

With the exception of the image, it was discovered that increasing the text size boosted the PSNR readings. This demonstrates that the resemblance between the original image and the stego image reduces when text size is increased, which is typically the case when the cover image has a lot of colour variation. The PSNR values are reduced by enlarging the text when the number of colours is restricted.

The PSNR readings followed a different pattern with the grayscale pictures, where the values fell as the text size increased. The MSE, which is similarly connected with the amount of colour variations in the cover picture, was lowered by expanding the text size for all the colour images under study, with the exception of the pepper image, where the bigger the colour variations, the lower the MSE value. The MSE values with the grayscale photographs, where the values fluctuated from one image to the next, did not, however, show a clear pattern. This may be explained by the histogram of each image's pixel values, which either evenly distribute over the grayscale or do not. The four suggested ways effectiveness was further assessed by contrasting their outcomes with those of other approaches on colour and grayscale pictures with various text sizes.

6.2LIMITATIONS

In comparison to the reference findings, our techniques exhibited lower MSE values and greater PSNR values. However, when compared to other techniques, the (2D-DWT-3L) with combination (AES and RSA) performed the slowest. It was also discovered that while text encryption boosts text security, it lessens the cover image's invisibility. In other words, data encryptions somewhat amplify the distortion of the cover picture, making it apparent to undesirable individuals. In conclusion, as compared to the reference methodologies employed in this investigation, our proposed approaches performed better at concealing sensitive data.

6.3 FUTURE SCOPE

We can improve information security practises in the future work and provide a channel for safe data exchange. This project may be expanded to apply to other types of data files, such

audio and video. Additionally, any Arabic text in the cover media may be used to create a powerful strategy for concealing Arabic text. We will attempt to emulate several communicating (normal and covert communication) parties on a big scale implementation. By creating a quantum steganography system that no one can duplicate, we want to improve the technique already in use, making it stronger than classical steganography.

REFERENCES

[1] G. F. Siddiqui et al., "A Dynamic Three-Bit Image Steganography Algorithm for Medical and e-Healthcare Systems," in IEEE Access, vol. 8, pp. 181893-181903, 2020, doi: 10.1109/ACCESS.2020.3028315.

[2] G. Prabakaran, R. Bhavani and P. S. Rajeswari, "Multi secure and robustness for medical image based steganography scheme," 2013 International Conference on Circuits, Power and Computing Technologies (ICCPCT), 2013, pp. 1188-1193, doi: 10.1109/ICCPCT.2013.6528835.

[3] M. S. Sreekutty and P. S. Baiju, "Security enhancement in image steganography for medical integrity verification system," 2017 International Conference on Circuit ,Power and Computing Technologies (ICCPCT), 2017, pp. 1-5, doi: 10.1109/ICCPCT.2017.8074197.

[4] M. M. Hashim, M. S. Taha, A. H. M. Aman, A. H. A. Hashim, M. S. M. Rahim and S. Islam, "Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography," 2019 7th International Conference on Mechatronics Engineering (ICOM), 2019, pp. 1-6, doi: 10.1109/ICOM47790.2019.8952061.

[5] Y. Srinivasan, B. Nutter, S. Mitra, B. Phillips and D. Ferris, "Secure transmission of medical records using high capacity steganography," Proceedings. 17th IEEE Symposium on Computer-Based Medical Systems, 2004, pp. 122-127, doi: 10.1109/CBMS.2004.1311702.

[6] Bala Krishnan, R., Rajesh Kumar, N., Raajan, N.R. et al. An Approach for Attaining Content Confidentiality on Medical Images Through Image Encryption with Steganography. Wireless Pers Commun (2021). https://doi.org/10.1007/s11277-021-08477-1

[7] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319263.

[8] T Manikandan *et al* 2021 *J. Phys.: Conf. Ser.* 1917 012016
https://iopscience.iop.org/article/10.1088/1742-6596/1917/1/012016/meta

[9] Jing Liu, Guangming Tang, Yifeng Sun (2013). A secure steganography for privacy protection in healthcare system. , 37(2), –. doi:10.1007/s10916-012-9918-z

[10] Yoon-Su, Jeong; Seung-Soo, Shin (2019). Staganography-based healthcare model for safe handling of multimedia health care information using VR. Multimedia Tools and Applications

[11] Jain, Mamta, Rishabh Charan Choudhary, and Anil Kumar. "Secure medical image steganography with RSA cryptography using decision tree." 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I). IEEE, 2016.

[12] Liao, Xin; Yin, Jiaojiao; Guo, Sujing; Li, Xiong; Sangaiah, Arun Kumar (2017). Medical JPEG image steganography based on preserving inter-block dependencies. Computers & Electrical Engineering, (), S0045790617302756–. doi:10.1016/j.compeleceng.2017.08.020

[13] Durgadevi, S., et al. "ENHANCE SECURITY FOR MEDICAL IMAGES THROUGH SECURE FORCE CRYPTOGRAPHY WITH STEGANOGRAPHY TECHNIQUES." (2019).

[14] Arik, Sabri; Huang, Tingwen; Lai, Weng Kin; Liu, Qingshan (2015). [Lecture Notes in Computer Science] Neural Information Processing Volume 9492 || A Medical Image Steganography Method Based on Integer Wavelet Transform and Overlapping Edge Detection. , 10.1007/978-3-319-26561-2(Chapter 52), 436–444. doi:10.1007/978-3-319-26561-2_52

[15] https://drive.uqu.edu.sa/_/aagutub/files/Publication_Journals/2020_IJCSNS_Esharq_Paper2.pdf

[16] Phang, Mei Ling, and Swee Huay Heng. "No. 6 A Survey on Crypto-Steganographic Schemes and A Use Case in Healthcare System." Journal of Engineering Technology and Applied Physics 1.2 (2019): 25-33.

[17] Al-Dmour, Hayat; Al-Ani, Ahmed; Hung Nguyen, (2014). [IEEE 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC) - Chicago, IL (2014.8.26-2014.8.30)] 2014 36th Annual International Conference of the IEEE Engineering in Medicine and Biology Society - An efficient steganography method for hiding patient confidential information. , (), 222–225. doi:10.1109/EMBC.2014.6943569

[18] Hussah N. AlEisa, "Data Confidentiality in Healthcare Monitoring Systems Based on Image Steganography to Improve the Exchange of Patient Information Using the Internet of Things", Journal of Healthcare Engineering, vol. 2022, Article ID 7528583, 11 pages, 2022. https://doi.org/10.1155/2022/7528583

[19] Elhoseny, Mohamed; Ramirez-Gonzalez, Gustavo; Abu-Elnasr, Osama M.; Shawkat, Shihab A.; N, Arunkumar; farouk, Ahmed (2018). Secure Medical Data Transmission Model for IoT-based Healthcare Systems. IEEE Access, (), 1–1. doi:10.1109/ACCESS.2018.2817615

[20] Shehab, Abdulaziz, et al. "Secure and robust fragile watermarking scheme for medical images." IEEE access 6 (2018): 10269-10278.

[21] Roseline Oluwaseun Ogundokun, Oluwakemi Christiana Abikoye, "A Safe and Secured Medical Textual Information Using an Improved LSB Image

Steganography", International Journal of Digital Multimedia Broadcasting, vol. 2021, Article ID 8827055, 8 pages, 2021. https://doi.org/10.1155/2021/8827055

[22] Jain, Mamta; Lenka, Saroj Kumar (2016). Diagonal queue medical image steganography with Rabin cryptosystem. Brain Informatics, 3(1), 39–51. doi:10.1007/s40708-016-0032-8

[23] Islam, M. Mahfuzul; Kamal, A.H.M. (2014). Facilitating and securing offline e-medicine service through image steganography. Healthcare Technology Letters, 1(2), 74–79. doi:10.1049/htl.2013.0026

[24] Sajedi, Hedieh (2018). Applications of data hiding techniques in medical and healthcare systems: a survey. Network Modeling Analysis in Health Informatics and Bioinformatics, 7(1), 6–. doi:10.1007/s13721-018-0169-x

[25] Abbas Cheddad; Joan Condell; Kevin Curran; Paul Mc Kevitt (2010). Digital image steganography: Survey and analysis of current methods. , 90(3), 727–752. doi:10.1016/j.sigpro.2009.08.010

[26] Ibaida, Ayman; Khalil, Ibrahim (2013). Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems. IEEE Transactions on Biomedical Engineering, 60(12), 3322–3330. doi:10.1109/TBME.2013.2264539

[27] Jeevitha, S.; Amutha Prabha, N. (2019). Effective payload and improved security using HMT Contourlet transform in medical image steganography. Health and Technology, (), –. doi:10.1007/s12553-018-00285-1

[28] Usman, Muhammad Arslan; Usman, Muhammad Rehan (2018). [IEEE 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) - Las Vegas, NV, USA (2018.1.12-2018.1.15)] 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC) - Using image steganography for providing enhanced medical data security. , (), 1–4. doi:10.1109/CCNC.2018.8319263

[29] Kaur, Sumeet; Bansal, Savina; Bansal, R. K. (2014). [IEEE 2014 International Conference on Computing for Sustainable Global Development (INDIACom) - New Delhi, India (2014.3.5-2014.3.7)] 2014 International Conference on Computing for Sustainable Global Development (INDIACom) - Steganography and classification of image steganography techniques. , (), 870–875. doi:10.1109/indiacom.2014.6828087

[30] K. Thangadurai and G. Sudha Devi, "An analysis of LSB based image steganography techniques," *2014 International Conference on Computer Communication and Informatics*, 2014, pp. 1-4, doi: 10.1109/ICCCI.2014.6921751.

[31] Jain, Mamta; Kumar, Anil; Choudhary, Rishabh Charan (2017). Improved diagonal queue medical image steganography using Chaos theory, LFSR, and Rabin cryptosystem. Brain Informatics, 4(2), 95–106. doi:10.1007/s40708-016-0057-z

[32] Mansour, Romany F.; Abdelrahim, Elsaid M. (2018). An evolutionary computing enriched RS attack resilient medical image steganography model for telemedicine applications. Multidimensional Systems and Signal Processing, (), –. doi:10.1007/s11045-018-0575-3

[33] M. Hassaballah;Mohamed Abdel Hameed;Ali Ismail Awad;Khan Muhammad; (2021). A Novel Image Steganography Method for Industrial Internet of Things Security . IEEE Transactions on Industrial Informatics, (), –. doi:10.1109/tii.2021.3053595

[34] Sajjad, Muhammad; Muhammad, Khan; Baik, Sung Wook; Rho, Seungmin; Jan, Zahoor; Yeo, Sang-Soo; Mehmood, Irfan (2017). Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices. Multimedia Tools and Applications, 76(3), 3519–3536. doi:10.1007/s11042-016-3811-6

[35] Sajedi, Hedieh; Rahber Yaghobi, Shabnam (2019). Information hiding methods for E-Healthcare. Smart Health, (), 100104–. doi:10.1016/j.smhl.2019.100104