Image Steganography algorithm for Medical and e-health care system

Shreya Gupta
Department of CSE,
Jaypee Institute of Information and Technology
Noida, Uttar-Pradesh, India
Email: 21303007@mail.jiit.ac.in

Dr. Amanpreet Kaur
Department of CSE,
Jaypee Institute of Information and Technology
Noida, Uttar-Pradesh, India
Email: amanpreet.kaur@mail.jiit.ac.in

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. With the help of the Internet of Things (IoT), the real and digital worlds are combined to form a uniform, networked communication system. As a consequence of the IoT's rapid expansion in the healthcare sector, the safety and confidentiality of the patient records become key problems for medical care applications. This paper proposed a dynamic security technique to safeguard the diagnostic text data in medical imaging. The suggested model is created by combining a proposed integrated encryption method with the 2D Discrete Wavelet Transform 2 Level (2D-DWT-2L) steganography system The suggested composite encryption technique combines the Rivest, Shamir, and Adleman (RSA) and Advanced Encryption Standard (AES) techniques. The suggested model starts with the cryptography of the data and further uses 2D-DWT-2L to conceal the outcome in a cover picture. Grayscale and color pictures are used as cover images to conceal different text formats. Unique encryption keys are created using these techniques, but the real data is protected. The performance of the proposed system was evaluated using statistical metrics including the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM), Structural Content (SC), and Correlation—were used to evaluate the effectiveness of the suggested method. When compared to current methodology, the suggested system showed its potential to conceal the sensitive patients' data into a selected image with indistinguishable and negligible degradation in the obtained stego-image.

Keywords- Steganography; Cryptography; Peak Signal-to-Noise Ratio (PSNR); Advance encryption standard (AES); 2D Discrete Wavelet Transform (2D-DWT-2L); Rivest, Shamir and Adleman (RSA); Structured Similarity (SSIM); Mean Square Error (MSE); Bit Error Rate (BER); Structural Content (SC); Haar Wavelet Transform (HWT); Correlation.

I. 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.

The science and technique of concealing data so that only the intended receiver is aware of its presence is known as steganography. The Greek word "stegano," which indicates "covered," and "graphic," which indicates "writing," are the source of the word "steganography." 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 encrypt a unique symmetry with a private key, then encrypt this key cypher with the recipient's asymmetric public key. The message is then encrypted using the same cypher and secret key. 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 (AES and RSA). Due to the AES algorithm's high effectiveness in the encryption block, it is used for data transfer. Due to the AES 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 patent mark.

The stego key is utilised throughout the fixed method to create it challenging to extract the embedded message without passing this key. The

result of the message embedding procedure is shown by the stego image. The steganography key is utilised while integrating and further 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.

A. An Overview

- Encryption

Data transmission and storage have become more dependent on information security. The security backgrounds presented in this chapter make use of numerous encryption algorithms. The extensive usage of images and the quick development of electronic data exchange 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 [6]. A significant advancement in encryption technology has been made recently, and a variety of encryption techniques are now utilised for image protection. These techniques generate unique encryption keys, but the actual text is hidden. To securely transfer dataset, encryption and decryption mechanisms were created and put to use.

- Cryptography

Primary objective of secret writing is to conceal the real significance of the message being conveyed. Information security in an electronic world demands a wide range of technical and legal abilities. Through encryption, technical means are made available. Given that the study and use of strong encryption techniques in the context of outsiders constitutes cryptology, commonly known as cryptography (adversaries). In a wider sense, it entails developing and analysing techniques that mitigate the impact of adversaries. [13] Electrical engineering, computer science, and mathematics all converge in the encryption modem. Although there are other ways to provide information security, cryptography is one such set of technologies.

B. Goal:

It has Cryptography as one of its features, which includes a variety of security goals, the ability to protect data privacy, prevent data alteration, and other features. Today, a significant security coding is employed frequently due to its benefits. Among all the goals for the protection of data mentioned above, the following four are considered as the cornerstone. Confidentiality, authenticity, integrity, and non-repudiation are these goals [11]. For cryptography to accomplish its fundamental goal, every one of these 4 categories have been stated in both principles and application be effectively addressed. Fraud and other nefarious

activity detection and prevention are goals of encryption.

The goal of this paper is to combine a novel hybrid method for data protection by combining steganography with encryption techniques. With the help of this technology, a secret message can be encrypted and embedded into a cover image to achieve maximum imperceptibility, longevity, and little degradation of the extracted image. The major goals of these method are:

- Create an integrated protection strategy that combines steganography (LSB and DWT) with data encryption to enhance the productivity, resilience, and unidentifiable stego pictures. [15]
- Use LSB and DWT to build a protection mechanism for hiding data sets in an image.
- Determine how effectively the created system secures and retrieves the original data.

C. Terminologies:

i. Plain text: The secret text sender who wish to engage with some other person that text is referred as plain text.

ii. Cipher Text: It refers to a message that is unintelligible to everyone. In other words, the communication is pointless, and before the information is really transmitted, an encoder will change the plain-text version of the message into something that is impossible to read or comprehend.

iii. Encryption: This definition of encryption describes the procedure used to change 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.

iv. Decryption: This procedure decrypts the data.

In other words, it is the process to change cypher data to plain data. We use the decrypted procedure side in the second method to obtain the aid of the first method (cipher text message). To ensure that message is transmitted in this situation, the decryption technique and key must also be used.

v. Key: It alludes to a particular character, alphanumeric text, or a number. Because the confidentiality of the encryption method is heavily dependent on the cryptography key, it is important to make the right decision. This key is utilised for the first two phases of encryption (plain text) and decryption (cypher text) respectively. Symmetric key cryptography is the practise of encrypting and decrypting data using the same key. However, when using multiple keys in a cryptographic

system, a separate secret key must be used for first, a second key to other, and a third key for decryption. Asymmetric Cryptography Key is the term used to describe this mechanism.

Encryption: It states that this method, which is also known as encryption, is used to change 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.

- Cryptanalysis

The art or science of coding how systems fail. 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.

- Steganography

The study and technique of concealing data so that only the beneficiary is aware of its presence is called steganography [8]. The phrase literally means "covered writing" and derives from the Greek words "steganos" (covered) and "graphic" (written). The method for secure transmission in which a sort of data (a hidden text) is camouflaged inside the image which is unimportant, to prevent the viewer from having any questions about the concealment of the secret information, that unimportant picture is called cover picture.

- Advanced Encryption Standard (AES) algorithm

Current parties worldwide have been asked by the NIST to contribute suggestions for new criteria. They were expected to support a block size of at least 128 bits in all submitted ideas, and the three primary volumes must be made up. The final iteration of the AES standard became unveiled in 2001 [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, then this application technique is iterated over (Nr - 1) times.

These (sub-bytes, shift-rows, and mix-columns) steps make up the round suction, which also includes the round key. The Mixed-Column step in the (Nal) round is reckless. The preceding 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 bits of data. Prior to beginning work on the filled matrices, the program will first create a matrix with a simple text block. The matrix state's encrypted text is acquired following the last round. A matrix will now read the note (column-by-column). Every stage operates continuously (sub the bytes, shift the rows, mix the columns and Add keys).

```
%% AES ENCRYPTION ...
[s_box, w, poly_mat] = aes_init;

% Convert plaintext from hexadecimal (string) to decimal representation
plaintext_AES = data_text_AES;
% Convert the plaintext to ciphertext,
% using the expanded key, the S-box, and the polynomial transformation matr
ciphertext_AES = cipher (plaintext_AES, w, s_box, poly_mat, 1);
```

Fig. 1. AES encryption

i. AES Performance Evaluation

Use of a cryptography that supports blocks longer than 128 bits is a prerequisite for the AES algorithmic input 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 with respect to: “Are compared to the real security algorithm for other algorithms offered.” It is critical to guarantee the consistency of 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 properties of the implementation and the algorithm:

All 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.

ii. Hardwired electronics using AES

Only public key is used to encrypt and decrypt in the symmetric key algorithm known as AES, making it suitable for hardwired electronics. It has

set text block sizes of 128 bits of text and keys that are either 128, 192, or 256 bits long (plain or encrypted). Longer messages are first split into 128-bit chunks and then 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.

- 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. RSA was picked due to its broad use and in-depth examination, their shared affiliation with the Massachusetts Institute of Technology (MIT), and the fact that they were all MIT students [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 key length is (1024) bit length.

A symmetric key is frequently used to encrypt data using private or secret keys. It is a kind of algorithm which, in general, uses a public key for both encryption and decryption process. 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. And hence, it's indeed crucial for both entities to preserve the login key's secrecy.

The sender must encrypt the message using the secret key before it can be delivered to the receiver. On the other side, the recipient will encrypt the message he receives using the same key. It serves as the message's covert key confirmation service in this instance. Additionally, it distinguishes the missionaries from other harmful sources.

```
ciphertext_AES = cipher (plaintext_AES, w, s_box, poly_mat, 1);
%%  RSA ENCRYPTION...
disp('Implementation of RSA Algorithm');
p = input('\nEnter the value of p: ');
q = input('\nEnter the value of q: ');
[Pk,Phi,d,e] = intialize(p,q);
[N,Phi,d,e] = intialize(p,q);
MAsg = data_text_RSA;
Length_1=length(MAsg);
% % %Encryption
for A= 1:Length_1
   cipher_RSA(A)= crypt(MAsg(A),N,e);
end
disp('Cipher_RSA Text of the entered Message:');
disp(cipher_RSA);
```

Fig. 2. RSA encryption

Public Key

If the key is known, the integrity of the message being sent is compromised. However, creating a safe means of key exchange between the correspondents is crucial. 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. It demonstrates how a message is encrypted, making it only capable of being decrypted by the intended receiver. As a result, Alex secures a message and sends it to Bobby using his public key. Bob decoded the ciphertext using his secret key.

Implementation

1. Key will be generated.
2. Encryption process
3. Decryption process

- Transform Domain Technique

Transformation using wavelets (WT) One of the essential and useful computing tools for a variety of image processing and signal processing applications, what we now refer to as a "wavelet," 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. Very massive wavelets may be used to detect coarse details, whereas incredibly tiny wavelets can be utilised to extract very precise features from a signal. The transformation of pixel domain information into spectral domain information wavelet is a common step in image steganography models. This is due to the wavelet transform's pixel-by-pixel division of the information at both high and low frequencies. The wavelet-based domain is recommended for several steganalysis operations because to its many advantages.

Wavelets are a powerful tool used in a wide range of statistical applications, including as compression techniques, data analysis, visual softening and quantization, graphic design, biometric authentication, and behavioural analysis.

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), spectral 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. This approach has the advantage of embedding the data that is more resistant to photo editing, resizing, and reduction. More pixels or the entire image are covered by the data as well.

- Discrete Wavelet Transform (DWT)

A discrete wavelet transform (DWT) divides an input signal into a collection of sets, each set consisting of a data series of parameters that

describe the signal's temporal development in the associated spectral range. [14] It represents one of the spectral domains where steganography may be applied. 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 implemented to the entire picture, these shortcoming of DCT were lessened when employing it. DWT delivers better power compactness than the DCT since it doesn't produce any obstructing distortions. In the DWT, the picture signal is filtered using two different types of filters.

```
[ll1,hl1,lh1,hh1]=dwt2(IMAge,'haar');
DWT_1=[ll1,hl1;lh1,hh1];
figure,imshow(DWT_1,[]);
title('1-level decomposed cover image');
```

Fig. 3. DWT_1

```
[ll2,hl2,lh2,hh2]=dwt2(ll1,'haar');
b=[ll2,hl2;lh2,hh2];
DWT_2=[b,hl1;lh1,hh1];
figure,imshow(DWT_2,[]);
title('2-level decomposed cover image');
```

Fig. 4. DWT_2

```
[ll3,hl3,lh3,hh3]=dwt2(ll2,'haar');
c=[ll3,hl3;lh3,hh3];
cc=[c,hl2;lh2,hh2];
DWT_3=[cc,hl1;lh1,hh1];
figure,imshow(DWT_3,[]);
title('3-level decomposed cover image');

[Rows_2 Col_2]=size(hh3);
hh3_16 = (hh3);
Length_2 = numel(Str);
Length_3 = 1;
```

Fig. 5. DWT_3

- 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) which entails approximated and discretization terms, information separation, collecting enabling conditions, and component 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.

Functionality of Haar

Wavelets are basically math concepts that was created for frequency-based information sorting. A certain vector space's orthogonal basis is referred

to as a "wavelet" in this context. The information is transformed from the time domain to the spectral domain using a discrete wavelet transform, and then each component is saved with the appropriate resolution level.

When doing a 2D discrete wavelet transform, the rows and columns are initially transformed [35]. A straightforward use of the Haar DWT equation is shown in Eq (1). The Haar DWT does exceptionally well at identifying features like corners and edges. When the immersing process is complete, the steganographic picture is created using the inverse Haar DWT. The horizontal and the vertical operations are conducted as 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)

a. Operation on the horizontal plane:

Two strands, one is for low frequency range and another for high frequency range, will be created inside a single picture. Pixels are horizontally scanned i.e., starting from left and ending at right. Processes of summing and subtracting are applied to the surrounding pixels. The left side, that symbolises the low bandwidths, 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 were further differentiated from low and high frequencies acquired from the horizontal operation. For the summing up and subtracting mechanism, every pixel will be analysed over, but in the vertical plane. The top half will hold the sum of the neighbouring pixels.

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 will be 0. When this characteristic is true, then transform is energy invariant.
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
a temporary array, it is memory efficient.

- Image type

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

1. Binary picture
2. A grayscale picture
3. An index image
4. A RGB or true colour image

a. The binary image

Pixels only come in grey. We are just required 1 bit per pixel because there are only 2 feasible values for each pixel (0, 1).

b. Grayscale icon

The typical range of grayscale values for pixels is 0 (black) to 255. (white). A pixel is usually defined by 8 bits, which is exactly equal to 1 byte. There are other greyscale levels used, although they were often powers of 2.

c. Indexed picture

An indexing picture is composed of an array and a coloured mapped vector. 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.

d. RGB or True colour picture

The proportions of the colours red, green, and blue in each unit provide its distinct colour. There are totally 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 every unit are presented by a "stack" of 3 matrices in such an image. This indicates that there are 3 values that correlate to each pixel.

II. RELATED WORK

G.F. Siddiqui, [1] proposed the Image Region Decomposition (IRD) approach, which has better hiding capacity and contains more hidden information in medical health pictures. The technique separates the greyscale Magnetic Resonance Imaging (MRI) pictures into different zones of low, medium, and high intensities. They operate a frame of n Least Significant Bits (LSBs) in each of the k units that make up each area. 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 calculate the performance of proposed IRD

algorithm over the variety of brain MRI pictures. The results showed that the MRI steganographic picture is undetectable, much like the real image, and that this can be achieved by modifying the 2 and 1 LSBs in the least-intensity region. Compared to other approaches of a similar kind, there suggested steganography technique offers the superior average PSNR value. The empirical findings demonstrate that, when compared to current approaches, the suggested IRD algorithm adversely enhances imperceptibility and data embedding capability.

Dr. Bhavani R, [2] Proposed a safe, confidential and reliable medical image steganography technique. Thus, the preservation of digital medical photos, the suggested method offers an effective storage security mechanism. They proposed an efficient steganography method employing the Integer Wavelet Transform to encrypt the MRI medical data into a single container image (IWT). The faux box image was created by flipping the container picture to the left. The patient's diagnostic' hidden picture was then found, modified with Arnold, and scrambled. In the first case, the jumbled secret data was combined with the dummy box image to generate a false secret picture. The second scenario involved capturing the container picture, combining it with the false secret image, and creating a stego image. The medical image that was recovered has satisfactory visual quality.

[3] Medical picture tampering is possible when patient's medical data is transferred over a network which is not secure. Therefore, it's 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 utilizing the SHA method to verify the integrity. The discrete wavelet transform will be used to incorporate the hashing function (H1) in the RONI. By comparing the hashing at the recipient's end, they may verify the validity of a medical picture. If any modifications are made, the hashing does not match. This paper postulates a fresh strategy for boosting security. With the aid of spatial reversible steganography, the changed medical picture is concealed within a seemingly normal image. They 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 (HMF) is utilized for guiding the random selection process. 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: In order to monitor and trace each bit in the steganographic picture during embedding, the hidden data must first be segregated. Then, during integrating, the 0- and 1-bits must be verified and plotted. 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 presence of those data via image steganography was 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 conventional Least Significant Bit (LSB) modification approaches of information concealing, Bit Plane Complexity Segmentation (BPCS) was developed. Its foundation is the notion that information can be concealed even in higher bit-planes if it is concealed in blocks that appear to be complex. This method creates a total of 24 bit-plane by dissecting every color level in an RGB picture into its 8 distinct bit-plane (8-bit greyscale pictures will have just 8 bit-plane). The 8-bit data points, commonly referred to as Pure Binary Code or PBC, are first transformed to Canonical Gray Code as part of the bit-plane decomposition for the reasons listed in (CGC). The distribution of 1s and 0s for every 8x8 block in particular 24 bit-plane, 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] provides a technique for concealing biomedical data that locates the sensor to detect across the DICOM picture using a Queen Traversal pattern and scrambles the biomedical DICOM picture using a Sudoku-based algorithm. It conceals the encrypted or scrambled normal pictures that contain sensitive health data. The effectiveness of the system in relation to the many parameters of relevance is established by experimental results. In this expected work, the experts of the suggested system present and discuss a unique approach for encapsulating hidden content in scrambled DICOM pictures. The famous chess game in which the Queen Traversal pattern is utilized for identification of the pels. As a result, the illegal material recovery needed a huge amount of intricacy and a significant burden. The main DICOM picture has been split into an exact proportion of smaller parts and has been randomized using a Sudoku method. During the exercise of embedding hidden medical data, the

travel sequences were used to find the pictures precludes. The secret material is integrated first by LSB conversion algorithm, and DICOM stego image is produced after the final descrambling. The stego DICOM pictures produced by this suggested method have the least Means Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values. The optimal traversal method for identifying the precludes and Picture organized and disorganized methods is the key (secret) to content extraction.

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 information security for health care pictures. This paper's objective was:

- By solely utilizing the main picture's boundary areas for information hiding, they offer detection accuracy.
- By using data compression on the hidden pictures, it provides excellent performance and
- use swapped Huffman tree encoding (SHT) to protect and preserve the tamped information.

While briefly explaining 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] medical security using Image Steganography is combination of various techniques which has been put forth. The suggested model 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. The main picture is converted into a steganographic picture using MATLAB 2021 and a random pixel generator. This steganographic picture is then validated using privileges such a login Details, passcode, and SMS confirmation using a device called Pega. The major goal of this study is to ensure complete security while ensuring adequate and safe picture delivery. Additionally, paper suggests that in order to validate identification, the sender and receiver should be authenticated more than once. The hidden picture is concealed throughout the encryption process by randomly rearranging the cells using a random pixel generator method. The randomly generated key is only known to the communicator and the collector. The Pega Database, which sends emails, was used to extract the user ID and password. The Pega tool sends SMS to the authenticated communicator's phone number. 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 verification and an OTP, the authenticated user proves his identity on the transmitter side. Using the Pega tool, email verification is carried out by delivering the authorized user's login information to the sender's email address. The OTP verification procedure is finished when the SMS is sent to the giver's cellphone number. After user verification, the user will be allowed to send the private picture. The encryption and steganography processes are implemented in the backend using MATLAB. The transmitter end handles both encryption and steganography completely. Here, the hidden picture has been scrambled by using XOR Cipher Encryption concept, then image steganography is applied using the LSB approach, and lastly, a steganographic picture is created by utilizing MATLAB.

Jing Liu [9], suggested a steganographic technique that can offer very secure protection for sensitive data in medical systems. Their approach divides a main image into integrating parts with three successive, non-overlapping bits using a Hilbert filling curve once after translating it into a sequence of 1D bytes. We utilized the adaptive pixel pair match (APPM) approach to insert numbers with in pixel value differences (PVD) of the 3 pixels, and the foundation of the hidden numerals depends on the dissimilarities between 3-pixel value. It is possible to minimize the distortion of the picture triggered by data integration by addressing an optimal solution. We provide an APPM-based approach that takes HVS into account. Comparing Hong et al, Given the same immersion ratio, APPM demonstrates the least distortion when compared to other integrating approaches as n-bits LSB replacement, LSBMR, and DE. A crucial requirement for an integrated technique when taking HVS into account is the ability to embed digits in several ranges, which is something that APPM also supports. However, when a big base is used, APPM exhibits significant distortion. The suggested methodology uses APPM to embed data in PVD. To convert a 2-D image's pixel matrix to a 1-D bit series, a Hilbert filling curve is utilized.

The authenticity of client audio-visual picture data handled by specialist diagnostic tools using VR must be ensured. Jeong Yoon-su, [10] suggest the steganography-based medical approach. The suggested technique attempts to prohibit medical team from using VR to illegally access multimedia picture data obtained by specialized diagnostic tools without the user's approval. This suggested model encrypts multimedia health care information with a hybrid cypher using the client credentials as well as signature. The suggested model incorporates components that guarantee the security and privacy of the person's

diagnostic pictures while maintaining the quality of the audiovisual pictures that was recorded using specialized diagnostic products. Audiovisual health data seen through VR is also protected from manipulation since the person's signature was protected using crypto-steganographic based obfuscation techniques. The suggested model, in particular, gives direct counselling linked to clients' medical condition as well as first care in association with the medical healthcare system in order to improve the handling of client's private pictures for users in hospitals. The suggested model includes the following attributes: For the confidentiality of data:

- The fidelity of encoding and decoding is first secured.
- Moreover, the security of the healthcare data created by specialized diagnostic tools is protected while the certification is guaranteed by the diagnostic imaging technology.
- Lastly, medical image information is safely communicated via steganography techniques.

In this paper Mamta Jain, Anil kumar, [11] A unique mystery transmission method that is a persuasive choice for conveying secret therapy health data together with the appropriate medicative carrier image is suggested using the notion of indefinite quality. Using a prediction model, the sender randomly distributes the secret information blocks to the carrier, enhancing security standards and significantly affecting the calculation that is presented. 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 protect the diagnostic info. A predictive model shows a perfect division between corresponding groups to provide options. By analyzing the results and histograms, it is discovered that the associated secret treatment steganographic pictures cannot be used to assess subtlety bending, and that the PSNR, MSE scores, and range of largest concealment restriction outperform other current plans.

In this paper, Xia Liao and Jiaojiao Yin [12] suggest a brand-new steganographic method for JPEG medical images that is in accordance with the cross-functional variables interdependence. Fundamental approach is basically 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 unique private communication method which integrates cryptography and steganography methods to add an additional layer of protection and make it impossible for a stenographer to read the encrypted message without the key is described. The Strong Compel AES algorithmic programme was used to first encode the secret pictures, and then JSTEG and LSB methods were used to hide the encoded photos in the main image. As a result of the cypher picture being hidden between the cover photographs using steganography, the key image may transfer around an effective channel without appearing strange. Two parameters, PSNR and MSE, are computed.

In order to conceal the EPR information in the high frequency component 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 secret information in sharp areas of the picture, then uses an edge detection algorithm that makes use of overlapping blocks. Utilizing overlapping blocks is done besides order to broaden the parameterization payload by minimizing the quantity of unwanted pixels. By encoding two hidden data into 3 bits components via an XOR method, that only modifies 1 bit at the very most, the discrepancy in between main and steganographic pictures is reduced. The study's findings show advancements in integrating capability and interpretability compared to one of the available EPR concealing techniques.

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 paper, Mei Ling Phang and Swee Huay Heng [16] suggested few techniques, including a safe and reliable technique for retrieving corner and gentle zones from a photo utilising composite feature extraction, 2-component LSB modification to inadvertently embed hidden message in corner areas, dynamic LSB alteration to erroneously encode hidden message in soft areas, and the well-known AES encryption method to encode messages until integrating. Additionally, they showed how this approach withstands both

optical and analytic steganalysis approaches. Thus, this crypto-steganographic system for the medical industry was able to fulfil both the essential criteria for steganography and the primary goals of cryptography, which safeguard the text's secrecy.

In order to secure patient information, Ahmed Al-Ani and Hung Nguyen [17] suggested an image 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 precise sections for integration that are fewer susceptible to alterations with the help of HVS. The disruption is additionally lessened by utilising the 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 client's private data in their diagnostic 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 substance is utilised to conceal the hidden picture in a coloured photo, IWT with LSB is used to conceal the hidden image in a grayscale image. By evaluating the mean square error (MSE) and PSNR, one may determine the amount of distortion among the main picture and steganographic picture, 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 safe person's healthcare information transfer system utilizing the both coloured and grayscale photographs as a main picture. 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 6 quantitative measures (PSNR, MSE, BER, SSIM, SC, and correlation) were used to evaluate overall performance. The suggested model demonstrated its ability to cover up the private data of the person into a main picture and little degradation in the received stego-image when compared to current approaches.

The grouped block approach is used in this paper, SVD-based delicate 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, 2 verification factors: frame authorization and readjustment 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 readjustment picture and the tamper localization accuracy evaluated by equated to the current methods. Despite of 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.

III. PROPOSED METHOD

This paper study suggests a medical reliability to protect the conveyance of patient records in IoT contexts. 4 ongoing mechanisms make up the suggested model:

- The private information of the person is hidden using a suggested integrated encryption method that combines the RSA and AES encryption techniques.
- Using 2D-DWT-2L, the encoded info is concealed under a cover picture, creating a steganographic-picture.
- Extracting the integrated information.
- Need to get the real information, the extracted information is decoded.

Cryptography is the technique of encrypting messages so that only authorised persons may read them, preventing hacking. The symmetric AES algo utilized the only key across both ends. Larger data are split into pieces before transmission. Evidently, longer keys demand a lengthier encrypt and decrypt operation while simultaneously making the cypher harder to crack. It benefits from a configurable key size that ranges from (2–2048) bits.

This research applied DWT steganography process that work in spatial domain at both the 1-level and 2-level levels. It divided photograph in two parts with up and down iterations. 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. Suggested technique differs from conventional data concealing algorithms in that it may hide information of a substantial quality.

A. Data Encryption Scheme

The presented method carries out the cryptographic system. Encryption and decryption procedures make up the cryptographic system. Using a secret public key, odd part is encoded utilizing AES algorithm. Even sections are encrypted using the RSA algorithm and a hidden private key. the client edge's usage of hidden key during the decryption procedure. 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 which is not known to the secret key or additional knowledge. Finding secret key with aid of the session key and techniques might impossible. One key, the private key for encryption, is all that is necessary to offer the obfuscation 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 among communicator and recipient. It’s the outcome for 1997 competition. The NIST has urged current parties across everyone to provide suggestions for unique benchmarks. They were expected to support a block size of at least 128 bits in all submitted ideas, and the three primary volumes. AES's final standard were introduced in the year 2001, shows how the main cypher system works. Rijndael algorithm's simplicity and ease of hardware and software implementation were key factors in its success.

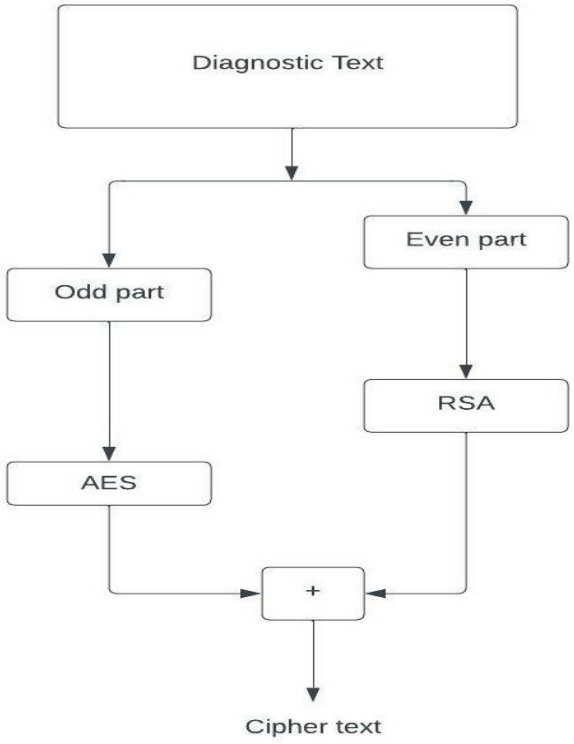

Fig. 6. Data encryption scheme

B. Embedding Procedure

The A Haar-DWT was used in this procedure. With regard to Haar-DWT, 2D-DWT-3L may be formulated that applies low- and high- filters with the picture’s row before the outcome is deconstructed along the image's columns.

The main picture and a hidden data message are inputs into the embedding process, which generate a steganographic-picture. While the hidden message is conversely captured throughout the extraction procedure. The hidden data is transformed to ASCII during the embedding procedure and further cloaked in in-plane variable is determined by HH3.

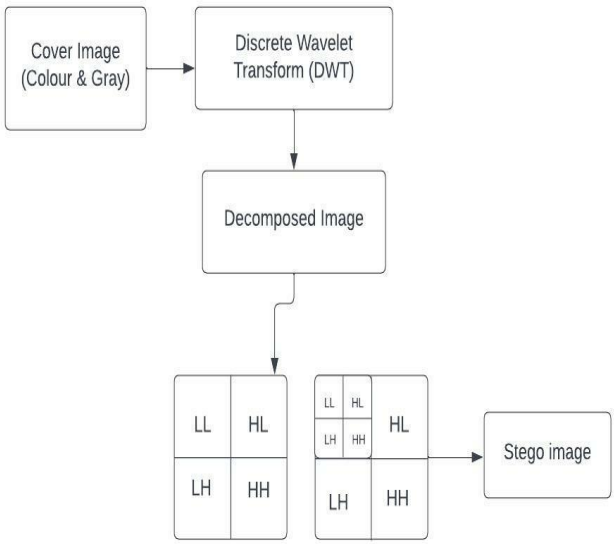

Fig. 7. Steganographic scheme

C. Extraction Procedure

The 2D-DWT method basically utilised to decode the hidden data which was encoded and further integrated into the main picture. The main picture in which the hidden data was integrated is created from the approximate reconstruction after the hidden information was retrieved by invoking the ID-DT2 for the initial level and then, and the second stages after that.

Discrete Wavelet Transform

A wavelet function is any mathematical transformation in which the wavelets are uniformly generated. 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 decided to implement to the entire picture, this shortcoming of DCT is lessened when employing it. Instead of any constraint artefacts, DWT offers improved compression of energy 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 filter (L): In contrast to a higher one, a lower pass filter retains pixels with low frequency information.

In order to effectively deconstruct the signal, it is split further in 2 ways: the clarified explained part (higher one) and the estimation part (lower one), Then further these signals are sub divided into 4 sub parts in a picture which are (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 factored into further 4 more sub parts.

The hidden text data are concealed into all other parts except the lower part since, our eyes are more delicate to the lower parts. Because the other three

parts consist of higher parts and consequently include any kind of data, concealed text into them will not significantly distort the picture. 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.

D. Decryption scheme

Decryption is the method of returning encoded information into the readable form that will familiar to everyone; 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.

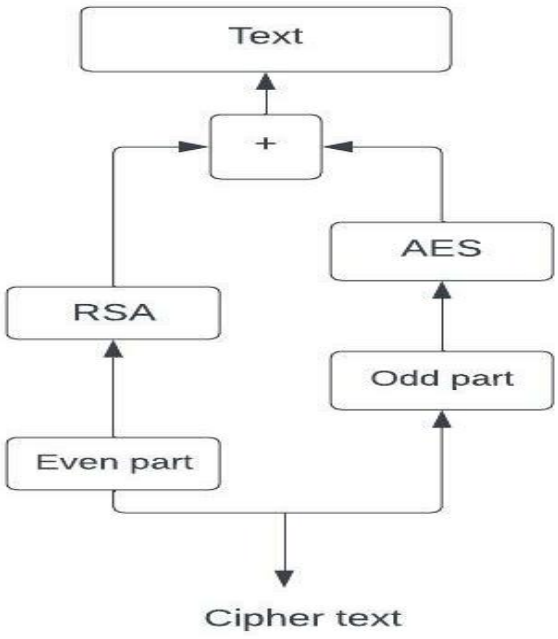

Fig. 8. Decryption scheme

E. Proposed Methodology

- Algorithm 1: AES and RSA algorithm
  The normal data is divided into odd and even fragments during the encoding method, respectively.
  T-ODD is encrypted with AES utilising a set of private public keys. T-EVEN is encrypted with the RSA using the hidden key.

- Algo 2: 2D-DWT-2L Algorithm
  Low- and high- filters can be utilised to create the consecutive transformation known as 2D-DWT-2L.
  Least significant bit:

1) Determine the pixel's value.
2) Transform it into its corresponding binary form.
3) Correctly adjust the least significant bit.

F. Data Flow Diagram

A data flow diagram (DFD) is a graphical representation of an example. It serves as an example of how information will "flow" through a sequence, representing the method element. They frequently serve as an initial step in developing a broad understanding of the procedure that will be described later. A DFD shows the various input data types in relation to the output as well as the approach and departure points for the information as well as the manner in which it will be gathered.

It doesn't explain how the methods will be used in succession or if they will operate jointly or independently.

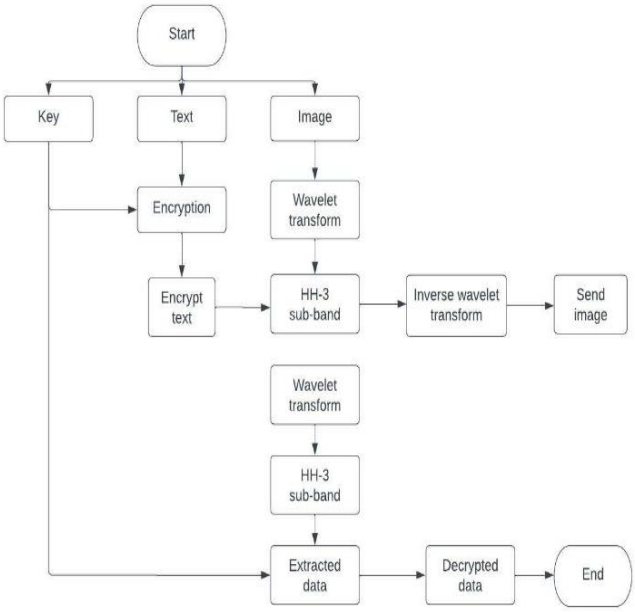

Fig. 9. Flow diagram

Proposed system Advantage

- Steganography has the advantage that it may be used to send classified communications without the transmission being noticed.
- AES is quicker, and the transfer of data is safe, secure, and protected.
- AES keys can be up to 128,192 or 259 bits long, making them more difficult to crack than DES keys. The encrypted text is placed in the wavelet converted image's LL-sub band.
- When compared to current methods, the developed scheme showed its ability to conceal the client's information into a main photograph with strong visual quality, reduced ability, and little modification in the resulted picture.

G. Convert Plain 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 all rounds. The byte substitution, 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. Circular bytes are utilised in shift rows. Shift in each row, keeping the first row intact while shifting the 2nd row rotate the row 1-byte from left to right and the 3rd rotate the row 2-bytes from left to right. It can also process and decrypt inverts by shifting each row one byte to the right. Each column is broken down and analysed, and every byte is changed with a number that depends on every byte in that column. Since the steps are carried out in reverse order, AES decryption is not the same as encryption, but it is said that it has the similar process but in opposite cypher with same steps which was occurred in encryption but the keys are different ever time.

Choosing a folder for a picture:

Choose an image folder that person wishes to conceal text behind first. Also, chosen picture should have a set length and breadth. When you

save picture in a folder as a jpg, it becomes an authentic image file.

Image Steganography

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 LL Sub band must be used for the binary cypher. The image may be returned to its original size by using the IWT function. Then the recipient receives the picture.

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 then split the picture into four parts as LL, LH, HL, and HH. Select the necessary LL part into 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.

Image Restoration:

The data folder is opened with the f-open function and saved in the consonant "fid," while 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 sequence is put into the appropriate sub-parts in order to conduct various additions and subtractions on it. The text can be used to restore the image**.**

IV. EXPERIMENTAL SETUP

The fundamental goal of the project is essentially changed at the execution step in order to run code. The stage's intention is to translate the goal focused on the best possible outcome into the proper coded language. The execution portion of the work is covered in this section, along with information on the programming language and development methodology used. Through its step-by-step approach, it also gives a basic overview of the key elements of the project.

The following tasks are part of the execution phase:

1. Meticulous planning.
2. An examination of restrictions and structure.
3. Set goals for the methods to finish the transformation.
4. Then inspection must be done for the transformation process.

5 Appropriate analysis of the suggested choice.
6 Relevant vocabulary choice for the development of program.

A. System requirement specification

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.

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

1. Processor required: Intel core i5.
2. Space requirement: 1GB (minimum).
3. RAM: 4GB.

- Software Requirement: 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)

B. MATLAB

The numerical computational environment and fourth-generation programming language is called MATLAB. [19] Matrix manipulation, function and visualization of data, algorithm implementation, user interface design, and interface interaction with programmes written in other languages, such as C, C++, Java, and Fortran, are all possible with MATLAB, a tool created by Math Works.

In 2004 there were about a million users using MATLAB in both business and academia. Every research institution, as well as commercial businesses, frequently utilise MATLAB.
It is increasingly used in academia, 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 programme. Typing MATLAB code into the Window, is one of the components of the MATLAB Desktop, is the easiest way to run it.
Many different tools are available in MATLAB for recording and sharing your work. You may easily contribute your work or MATLAB functions as well as combine your MATLAB code with different coding style and software.

Toolbox for Processing:
The visual studio enables the execution of picture enhancement, image background subtraction, distinctive feature recognition, echo cancellation,

edge detection, numeric deformation, and pattern classification.

- 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, CT and MRI scanners, and other diagnostic tools. As a result, such pictures can be viewed, studied, and transformed into a range of data forms. 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.

Features of MATLAB:

- A developing framework for organising code, folder, and info.
- Variety of tools for explorations, patterns, and solving issues.
- High-level language for technical computing.
- Mathematical operations for numerical integration, filtering, optimization, Fourier analysis, statistics, and linear algebra.
- Graphics tools for data presentation.
- Instruments for providing unique GUI.

The MATLAB environment is extended by add-on toolboxes (collections of specialised MATLAB functions) to address specific kinds of issues in certain application areas.

Personal PCs, sophisticated server systems, and the Cheaha computing cluster all can easily worked up on MATLAB. This toolkit also enables the offloading of computationally demanding jobs to the campus compute cluster Cheaha. In addition, the basic operators, when necessary, are configured to handle matrices. And much of the tedious housekeeping that makes all this possible is handled by the MATLAB environment.

C. Language interaction

- Developing Framework

Start-up for construction of a system 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.

- Creating Applications/ 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

Check the code and analyse the features and maintain the data.

- MATLAB Tester

The time taken to execute every single line of code by MATLAB PROFILER.

- Database REPORTS

Report over effectiveness, file management after scanning every file in a directory.

D. Designing Graphical user interfaces

By laying out, designing, and editing user interfaces using the interactive GUIDE tool. With GUIDE, you may add MATLAB plots, Microsoft ActiveX controls. As an alternative, you may use MATLAB routines to programmatically generate GUIs.

E. *Environment for Development*.

You may utilise MATLAB functions and files with the aid of this group of tools and resources. The user interfaces for most of these programmes are graphical.

- Work with graphics.

The MATLAB graphics system are visible over here. It used high-level for image processing, animation, 2,3-dimensional data visualisation, and presentation graphics.

F. The Application Program Interface for MATLAB (API).

- Command window

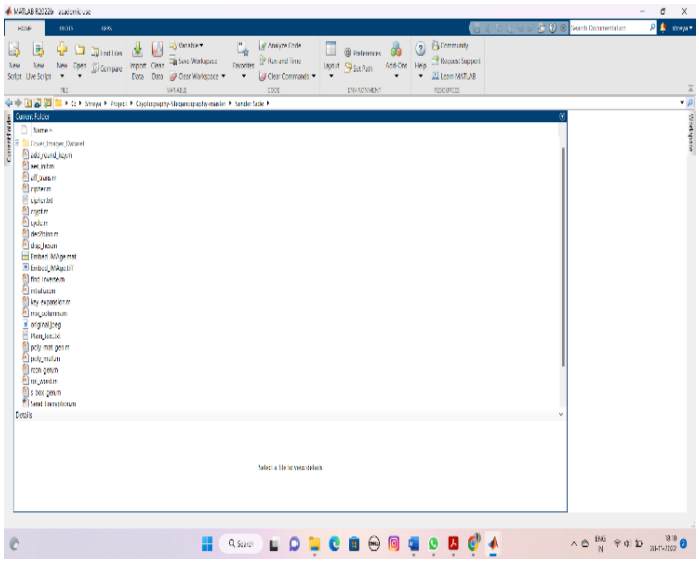

Fig. 10. Command window

- Command Priority

The Command History window keeps track of the lines you type in Window. You may use functions which you have used before as well as copy and run certain lines from the Command History.

- Run Third-Party Programs

From the MATLAB Command Window, external programmes may be launched. 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

The MATLAB desktop includes a built-in Web browser called the Help browser that shows HTML documents.

Click the help button or enter help browser in the Command Window to launch the Help browser. The Help Navigator, that can used to discover information, and the display panel, which shows the data, 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.

- 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 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.

G. 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

1. Request Path

MATLAB provide a search button to locate the files which are arranged in the directories of the app and anyone can easily figure out the functions and their executions. The latest directory on search button must contain multiple files which you can access in MATLAB and easily launch them too.

2. Workspace Browser

The variables accumulated throughout the session and kept in memory make up the workspace. Use the workspace browser or the who and who's functions to explore the workspace and details about each variable.

Select the function, 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. 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 Data from the menu or use the load function data to read in MAT-file.

- Array editor

To view the function in Editor you need to double click on that thing. In the workspace, strings, cell arrays of strings, and 1,2-dimensional arrays may all be viewed and edited visually using the Array Editor.

- Editor/Debugger

Create and debug files, that are programmes you build to run MATLAB, using the Editor/Debugger. This offers a graphical user interface for file debugging in summing up to simple text editing. Any text editor, such as Emacs, may be used to produce M-files, and settings can be used to choose that editor as the default. If wanted to utilised 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.

H. Data Analysis and Access

The whole data analysis process is supported by MATLAB, including data collection from other equipment, analytics, and compression, visualisation, and digital analysis, as well as the creation of output suitable for presentations.

1) Data anatomy

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

- Correlation,
- Thresholding and smoothing
- Extracting parts of data
- scaling, and averaging
- Matrix analysis;

2) 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.

3) 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:

- Direction and speed.
- Histograms.
- Surfaces
- Polygons
- Bubble/scatter plots
- Animations.

Volume visualization and 3D plotting

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

V. RESULT AND ANALYSIS

AES Encryption

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's substitution employs a single 16x16 byte table that contains a permutation of all the given values. The byte indexed with row and column replaces each state byte. Circular bytes are utilised in shift rows. The byte indexed with row and column replaces each state byte. Circular bytes are utilised in shift rows. 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 handled by column and invertible for encoding. AES decryption is not the same as encryption because the steps are carried out in the opposite order, but it is defined as an equivalent inverse cypher that uses the same steps as encryption but with a different key.

1. Performing numeric computation

These complexes mathematically sophistication equations form the foundation of the MATLAB language. The LAPACK and BLAS libraries for linear algebra subroutines are utilised by the basic mathematical operations.

The following categories of functions are available in MATLAB for carrying out mathematical operations and data analysis:

- Manipulating matrices and linear algebra
- Data analysis and statistics
- Optimization and quantitative incorporation.
- ODEs, sometimes known as ordinary differential equations, and PDEs, or partial differential equations (PDEs).
- Operations on sparse matrixes.

Doubles, singles, and integers are only a few of the many data types that MATLAB can operate on in its arithmetic operations.

After receiving a picture as input, the network returns a tag to every object depicted in the picture along with the possible outcomes for every segment of object.

- Explore and load picture data.
- Specify the architecture of the network.
- Provide choices for training.
- Develop the network.
- Determine the classification accuracy and predict the labels of fresh data.

RSA Encryption

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

Encryption

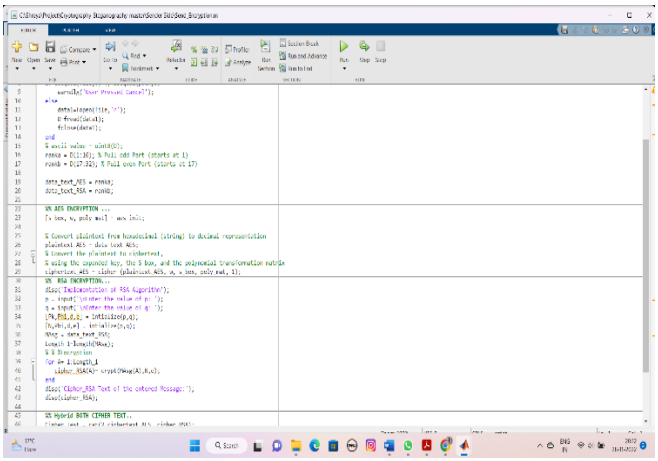

Fig. 11. Encryption code

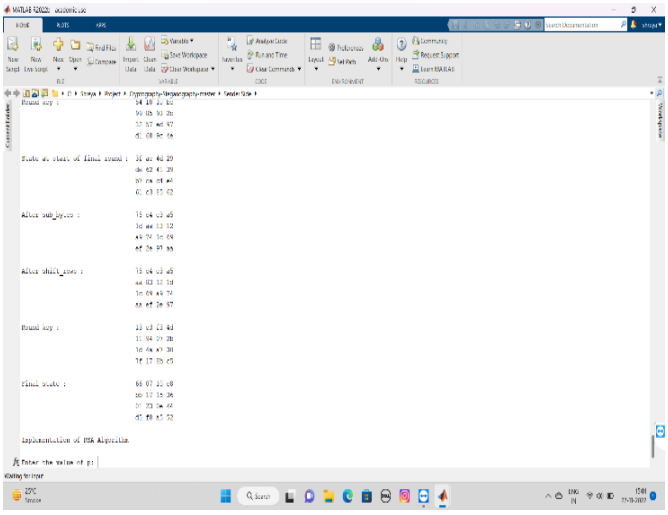

Fig. 12. Encryption process

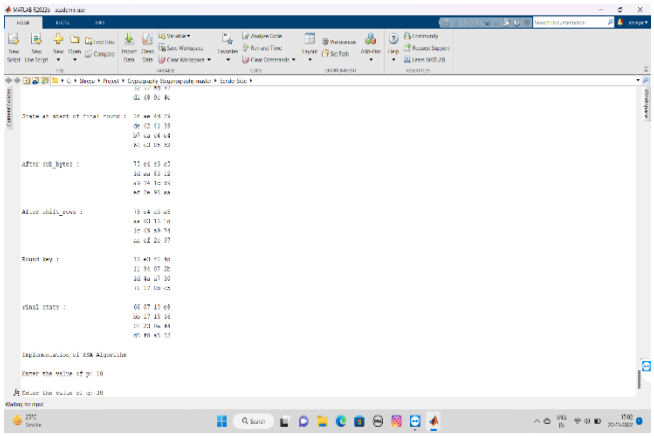

Fig. 13. Input key values

Select text to encrypt

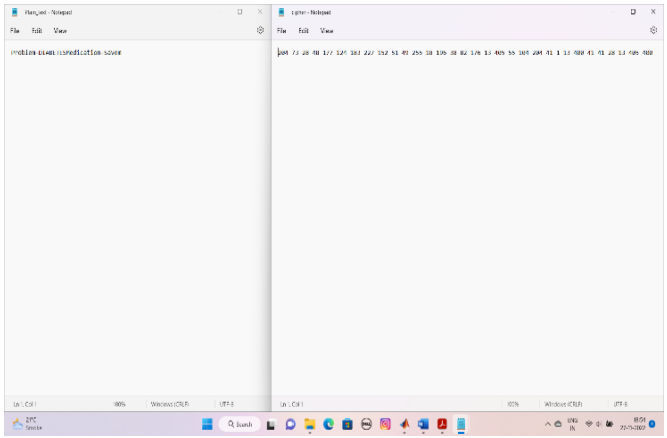

Fig. 14. Cipher text

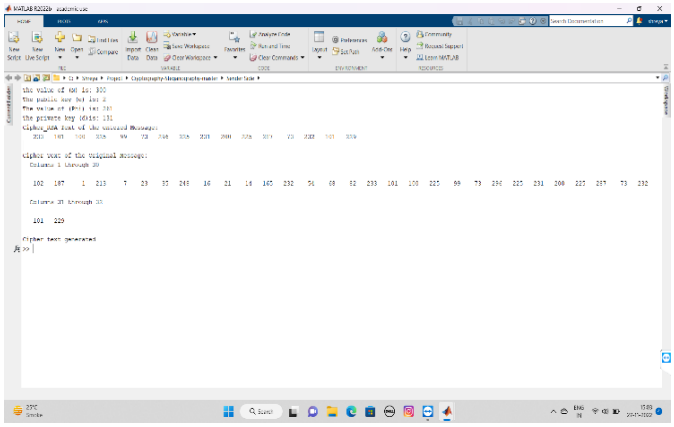

Fig. 15. Cipher text generated

Decryption

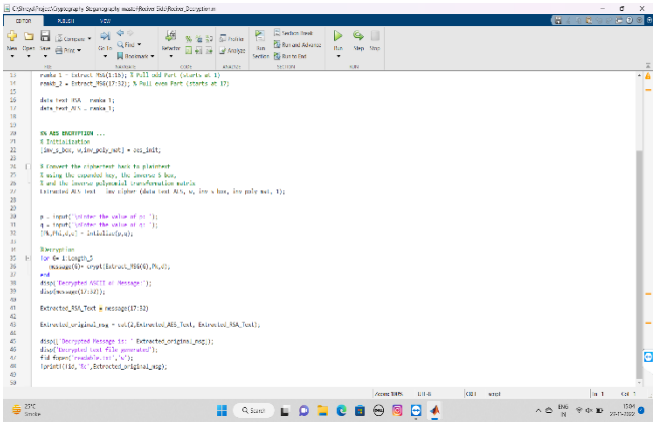

Fig. 16. Decryption code

Decrypted data

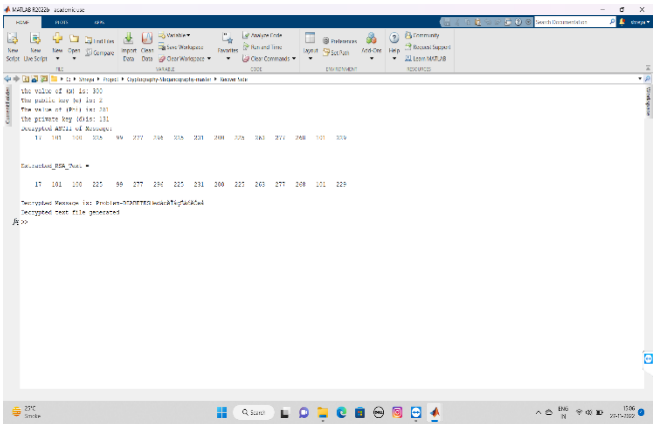

Fig. 17. Plain text

A. 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 LL Sub band must be used for the binary cypher. The image may be returned to its original size and recipient receives the picture.

Sender side

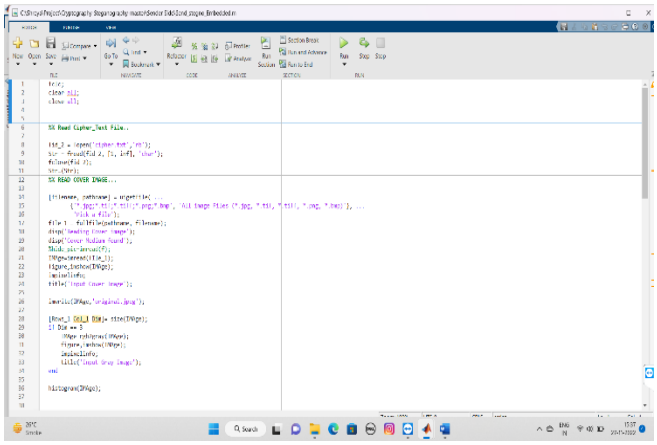

Fig. 18. Read cover image code

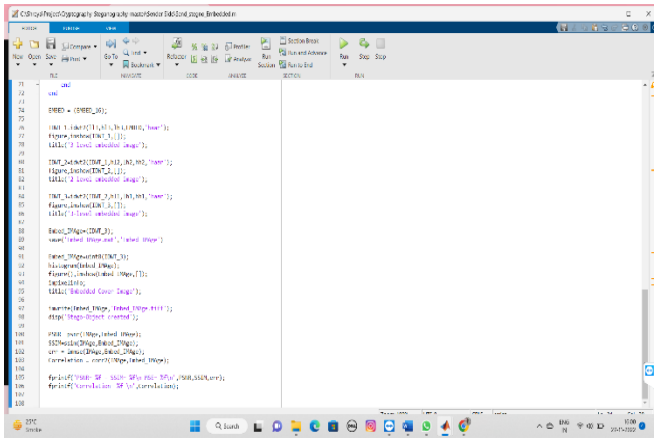

Fig. 19. Decomposed cover image

Input Colour image

Fig. 20. Normal image

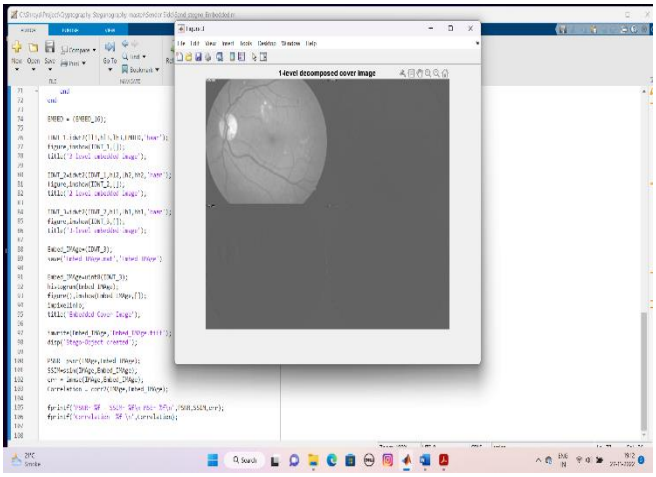

Fig. 21. 1-level decomposed

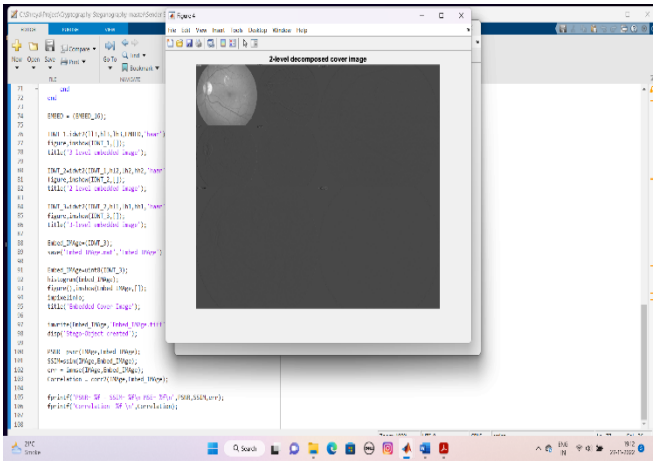

Fig. 22. 2-level decomposed

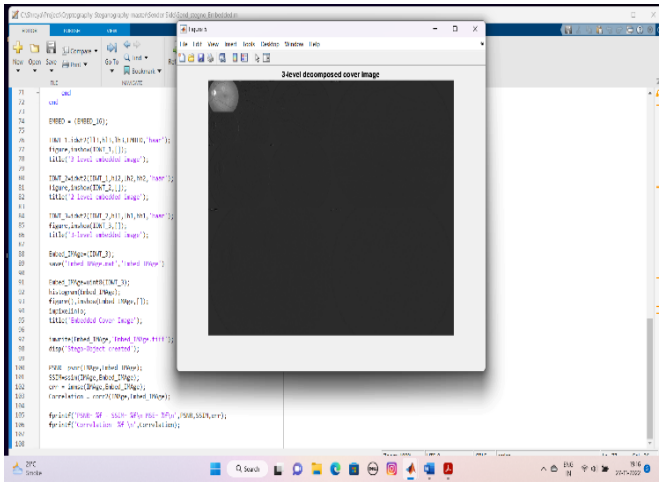

Fig. 23. 3-level decomposed

Receiver side

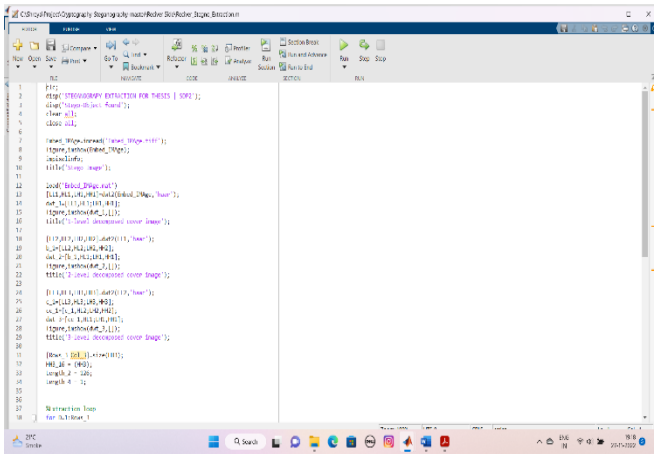

Fig. 24. Extraction code

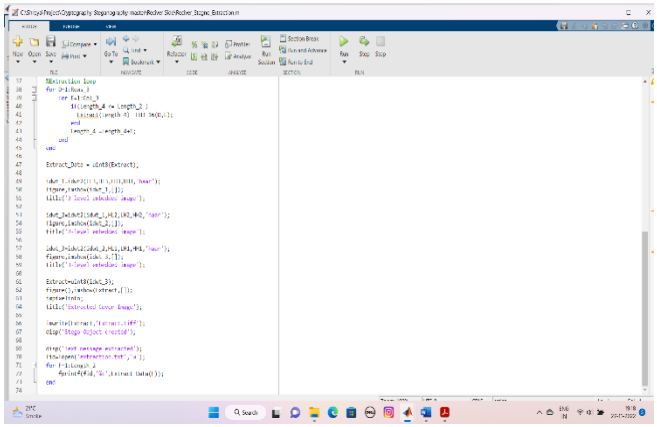

Fig. 25. code

Extracted Image

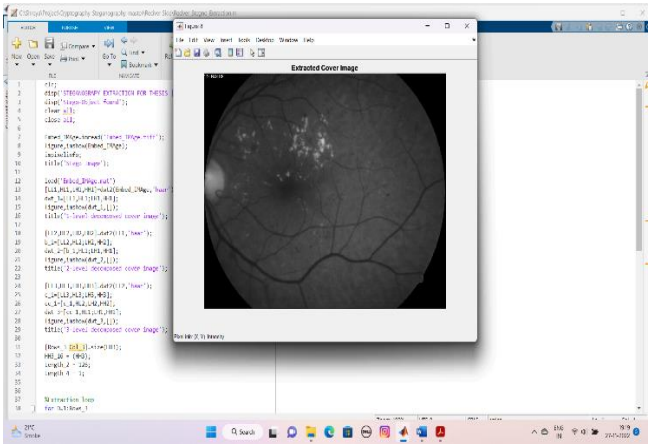

Fig. 26. Grey extracted image

VI. EVALUATION AND DISCUSSION

We compare our method with 100% 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.

Coloured Image

Fig. 27. Coloured image

Values

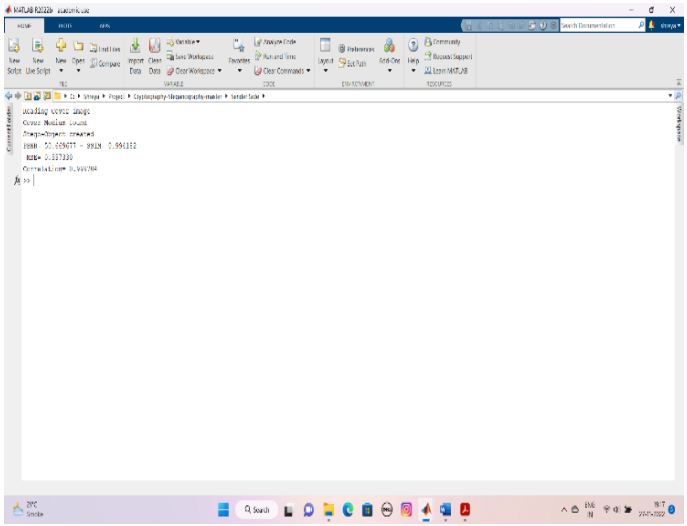

Fig. 28. PSNR, SSIM and MSE values of coloured image

Graph

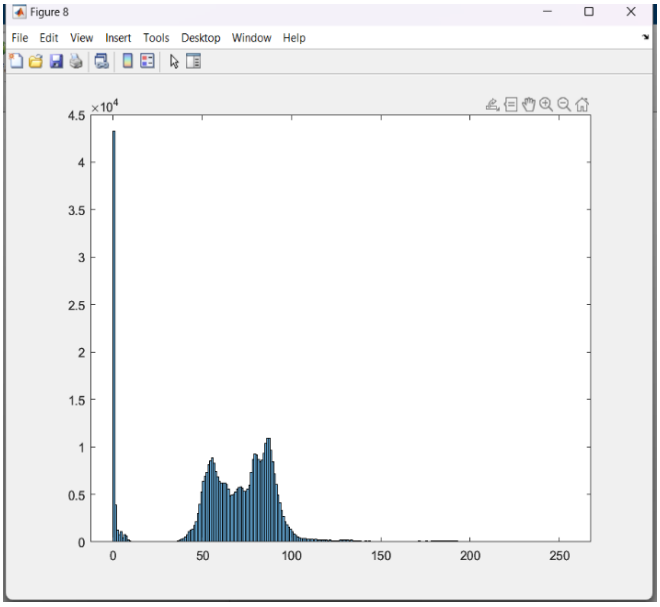

Fig. 29. Graph of coloured image

TABLE 1 Results of PSNR and MSE value of coloured format of data set

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

Grey Image

Fig. 30. Grey image

Values

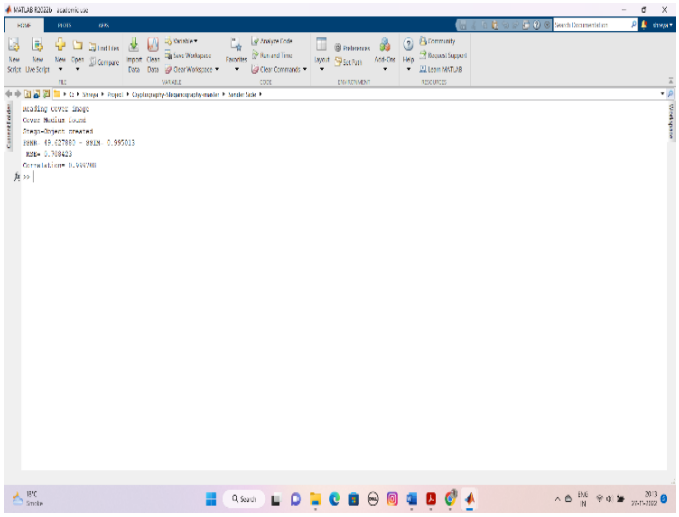

Fig. 31. PSNR, MSE and SSIM values of grey image

Graph

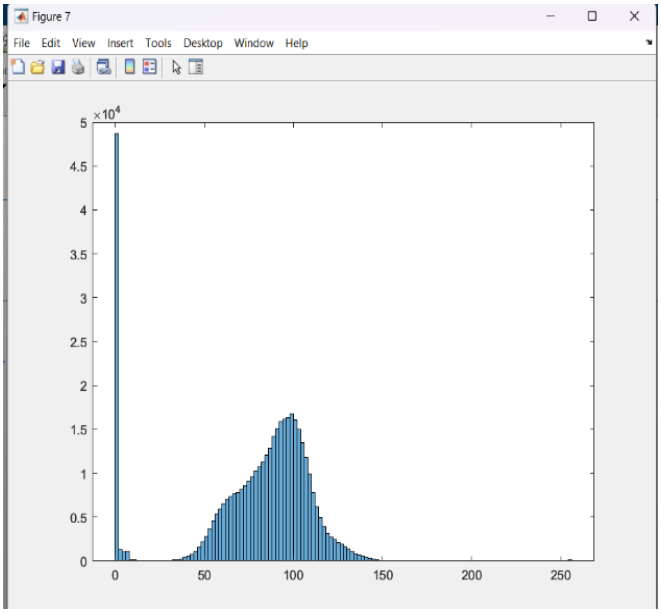

Fig. 32. Graph of grey image

TABLE 2 Results of PSNR and MSE value of grey format of data set

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

A. 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 MSE 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 lower MSE value.

TABLE 3 Comparison

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

VII. CONCLUSION AND FUTURE SCOPE

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 greyscale pictures with variety of content, all of the two implied steganography techniques (LSB and 2D-DWT-3L) along with the encryption techniques (AES and RSA) algorithms performed better. That will be only depend on 4 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 pepper picture, it was discovered that if the text size will increase then it will automatically increase the PSNR readings. This demonstrates the resemblance among the real picture and the stego picture reduces when data 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, in real image.

The PSNR readings followed a different pattern with the grayscale pictures, where the values fell as the text size increased. The MSE data along with greyscale photographs, where the data fluctuated from a picture 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.

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, our suggested approaches fared better at concealing sensitive information than the standard methodologies used in this analysis.

VIII. FUTURE WORK

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, different text in the main picture may use to create a powerful strategy for concealing Arabic text. On a massive implementation, we'll attempt to imitate the behaviour of several nature of the interaction. 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.

REFERENCE

[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** 012016https://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.