



Daffodil
International
University

Image Steganography with Triple DES and Random Pixel Selection: A Secured Data Hiding Approach

Submitted by

Fuad Ahamed Rahat

ID – 201-35-2999

Department of Software Engineering
Daffodil International University

Supervised By

Md. Maruf Hassan

Associate Professor

Department of Software Engineering, FSIT
Daffodil International University

This Thesis report has been submitted in fulfillment of the requirements for the Degree
of

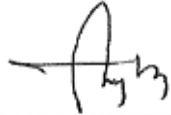
Bachelor of Science in Software Engineering.

Fall-2023

© All right Reserved by Daffodil International University

APPROVAL

This thesis titled on “Image Steganography with Triple DES and Random Pixel Selection: A Secured Data Hiding Approach”, submitted by Fuad Ahamed Rahat (ID: 201-35-2999) to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.



BOARD OF EXAMINERS

Chairman

Dr. Engr. Abdul Kader Muhammad Masum
Professor

Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



Internal Examiner 1

Md Khaled Sohel
Assistant Professor

Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



Internal Examiner 2

Fatama Binta Rafiq
Lecturer (Sr. Scale)

Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University



External Examiner

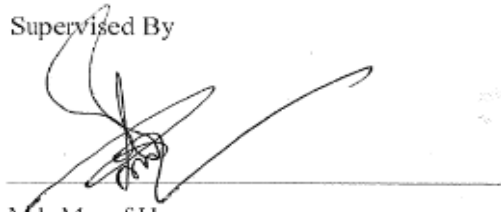
Dr. Md. Manowarul Islam
Associate Professor

Department of Computer Science & Engineering
Jagannath University

DECLARATION

I, hereby declare that, this thesis report is done by me under the supervision of Mr. Md. Maruf Hassan, Associate Professor. Department of Software Engineering, Daffodil International University, in partial fulfillment my original work. I am also declaring that neither this thesis nor any part therefore has been submitted else here for the award of Bachelor or any degree.

Supervised By



Md. Maruf Hassan
Associate Professor,
Department of Software Engineering,
Daffodil International University.

Submitted By



Fuad Ahamed Rahat
ID: 201-35-2999
Department of Software Engineering,
Daffodil International University.

ACKNOWLEDGMENT

First of all, I am grateful to the Almighty Allah for making me eligible to complete this thesis. Then I would like to thank my supervisor **Md. Maruf Hassan, Associate Professor, Department of Software Engineering**. I am extremely grateful and indebted to her as she has given me her expert, sincere and valuable guidance and encouragement. I would like to thank everyone who helped me in my thesis by their important suggestion. Without their passionate participation and input, the thesis could not be successfully conducted. I take this occasion to convey my sincere thanks to all faculty members of the Department of Software Engineering for their help and encouragement.

ABSTRACT

In recent years, the fast development of digital communication and information technology has made it crucial to ensure secure data transfer between the sender and the recipient. Steganography thus introduces a strong way to communicate secret data and conceal information in the right multimedia carrier, like that image, both audio and video files. In this work, we explore an innovative approach to image steganography, integrating the Triple DES encryption algorithm and a Random Selection of Pixels technique to enhance the safety and imperceptibility of hidden data. The encryption process involves the Triple DES algorithm for robust protection of confidential information, while a strategic Random Pixel Selection method ensures discreet embedding within the image. 3DES uses a 168-bit key length which is much more secure than a 56-bit key of DES, making it more resistant to many attacks. An additional layer of security is provided in 3DES through the alternative use of DES. Even if one of the keys is compromised, the intruder would need to break two more layers of encryption. Then, Random pixel selection can enhance the security of the steganographic technique. By choosing pixels randomly and employing an 8-directional pixel selection approach, the pattern of changes in the image becomes less predictable. This randomness can make it more difficult for opponents to detect the existence of secret information. The distinctive contribution of this work lies in its ability to significantly improve imperceptibility compared to existing methods, offering a robust and visually seamless data hiding approach within the realm of image steganography.

Keywords: Image Steganography, XOR, 3DES algorithm, Random Selection of Pixels technique, LSB (Least Significant Bit), 8 Directional pixel Selection

TABLE OF CONTENTS

APPROVAL	i
DECLARATION	ii
ACKNOWLEDGMENT	iii
ABSTRACT	iv
Chapter 1: INTRODUCTION.....	1
1.1 Background	1
1.2 Fundamental requirement for steganography.....	2
1.3 Problem Statement	2
1.4 Research Objective	3
1.5 Scope of works	4
1.6 Contribution	4
1.7 Solution requirement.....	5
1.8 Thesis Outline	6
Chapter 2: Literature Review.....	8
2.1 Commencement of the study.....	8
2.2 The history of image Steganography	9
2.3 The evaluation of image Steganography over time.....	10
2.4 Application of image Steganography	11
2.5 Research Gap.....	14
2.6 Research Objective.....	15
2.7 Closure of this study.....	16
Chapter 3: Methodology	18
3.1 General Steganographic System.....	18
3.2 Proposed Method.....	19
Chapter 4: Result and Discussion	34
Chapter 5: Conclusion and Future Scope.....	42
References.....	43

TABLE of FIGURES

Fig 1.1: Image Steganography Approach.....	5
Fig 3.1: General Steganographic System.....	18
Fig 3.2: Embedding process of the proposed Approach	20
Fig 3.3: Retrieve process of the proposed Approach	21
Fig 3.4: Block Diagram of the proposed image Steganography Approach	22
Fig 3.5: Diagram for Triple DES algorithm.....	25
Fig 3.6. Encryption and Decryption Process of 3DES.....	26
Fig 3.7: Select pixels at random to hide information.....	27
Fig 3.8: Each pixel's byte of text to be embedded (Red, Green, Blue).....	28
Fig 3.9: Random pixel selection	28
Fig 3.10: XOR Embedding Process	30
Figure 3.11: 8 Directional pixel Selection	31
Fig 4.1: GUI Of the Proposed method Implementation.....	37
Fig 4.2: Implementation of MATLAB Code.....	39

LIST OF TABLES

Table 1: Literature Review Table	17
Table 2: Table of results for the stego image analysis	34
Table 3: A comparison between the Stego image histogram and the cover image	35
Table 4: Comparison PSNR of our proposal with other researchers	40
Table 5: Comparison MSE of our proposal with other researchers	41

Chapter 1: INTRODUCTION

1.1 Background

Steganography has become an essential discipline as a result of the demands of protecting sensitive data and guaranteeing its covert transmission in the ever-changing world of digital communication and information exchange. In particular, image steganography has attracted a lot of attention due to its capacity to enshrine hidden information in the visual content of images, providing a discrete means of transmitting secure data. Over the course of a year, the information flow in the twenty-first and twenty-first centuries has grown quickly, with communication media utilizing a large amount of data that is exchanged through the Internet [1].

The present thesis explores the field of image steganography, concentrating on a novel technique named "Image Steganography with Triple DES and Random Pixel Selection." This method aims to combine the powerful encryption powers of the Triple Data Encryption Standard (Triple DES) with a deliberate pixel selection mechanism in a world where protecting digital data is critical. Combining these components results in an advanced and secure data hiding strategy that attempts to improve the privacy, accuracy, also imperceptibility among the hidden information. Researchers are compelled by the proliferation of information to create security protocols and safeguard data transmission between sender and recipient from cyberattacks [2].

Symmetric key block cipher Triple DES is well known for its strong cryptography and has been used extensively to protect sensitive data. In the context of image steganography, using Triple DES adds a strong layer of security to the concealed data, guaranteeing that an advanced encryption algorithm prevents unwanted access. In order to generate stego images (stg) with high imperceptible security, steganography algorithms must operate at multiple security levels [3].

Furthermore, this thesis incorporates a random pixel selection mechanism, adding a new dimension to the steganographic Procedure. The objective of the random pixel selection procedure is to make the embedded information more difficult to detect visually and stealthier. The proposed approach seeks to achieve a balance between perceptual transparency and embedding capacity by avoiding predictable patterns and selecting pixels at random locations within the image. This

ensures the effectiveness of the steganographic process. Numerous researchers are focusing on the frequency domain to improve camouflage and conceal sensitive information in JPEG images, but the embedding rate is constrained[4].

In an age where digital security is crucial, the combination of Triple DES and random pixel selection in image steganography represents a progressive step toward advancing the state-of-the-art in secure data hiding. This thesis looks at the suggested method's security, effectiveness, and potential applications in the broader context of secure digital communication. To that end, it investigates, implements, and evaluates the method.

1.2 Fundamental requirement for steganography

The three key components within a successful steganographic technique are in robustness, capacity, and imperceptibility. Maintaining that cover medium's visual and aural qualities while encoding the secret data is necessary for imperceptibility. For example, imperceptibility in image steganography makes sure that pixel value changes are sufficiently subtle to elude detection by statistical analysis tools and human eyes.[5] Achieving a delicate balance where changes are both imperceptible and resilient enough to withstand attempts at detection is the aim. The quantity of secret information that is embeddable within a specific cover the medium without compromising imperceptibility as is known as capacity, and it is another essential component of steganography. Greater capacity is important to take into account when designing steganographic systems because it enables the transmission of more data. To satisfy particular needs, one must carefully weigh the trade-offs between increased capacity and decreased imperceptibility. [6]Robustness describes a steganographic methods capacity about preserve this confidentiality that of concealed data in the face of possible attacks or modifications to the carrier. To ensure reliable extraction of the hidden data under a variety of conditions, a robust steganographic method should withstand multiple attacks, including compression, cropping, and other common transformations.

1.3 Problem Statement

The problem statement draws attention to the difficulties that come with image steganography, particularly the difficulty of finding a compromise between data security and image quality. This equilibrium has historically proven difficult to achieve with conventional encryption techniques.[7] The challenge is further compounded by the need to maintain minimal imperceptibility in image steganography. Therefore, it is imperative to investigate novel strategies

that tackle the security issue as well the hidden imperceptibility data in images[8]. In order to overcome these obstacles, the proposed research will simultaneously develop a technique to improve the imperceptibility of embedded information in the image steganography and introduce a novel encryption method that strikes the ideal balance between data security and image quality[9]. The goal of this dual-focused research is to advance the field of secured data hiding within images by offering a comprehensive solution.

PS1 → Balancing security and image quality remains a challenge due to reliance on conventional encryption

PS2 → Maintaining less imperceptibility in image steganography

1.4 Research Objective

The goal of the research is to address the intricate issues surrounding image steganography. Proposing an encryption method that optimizes the trade-off between data security and image quality is the primary objective of RO1. This objective recognizes the difficulties that conventional encryption methods presently face and aims to create a fresh strategy that, when used in conjunction with steganography, enhances overall data security. Simultaneously, RO2 seeks to demonstrate a spatial steganographic technique whose goal is to boost imperceptibility. This objective directly addresses the challenge of maintaining minimal visual impact in image steganography by focusing on improving imperceptibility.[10] Through the use of a spatial domain-focused steganographic algorithm, the combined research objectives seek to offer a comprehensive solution by introducing an innovative model that strengthens data security while also greatly enhancing the imperceptibility of hidden information within images.

RO1 → To propose an encryption method that achieves a more optimal trade-off between ensuring data security and maintaining the quality of the image.

RO2 → To propose a technique that simultaneously enhances the imperceptibility of the image steganography

Mapping:

1.RO1→PS1

2.RO2→PS2

Problem statement PS1, which illustrates how difficult it is to use traditional encryption techniques in image steganography while maintaining security and image quality. The consistent research objective (RO1) seeks to develop an encryption technique that more successfully strikes a balance between data security and image quality protection. Stated differently, the goal is to create a novel encryption technique that minimizes the effect on the cover image's visual quality while optimizing the security of the steganographic process. This mapping implies that developing a more advanced and efficient image steganography technique requires resolving the problems with conventional encryption. Problem statement PS2, which emphasizes the difficulty of preserving low imperceptibility in picture steganography, is the subject of the second mapping. In line with this, research goal RO2 seeks to suggest a method that also improves the image steganography's imperceptibility. To put it another way, the goal is to create and develop a spatial steganographic algorithm that greatly increases the hidden data's imperceptibility in the image. According to this mapping, the imperceptibility problem has to be solved as one of the most crucial things that can be done for improving image steganography. The suggested technique should be specifically designed to improve the visual transparency of the steganographic process.

1.5 Scope of works

This paper will only address image steganography with the solution I will offer. For steganography of audio or video, it is not applicable. We are doing small-scale work on this paper at the moment. I would recommend using audio or video in this topic's future research.

1.6 Contribution

The following is this paper's contribution:

- The proposed approach come out from traditional pixel selection technique where random pixel selection technique is used that is difficult to attackers to recognize the presence of secret data.
- Both the 3DES algorithm and XOR-based LSB provide good image quality as well as enhance the imperceptibility of the image.

1.7 Solution requirement

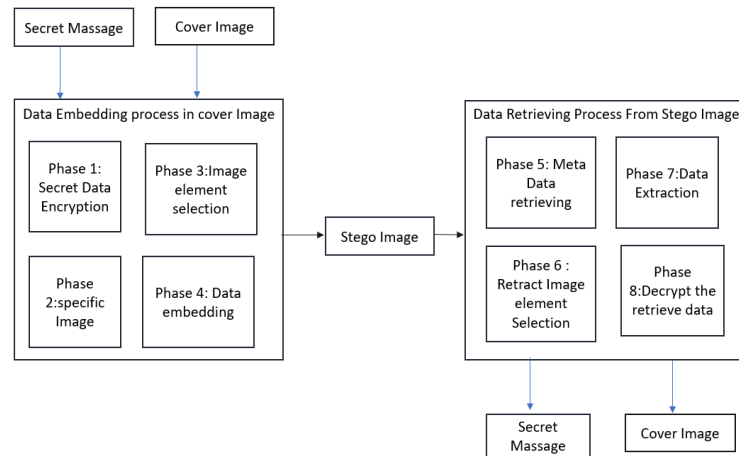


Fig 1.1: Image Steganography Approach

First of all, let me describe the Data Embedding Process. In the Phase 1: Secret Data Encryption by 3DES: In this initial phase, the secret data undergoes encryption using the Blowfish algorithm. 3DES is a block cipher with symmetric key. known for its secure and efficient encryption. The algorithm takes the secret message and a confidential key, resulting in a ciphertext that will have embedded in the cover picture. In the Phase 2: Specific Image: A specific cover image is chosen for the embedding process. This image serves as the carrier as for the encrypted confidential information. In this Phase 3: picture Element Selection by Random Pixel Selection: To enhance the concealment of the embedded data, image elements are strategically chosen based on random pixel selection technique. This involves identifying and selecting pixels along random pixels within the image. Phase 4: Data Embedding: In this stage, the chosen picture elements are embedded with the encrypted secret data. The method is to embed the encrypted data into the selected pixels, making sure that the changes are undetectable so as to preserve the cover image's aesthetic integrity. In the Phase 5: Retrieving Metadata: The initial step in the information retrieval procedure is for eliminating metadata for the embedded information. This metadata gives important details about the content that is embedded. Phase 6: Selecting Retract Image Elements Certain image elements are chosen, just like in the embedding process; however, the purpose of this stage is to remove this previously integrated information. The system uses the metadata that

was obtained in the previous stage to inform its selection, which helps it find and identify the precise pixels that have the embedded data. In the Phase 7: Data Extraction: The identified image elements are processed to extract the embedded data. This phase involves carefully separating the concealed information from the cover picture without causing any apparent distortions. In this Phase 8: Decrypt the Retrieved Data: The final phase involves decrypting the retrieved data using the 3DES algorithm with the appropriate key.

Image quality is the primary objective of the steganographic system. The most used metrics for assessing image quality are Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) [6]. One statistic to assess how much the embedded picture has degraded in comparison to the cover image is PSNR.

$$\text{MSE} = \frac{1}{a * b} \sum_{i=0}^{a-1} \sum_{j=0}^{b-1} [X(i, j) - Y(i, j)]^2 \dots \dots \dots (1.1)$$

$$\text{PSNR} = 10 \log_{10} \frac{\text{MAX}_X^2}{\text{MSE}} \dots \dots \dots (1.2)$$

The difference between two images is measured by MSE. Equations 1 and 2 define PSNR and MSE. The dynamic range of pixel values, or the greatest value that a pixel may take for 8-bit images, is I=255. Where are the row and column pixels in the original (cover) image, the row and column pixels in the reconstructed (stego) image, and the height and width of the image.

1.8 Thesis Outline

This content talks about how image steganography has changed over time, with an emphasis on a new method called "Image Steganography with Triple DES and Random Pixel Selection." This technique improves the security and imperceptibility of information hiding in pictures by combining this reliable Triple information Encryption Standard (Triple DES) with a random pixel selection mechanism. It is emphasized that the requirements of robustness, capacity, and imperceptibility are essential when assessing steganographic methods. Innovative approaches are necessary to address the challenges of balancing security and image quality in traditional encryption methods for image steganography. The goal is to present a novel encryption technique, especially designed for image steganography, that strikes the ideal compromise between data

security and image quality. The suggested method minimizes observable changes by directly embedding hidden data into picture pixels in the spatial domain. The paper proposes future research directions in audio and video applications, but its scope is restricted to steganography of images. The paper's contribution is the introduction a new method that improves security and imperceptibility, with an emphasis on image steganography. The proposed method is restricted to images, and it encourages further investigation into analogous techniques for audio or video steganography. In general, the information emphasizes how critical it is to develop safe data-hiding methods in the digital age.

Chapter 2- Literature Review

2.1 Commencement of the study

The approach used within to hide confidential information in an image the fact that it is challenging to identify or interpret is referred to as image steganography. Unlike cryptography, which concentrates on rendering a message's content unreadable to unauthorized users, Steganography tries to obscure the presence of the embedded information rather than its content. The confidential data in image steganography is embedded in the pixels of an image. The most common approach involves manipulating the least significant bits (LSBs) of the pixel values. Since these LSBs contribute less to the overall color or intensity perception, small changes in these bits are less likely to be noticed by the human eye. Applications for image steganography include digital watermarking, secure communication, and copyright protection. But it's important to note that steganography is not foolproof, and detection methods have been developed to identify steganographic or altered images. Researchers continually work on improving both steganographic techniques and detection methods in an ongoing cat-and-mouse game.

The two main categories of image steganography are as follows:

Domain of space: This approach directly embeds the data into the pixel intensity value. It is specifically utilized for lossless compressed images. because the format of the image affects embedding. The replacement of least significant bits (LSB) is a widely utilized approach in the spatial domain.[9]

Transform domain: This approach embeds the data in the previously altered image's frequency domain. To hide data in an image, many transformation techniques such as the Discrete Cosine Transform are employed. JPEG photos that have undergone lossy compression can be used using this approach.[10]

2.2 The history of image Steganography

Image steganography has a centuries-long history, as the concept of hiding information dates back to ancient times. While modern image steganography as we know it today has evolved with advances in technology, the basic principles have historical roots. Here's a brief overview of the history of image steganography:

Ancient Methods:

Ancient Greece: Histories suggest that ancient Greeks used a technique called "scytale" to hide messages. The note was scrawled on a piece of parchment wound around a rod of a particular diameter. When unwound, the message would be scrambled and appear meaningless. The recipient, having a rod of the same diameter, could decode the message.

Invisible Ink: Throughout history, various forms of invisible ink were used to conceal messages. These inks could be revealed through heat, chemicals, or other means.

During Wars and Conflicts:

World War II: Both the Axis and Allied forces used steganography during World War II.[11] For example, microdots—tiny photographs reduced to the size of a punctuation mark—were used to hide information.

Cold War Era: Steganography continued to be employed during the Cold War, with hidden messages in radio broadcasts, letters, and other forms of communication.

Digital Revolution:

- **Early Digital Steganography:** As computers became more prevalent, steganography evolved into the digital domain. Early techniques involved hiding data within the least significant elements of audio and digital image files.

1990s: This field of digital steganography gained attention, and researchers began developing more sophisticated methods. F5, a popular algorithm for image steganography, was introduced during this period.

Advancements in Technology:

- **Late 20th Century:** With the rise of the internet and digital communication, steganography became more accessible. Researchers developed various algorithms for hiding information in images, audio, and video files.

21st Century: Steganography tools and techniques continued to advance, and researchers explored new methods for embedding information while minimizing the impact on the carrier file[12].

Applications and Challenges:

Applications: Image steganography found applications in digital watermarking, authentication, and secure communication. It became a tool for protecting intellectual property and verifying the authenticity of digital content.

Challenges As steganography became more dominant, so did the development of steganalysis—methods for detecting hidden information. This led to an ongoing arms race between stenographers and those seeking to detect hidden content. In summary, image steganography has a rich history that spans ancient civilizations to the digital age[13]. Its evolution has been driven by the changing

landscape of communication technologies and the ongoing quest for secure and covert evidence exchange.

2.3 The evaluation of image Steganography over time

The evaluation of image steganography over time involves assessing the effectiveness of steganographic techniques, the development of detection systems (steganalysis), and overall safety and security and robustness among these systems. Here's an overview of how the evaluation of image steganography has evolved:

Early Assessments (1990s): - In the early years of digital steganography, researchers focused on basic techniques like LSB (Least Significant Bit) embedding. These methods were simple and provided a certain level of concealment but lacked robustness and security. - Assessment criteria included the imperceptibility of the steganographic changes (how visually similar the stage-image is to the original) and the capacity to hide data without causing suspicion.

Emergence of More Advanced Techniques (2000s): - Advanced steganographic algorithms, such as F5 and Outguess, were introduced[14]. These algorithms aimed to improve on the limitations of early methods and provide higher levels of security and robustness. - Researchers began considering metrics such as payload capacity, or the quantity of data that is potentially hidden, resistance to steganalysis, and the ability to withstand common image processing operations without losing the hidden information.

Focus on Security and Robustness (2010s): - As steganalysis techniques improved, the importance shifted to enhancing the security of steganographic algorithms. This involved developing methods to resist arithmetical and machine learning-based steganalysis. - Researchers explored the use of more complex embedding strategies, including spatial domain techniques, transform domain techniques (e.g., frequency domain), and adaptive devices that adjust to the characteristics of the cover image.

Integration with Cryptography (2010s - Present): - To enhance security, researchers explored the integration of steganography with cryptographic techniques. This combination, known as steganographic encryption, aimed to provide both confidentiality and covert communication.[15]

Evaluation criteria expanded to include the defense against assaults like known-plaintext attacks, selected-plaintext attacks, as well adaptive steganalysis.

Challenges and Future Directions: The arms race between stenographers and steganalysis continues. Researchers are faced with the challenge of developing steganographic methods that remain effective while withstanding increasingly sophisticated detection methods. - Ongoing research explores new paradigms, like steganography that is based on deep learning and steganalysis, to address these limitations in

traditional approaches- Real-world applications, such as digital forensics and secure communication, drive the need for steganographic techniques that can operate in diverse and challenging environments. Overall, the evaluation of image steganography has evolved from basic imperceptibility to more complex considerations of security, robustness, and integration with cryptographic methods[16]. As technology advances, the field continues to adapt to new challenges and opportunities, with a focus on providing secure and covert means of information exchange.

2.4 Application of image Steganography

Here are some applications where your proposed approach can be utilized:

- Secure Communication:** - **Military and Defense Communications:** In military and defense applications, secure communication is crucial. Your approach can be applied to embed sensitive information within images, providing a covert means of transmitting classified data.
- Digital Forensics:** - **Watermarking and Authentication:** Your steganographic method can be employed for digital watermarking, allowing for the authentication and tracking of digital media. This is particularly useful in the prevention of unauthorized copying and distribution.
- Intellectual Property Protection:** - **Protecting Digital Assets:** Industries such as media and entertainment can use your method to embed copyright information or ownership details within digital images, videos, or audio files to prevent unauthorized use or distribution.
- Medical Imaging:** - **Patient Data Security:** In medical imaging, ensuring the confidentiality of patient data is paramount. Your steganographic method can be used to conceal private patient data from view in medical pictures while preserving the integrity of the diagnostic data.
- Confidential Document Transmission:** - **Business and Legal Documents:** Your approach can be used for the secure transmission of confidential business or legal documents. Embedding data within images provides an extra layer of security during data transfer.
- Journalism and Whistleblowing:** - **Secure Information Transfer for Journalists:** Journalists and whistleblowers may use your method to securely transmit sensitive information or evidence without attracting attention.
- Research and Academia:** - **Secure Collaboration:** Researchers and academics working on sensitive projects or collaborative research can use your approach to embed information within images for secure communication and collaboration.
- Personal Privacy:** - **Private Messaging:** Individuals concerned about privacy can utilize your method for private messaging. Embedding messages within images adds an extra layer of concealment.
- Digital Rights Management (DRM):** - **Protecting Digital Content:** Content providers can use your steganographic

technique to embed information within images as part of a DRM strategy, preventing unauthorized access or distribution of digital content. Non-Forensic Techniques: Our methodology can readily be linked to anti-forensic techniques, which are utilized in cases where an individual attempts to conceal data from digital forensic examination. It is crucial that I emphasize the benefits of my Triple DES and Random Pixel Selection technique when I present this application in my thesis paper. Enhanced security, protection against specific types of attacks, and resistance to steganalysis are a few of these benefits. Discuss possible drawbacks and real-world application problems in each application domain.

Three main exercises are included in the secure steganography method proposed by the authors in [17] the pseudo-random sequence generator, the Least Significant Bit (LSB) substitution, and the Optimal Pixel Adjustment Process (OPAP). This approach uses two channels as data channels and the remaining channel as an indication channel, which uses the cyclic pixel and indicator technique. For the first pixel, the red plan is used as the channel for indications. On the subsequent pixels, the channels for indications are R, G, and B in a periodic cycle. The other two channels act as the data channels for the relevant pixels in the event that the indicator channel is not present. The bits to be embedded (i.e., the indicator channel's LSBs) depend on the intensity of the pixels. Insert k bits in G and $k+1$ bits in B if the LSBs of the indicator channel, let's say the R channel, are 00; if they are 01, insert $k+1$ bits in both G and B. Put $k+1$ bits in G and $k+2$ bits in B if LSB(R) is 10. Insert $k+2$ bits in G and $K+2$ bits in B if LSB(R) equals 11. To fully integrate data in a unique random number generator, a new 2-key based pseudo random generator is utilized. Fashion determined by the individual.

An image steganography technique based on LSB substitution and random pixel selection inside the necessary image area has been proposed by Madhu et al. [18]. After generating random numbers, it chooses the area of interest along the random pixels where the necessary message is placed. Increasing security in situations where the password is added using LSB pixels is the aim of this technique.

The Triple-A algorithm is an algorithm that was proposed in [18] The hidden message is concealed in the pixels' least significant bits in this algorithm, which follows the same LSB principle but uses A higher level of randomness in choosing the quantity of channels and bits in color. There two components to the algorithm: encryption and hiding. In the covering up phase, the RGB image is

utilized as cover media, and a pseudorandom number generator is needed. The foundation of PRNG is the provision of two fresh random numbers as seeds for every iteration. These PRNGs have two seeds: Seed1 (S1) and Seed2 (S2). Although S2 is restricted to the range [1, 3], S1 is only allowed the generate numbers in [0, 6]. The RGB image component that will be utilized to conceal the encrypted data is chosen using the S1 irrational quantity. However, The (S2) random number determines the number of the component(s) least significant bits that are used to hide the secret data.

One method that has been presented is the spatial domain method [8]. In order to minimize the stego's and the cover's difference, this suggested method's basic idea is To include the message portions into the cover image's third least significant bit (LSB-3). LSB -1 and LSB-2 can then be adjusted based on the message's bits. The key messages have been transposed before being integrated using a stego-key to further secure the data. In contrast to the suggested way, the results of this method demonstrated greater PSNR values, showing that, while keeping the same capacity, the LSB-1 image is of higher quality than the modified one.

In [19], The cover image's pixels are chosen at random using the Pseudo Random Number Generator (PRNG), that conceals each message byte inside three pixels. The peak signal-to-noise ratio (PSNR) of this investigation demonstrates improved visual quality and a potent hiding capacity. Compared to other ways, the method's limited hiding capacity prevents it from concealing other multimedia messages like images and sounds, since it consumes three pixels for every bite.

A hash-based 2-3-3 technique, as presented by the authors in [21], allows for the embedding of eight bits of message into a single pixel, or one character per pixel. As the name implies, this method substitutes the first two bits of the message for any two bits that are present in the least significant nibble (LSN) of the pixel's red value. In a similar vein, the final three bits of the message replace the final three bits of the LSN of the corresponding pixel's blue value, and the second three bits replace the third bit of the LSN of the green value. In this instance, a hash function is used to aid in the random bit selection process. While this approach works well in terms of increasing message capacity, they were unable to offer a definitive solution to the hash function collision issue.

A secret way of doing random LSB replacement of three bits per pixel (one bit per pixel value, such as Red, Green, and Blue) was proposed by the authors of [22]. Using this method, the

reference is concealed in the least significant bit (LSB) position of the associated pixel value, while the secret message bit is hidden in the random bit position of the pixel value (such as Red, Green, and Blue). to improve and expand the message's ability to be hidden.

This LSB matching determines whether to add a strong-minded random one or calculate one from the cowl image element. The bits and optional data carry the expected value and expand in lockstep with the elements as the pixel rises. The techniques have been modified predictably well with the play load as LSB collaborating and making only minor adjustments to the blanket image. It is possible that LSB matching will lead to distortion and resistance to the current steganalysis in order to show better performance in the previous method[20].

computation that combines district-based steganography with wild encryption to provide two layers of protection. CNN employed extra encryption data because of its random nature, which would make it harder for programmers to decipher the mystery data. The task assigned to the mystery information is first encoded using CNN. The mixed picture's edge district is then placed inside of them using network encode plot, and the LSB matching randomly selects which element from the cowl image to add or calculate. The bits and optional data expand in accordance with the elements and are carried in the desired worth as the pixel is raised. The approaches are changed reliably with the play load as LSB cooperating with little changes to the blanket picture [24]. To show better performance in the previous method, LSB matching might be a term of distortion and resistance to the current steganalysis.

2.5 Research Gap

It can be difficult to strike the correct balance between preserving the image's aesthetic appeal and implementing strong security measures when employing standard encryption techniques to secure data within images. Reliance on traditional encryption techniques could result in compromises with regard to image quality, data security, or both. Finding the best balance between security and image quality is a challenging task that calls for creative solutions that go beyond the bounds of current encryption methods. The degree to which the hidden data within an image can be hidden without noticeably lowering the visual quality of the picture is referred about as imperceptibility in this context of image steganography. The challenge highlighted in Maintaining less imperceptibility in image steganography is that existing techniques for hiding data within images may result in noticeable alterations to the visual appearance, making it easier for potential attackers

to detect the presence of hidden information[8]. Striking a balance between effectively concealing data and minimizing any visible changes in the image is crucial for successful image steganography. Maintaining less imperceptibility in image steganography emphasizes the need for methods that can enhance imperceptibility in the field of image steganography.

2.6 Research Objective

Here, the goal is to create and recommend a novel encryption technique designed especially for picture steganography. This approach seeks to strike a better balance between two important factors: protecting the image's visual quality and guaranteeing the safety of the hidden information. The intention is to get past the difficulties presented by traditional encryption methods, which frequently fail to find the best trade-off when it comes to image steganography. aims to offer a solution that improves data security Without sacrificing the overall the image's quality by proposing an encryption technique that strikes a more ideal balance between guaranteeing data security and preserving the image's quality. This goal is to introduce a new technique that increases imperceptibility in the area of image steganography. The goal is to create a steganographic algorithm that operates in the field of space, which means that this hidden data is actually integrated from each pixel in the image. This suggested method should minimize discernible changes to the image's appearance while permitting data to be hidden within it[21]. The need for a method that prioritizes imperceptibility while simultaneously enhancing security of hidden data is highlighted by the proposal of a technique that simultaneously makes image steganography more imperceptible. This ensures that the existence of concealed data is challenging to detect through visual inspection.

A strong encryption algorithm called Triple DES will be essential to encoding secret data into the picture. The embedded data is safely safeguarded by the encryption process, which also makes it challenging for unauthorized individuals to find or decrypt the secret content. By distributing these changes throughout the image, random pixel selection adds even more imperceptibility to the image. Rather than changing consecutive pixels, the method chooses random pixels to be embedded with the data[22]. This randomization contributes to a more visually seamless integration of hidden information by reducing visual artifacts that may result from patterns in the steganographic process. To strike a compromise between imperceptibility and data security, the suggested method combines random pixel selection with Triple DES encryption. Because of this

integration, the steganographic changes are minimal and have less of an effect on the original image's appearance while maintaining the confidentiality and indiscernibility of the embedded information.

2.7 Closure of this study

The thorough analysis of the body of research on image steganography has been instrumental in providing important background information and understanding for the formulation of the proposed thesis, "Image Steganography with Triple DES and Random Pixel Selection: A Secured Data Hiding Approach." The literature review emphasized the vital role that secure data hiding techniques play in protecting information contained in images, which has led to the investigation of cutting-edge cryptographic techniques and creative pixel selection strategies[23]. The literature review demonstrated a variety of steganographic techniques, from traditional LSB-based approaches to more advanced encryption algorithms. Because of its three-layered encryption architecture and track record of maintaining confidentiality, Triple DES has become a reliable option for cryptographic security. Experiments with different pixel selection strategies revealed how important randomness is for hiding information in an image and making it more imperceptible and resistant to detection. Specifically, the literature review shed light on how steganalysis techniques are developing and highlighted how the suggested method must not only prioritize security and imperceptibility but also be able to withstand criticism from more advanced detection techniques. The proposed model presents a novel and promising direction for the advancement of image steganography, aiming to address the shortcomings found in the current literature through the convergence of random pixel selection and Triple DES encryption.[24] Upon completion of the literature review, it becomes apparent that the suggested methodology incorporates components from various research avenues to establish a comprehensive and secure framework for data hiding. The forthcoming research builds upon the synthesis of previous studies' findings to place the suggested methodology in the larger picture of image steganography. This thorough literature review paves the way for contributions to the theoretical understanding and real-world implementation of secure image steganography, as well as the empirical investigation and validation of the suggested model.

Researcher Name	Year	Technique	Capacity	Limitation	PSNR
Pratiksha Sethi	2018	LSB based image steganography	N/A	Improving algorithm efficiency for larger data while enhancing cipher strength against brute force attacks.	73%
Kamaldeep Joshi	2020	The mixture of the YCbCr Color Model, 2-bit XOR LSB substitution in Cr, and crypto-algorithm.	30.75 kb	Implement Bluefish algorithm can improve image PSNR value.	68%
Mukesh Dalal	2021	Spatial domain-based embedding, LSB, DCT	27.53%	Embed secret data in a specific image frame region for discreet concealment.	37%
Sanjay Misra	2022	Modified LSB Steganography	N/A	Implement Higher Order bits and Error-diffusion technique to improve more Capacity in image.	68%
Sami Ghoul	2023	randomization, encryption and region-based	6300 kb	applying an additional layer of protection by making use of the current encryption techniques.	52.74-58.10%
S. M. Ammar Alam	2023	XOR-based data hiding in 2-LSBs	N/A	A parity-based embedding approach could enhance the quality of the image.	N/A
Moon et al.	(2018)	4LSB	12.5%	More prone to attacks	N/A
Kaur et al	(2019)	Hash-LSB	100%	A single image was utilized for the testing, and it was not tamper-resistant.	74.18

Table 1: Literature Review Table

Chapter 3- Methodology

3.1 General Steganographic System

Image, audio, video, text, and network steganography are the five categories into which steganography can be separated based on the cover media. Using an image as the cover object is how secret messages are hidden in image steganography. The image on the cover pixel intensities is applied in this procedure to conceal the secret data. Numerous methods, primarily categorized as a transform domain and spatial domain methods, can be used to embed data into the cover photo. These methods include Substitution of LSB, Pseudorandom Method, Distortion Method, Singular Value Decomposition, Discrete Fourier Transformation Method (DFT), Discrete Cosine Transformation Method (DCT), Discrete Wavelet Transformation Method (DWT), etc. The

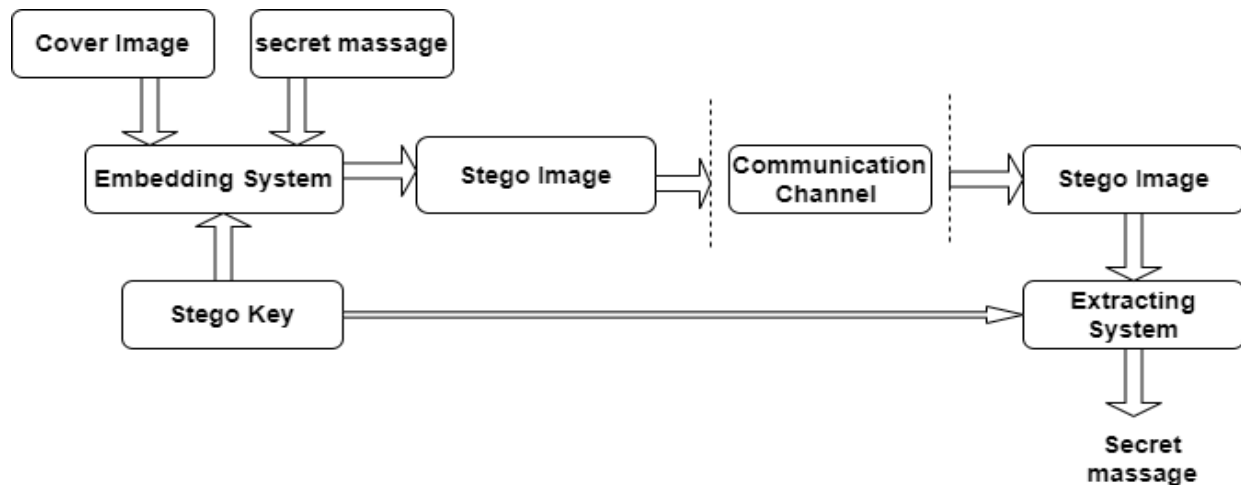


Fig 3.1: General Steganographic System

The figure shows the general steganographic system. Using the proper method and stego key, the embedding system appends the secret data to the cover image using the appropriate technique and stego key. After receiving the message over the communication channel, the recipient make use of the stego key and employed technique to retrieve the content from the Stego picture. In image-based steganography, there are two key prerequisites that researchers consider crucial for the concealing process. First of all, a steganography technique can conceal portions of a hidden message in a picture so that the stego-image and the original image are identical to the human eye; in other words, secret message is imperceptible. Second, the technique must enable the cover image to contain a significant amount of hidden data without sacrificing its imperceptibility [29]. Because there needs to be a balance established between these two criteria, the digital

steganography technique's parameters need to be carefully chosen. For an example, increasing the capacity beyond a given threshold value will affect the imperceptibility, and so on.

3.2 Proposed Method

The proposed methodology for image steganography with Triple DES and random pixel selection involves a systematic embedding process to ensure secure data hiding. Initially, a cover image and secret data are chosen for concealment. The secret data undergoes encryption using Triple DES, enhancing the security of the embedded information. To introduce an element of randomness and further fortify the process, a random sequence of pixel locations is generated. This sequence determines the pixels that will be used to hide the encrypted information within cover picture. The number of pixels required to accommodate the entire secret data is then calculated, contributing to the efficiency of the embedding process. Moving forward, the selected pixels from cover image are in encoded with encrypted information, effectively concealing this information within the visual content. A crucial checkpoint is established to confirm whether all secret bits have been successfully embedded. If the affirmative is reached, signifying the completion of the procedure of embedding, the stego picture is saved. In cases where not all secret bits are embedded, the process returns to pixel selection (Step 6), creating an iterative loop until all data is securely hidden. This embedding process ensures a robust and dynamic approach to steganography, utilizing Triple DES encryption and random pixel selection to enhance the security and effectiveness of data concealment within images.

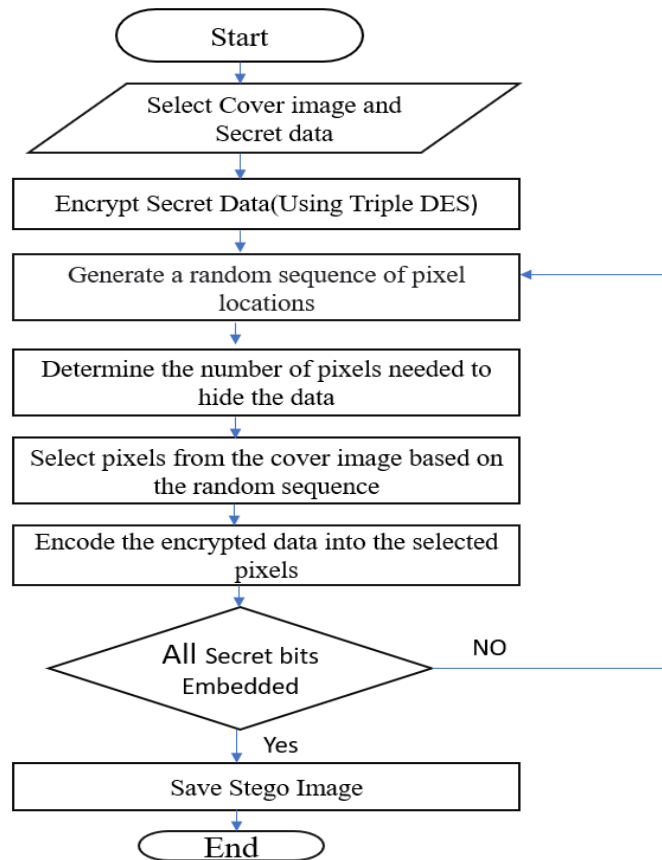


Fig 3.2: Embedding process of the proposed Approach

That extraction procedure in the proposed steganographic approach involving Triple DES and random pixel selection unfolds methodically to recover hidden information from the stego picture. Commencing with selection of the stego picture, the process proceeds to load the image into a steganography tool, facilitating subsequent steps. Retrieving the pixel selection sequence utilized during the embedding phase is pivotal, as it provides the blueprint for identifying the pixels containing concealed data within the stego image. Following this, the extraction of hidden data from the specified pixels transpires, utilizing the previously acquired pixel selection sequence. The extracted data, which is encrypted using Triple DES, undergoes decoding in the subsequent step. This decryption process is imperative for retrieving the original secret data. A crucial verification point is then introduced to determine whether all message bits have been successfully extracted[25]. If the extraction is complete, signifying the successful recovery of hidden information, the process concludes. However, if some message bits remain unextracted, the flow returns to the pixel extraction step, creating an iterative loop until all message bits are successfully

recovered. This meticulous extraction process ensures the reliable retrieval of concealed data from the stego image, leveraging Triple DES decryption and the pixel selection sequence to achieve accuracy and completeness in information recovery.

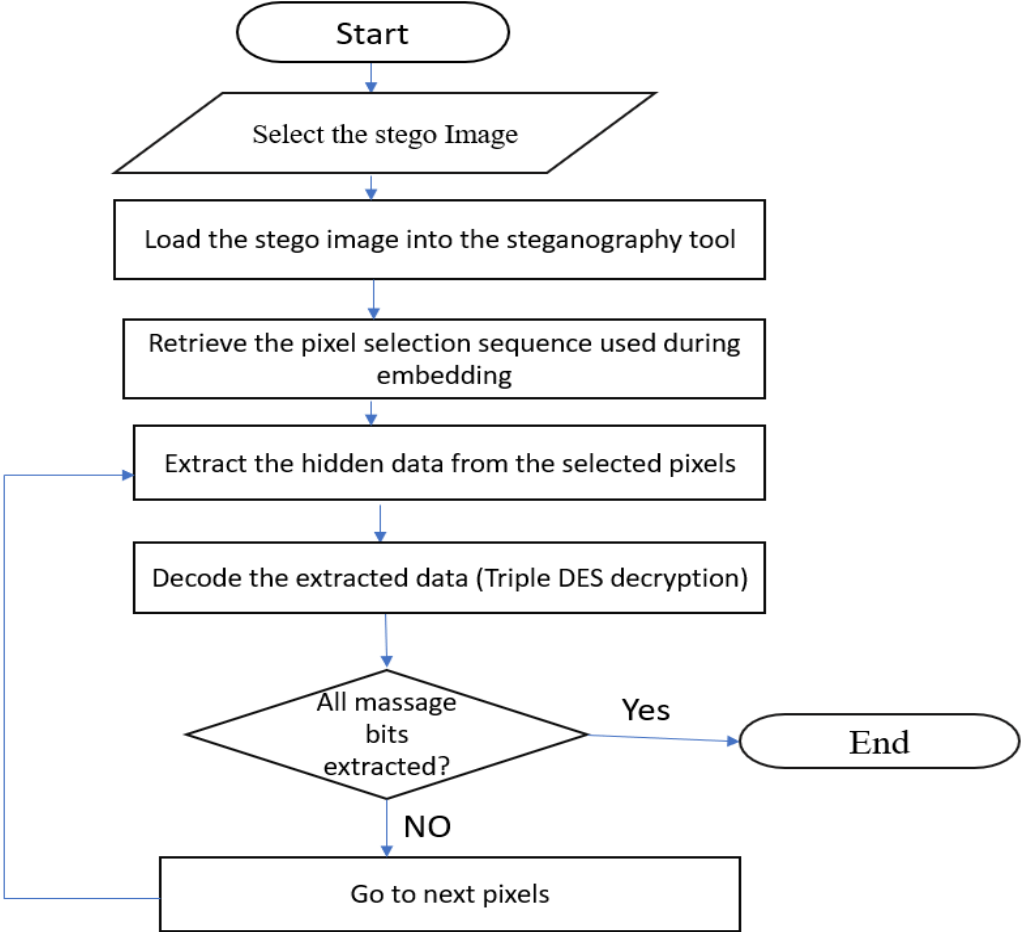


Fig 3.3: Retrieve process of the proposed Approach

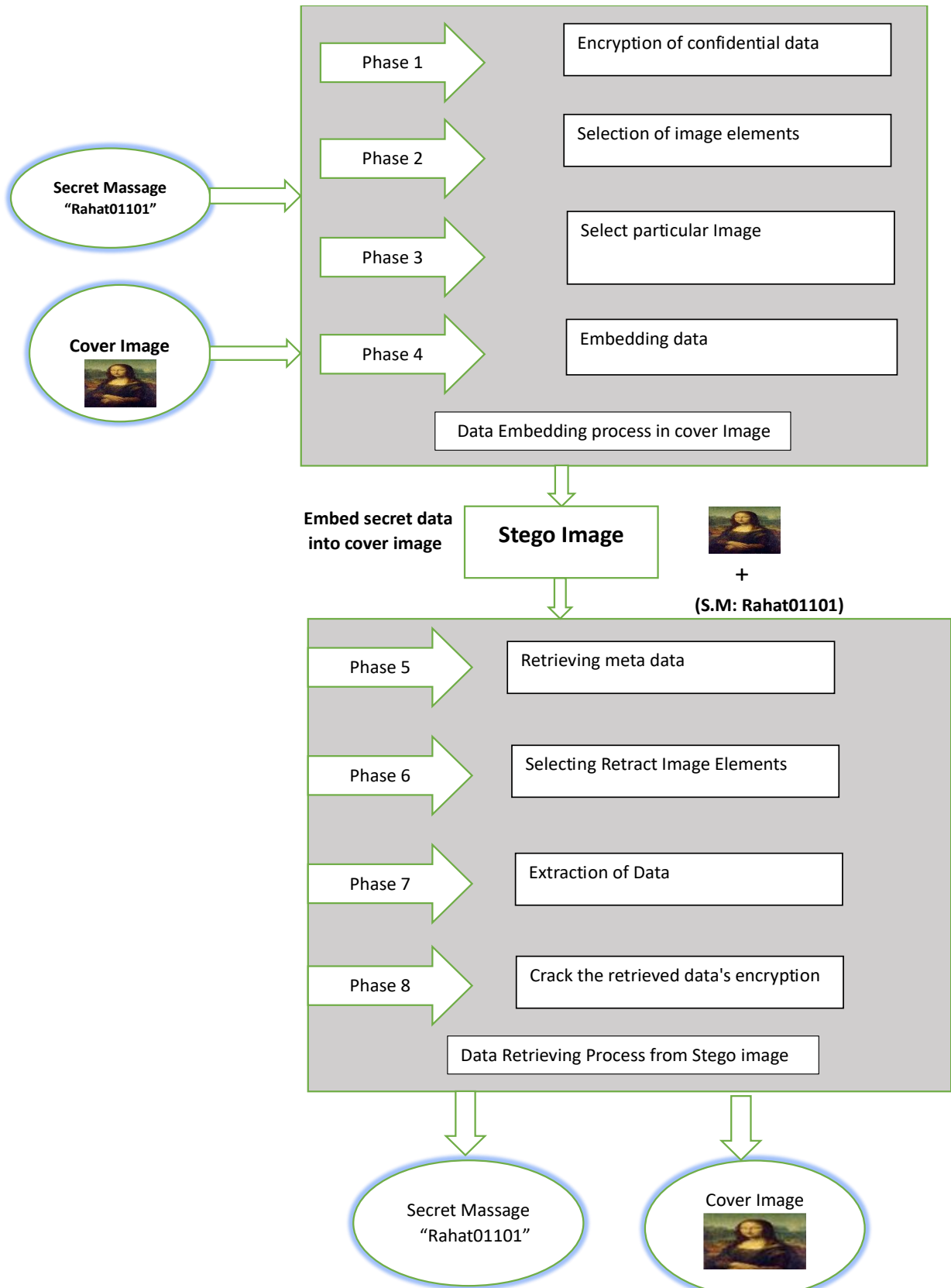


Fig 3.4: Block Diagram of the proposed image Steganography Approach

Phase-1: Secret Data Encryption by 3DES In this initial phase, the secret message "Rahat01101" undergoes encryption using the Triple DES algorithm. The algorithm employs three 56-bit keys (K1, K2, K3) to perform a series of transformations, including an Initial Permutation (IP), a Feistel network with 16 rounds, and a Final Permutation (FP). This results in a highly secure and complex transformation of the original message into an encrypted format.

Phase-2: Choose a Particular Image Selecting the cover photo is a crucial initial phase. "Monalisa.png" is selected, considering factors such as its resolution, format (PNG), and complexity. High resolution ensures more pixels for embedding without sacrificing visual quality, while a common format ensures compatibility. Complexity in the image, represented by diverse colors and patterns, aids in masking the changes introduced during the embedding process.

Phase-3: Image Element Selection by Random Pixel Selection Technique This phase focuses on selecting specific pixels within a defined Region of Interest (ROI) using the Random Pixel Selection technique. The ROI is chosen based on the intended location of data embedding. Randomly choosing pixels introduces an element of unpredictability and aids in distributing changes across the image, minimizing the likelihood of detectable patterns.

Phase-4: Data Embedding Using XOR LSB embedding, the data that is encrypted is introduced within the cover image. Modified are the selected pixels' least significant bits (LSBs) represent that corresponding bit of the encrypted data. XOR operation ensures a reversible process, and modifying LSBs reduces the cover image's visual impact. The randomness introduced in Phase-3 contributes to the imperceptibility of the changes.

Phase-5: Metadata Retrieving Metadata retrieval involves recording information related to the embedded data. This includes details about the Region of Interest (ROI), pixel coordinates selected during Phase-3, and any other relevant information. This metadata serves as a reference for the subsequent extraction phases, ensuring accuracy and reliability during the retrieval process.

Phase-6: Retract Image Element Selection This phase involves reversing the Random Pixel Selection technique used in Phase-3. The pixel coordinates saved during embedding are retrieved, allowing for the identification of specific pixels where the encrypted data is embedded. This retracing is crucial for accurate data extraction in the subsequent phases.

Phase-7: Data Extraction Data extraction focuses on retrieving the selected pixels' LSBs identified in Phase-6. The extracted LSBs are then reconstructed into binary format, representing the encrypted data embedded during Phase-4. The randomness introduced in Phase-3 ensures that the extraction process is not predictable, enhancing security.

Phase-8: Decrypt the Retrieved Data The final phase involves decrypting the extracted encrypted data using the Triple DES algorithm. The same three 56-bit keys used in Phase-1 are employed for key derivation and decryption. The result is the original secret message ("Rahat01101"), completing the steganographic process. The steganographic process starts with the secret message's encryption using 3DES in Phase-1, ensuring a secure and complex transformation. In Phase-2, a cover image is selected, considering factors such as resolution and complexity. Phase-3 employs the Random Pixel Selection technique, adding an element of unpredictability to the embedding process. The XOR LSB embedding in Phase-4 introduces the encrypted information into the cover picture, focusing on modifying the least significant bits for minimal visual impact. Metadata retrieval in Phase-5 records information about the embedded data and its location. Phase-6 retraces the steps of random pixel selection for accurate extraction. Data extraction in Phase-7 involves retrieving the LSBs of selected pixels and reconstructing the binary data. The final phase, Phase-8, decrypts the extracted data using 3DES, revealing the original secret message. The overall process emphasizes imperceptibility by distributing changes randomly across the image, ensuring the security of the embedded data through encryption, and making modifications subtle through LSB embedding. This combined approach seeks to achieve a balance between concealing the maintaining data and the cover image's integrity, resulting in a robust and secure image steganography technique. the extracted encrypted data is decrypted using 3DES, revealing The initial hidden message. The cover picture is then selected, and a specific region is chosen for embedding. Random pixel selection introduces an element of unpredictability, and XOR LSB embedding is employed for imperceptible modifications. Metadata is recorded to guide the subsequent extraction, where image elements are retracted using the reverse of the Random Pixel Selection technique. LSB extraction, along with metadata, ensures accurate data retrieval. Finally, the extracted encrypted data is decrypted using 3DES, revealing the original secret message. The synergy of these techniques enhances imperceptibility by minimizing visual impact, introducing randomness, and ensuring robust encryption. The steganographic procedure strikes a compromise between data hiding and cover image integrity, providing a secure and visually inconspicuous method for hiding sensitive information within digital images.

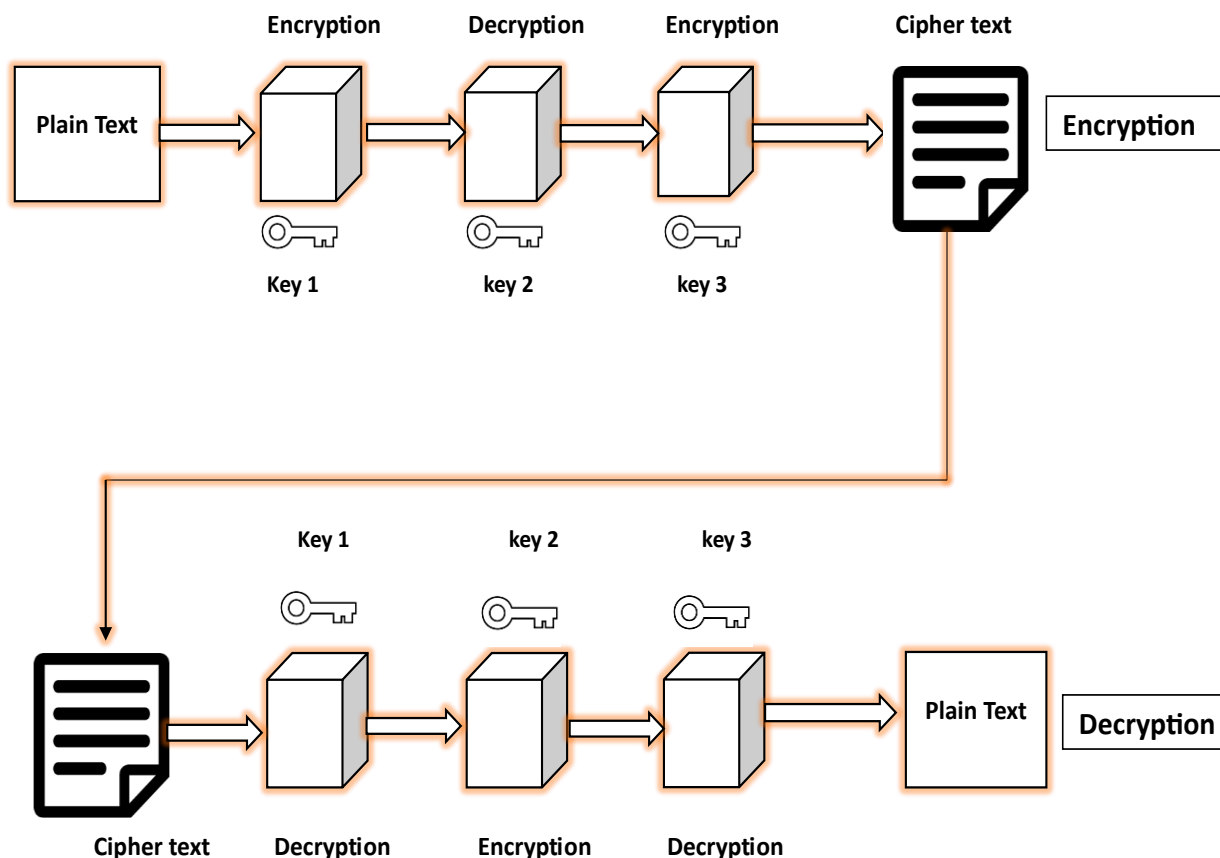


Fig 3.5: Diagram for Triple DES algorithm.

To improve the security of picture encryption, encrypted communication using the Triple DES algorithms is employed here. Encrypting images is necessary for communicating across multimedia and networks systems, where digital pictures must be saved and communicated over systems that handle large amounts of data. Pictures must be sent securely. Consequently, images are encoded before being delivered to the recipient; using a similar key, the collector must then decode the image. The page would then show the mistake if any of the letters in the key were composed incorrectly, so every letter needs to be composed fully. A new page will appear when you hit the scramble button; you must select the document, enter a key, and provide an incentive for the collector to encrypt the photo. Once the recipient touches the decoder and inputs the key as instructed by the sender, the key picture will be obtained over the system. An upgrade from DES encryption was proposed with the 3DES (Triple DES) standard. This standard uses an encryption method similar to the original DES, but it applies the encryption three times to increase the level of security. It was used to eliminate the brute force assaults in DES and the meet-in-the-middle

attack that happened in 2-DES. Its greater key length, which blocks various shortcut attacks that could shorten the time it takes to break DES, and its established dependability are further advantages.

Triple DES is renowned for having strong security characteristics. The DES method is applied to each data block three times, which significantly increases security when compared to a single DES application. Though it is not as new as some of the more recent symmetric encryption algorithms, 3DES is still very secure and has weathered the test of time[25]. In the security world, 3DES has grown in credibility over time. Because of its wide range of applications and dependability, it is regarded as trustworthy and is a good option in situations where security is crucial. Implementing 3DES is not too difficult, and there are proven libraries and tools available for integrating it into many applications. This simplicity of use may work to your project's benefit.

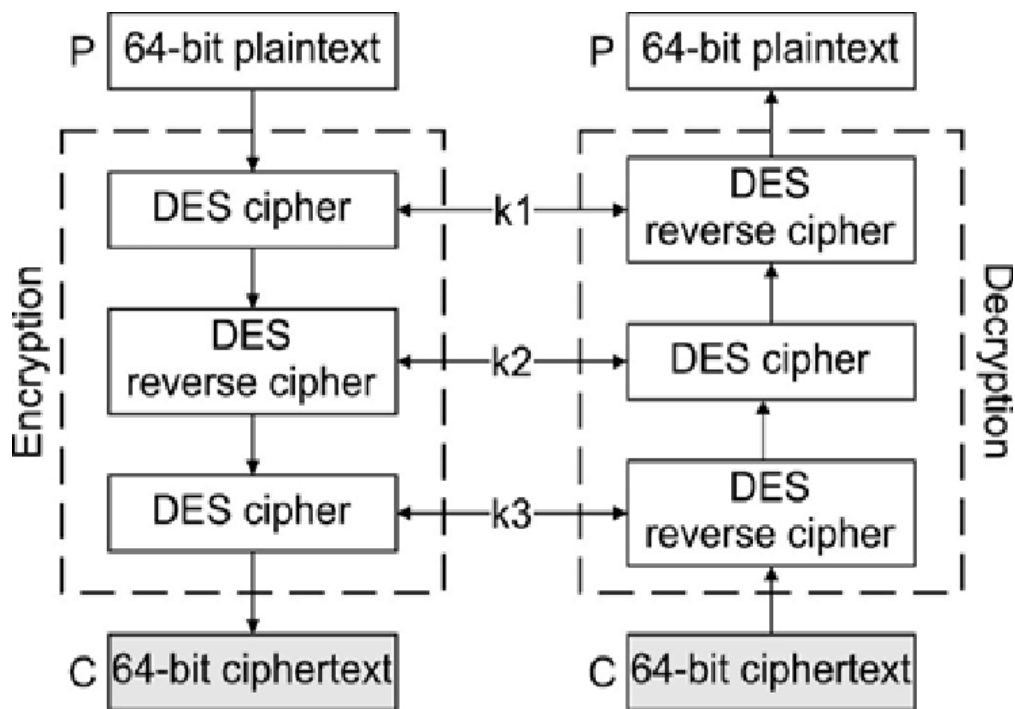


Fig 3.6. Encryption and Decryption Process of 3DES.

- Use a single DES to encrypt a message block (plaintext). utilizing a K1 key.
- Utilizing the K2 key, decrypt the step 1 results.
- Encrypt the output from step 2 with the K3 key to generate cipher text.

- The ciphertext decryption process reverses the 3DES Encryption process, which comprises decryption using K3 keys, encryption using K2 keys, and decryption using K1 keys.

In order to strengthen document security, the 3DES approach is applied in this work by using distinct keys, taking into account both the algorithm's strengths and weaknesses.

			3 rd				
1 st							
			2 nd				

Fig 3.7: Select pixels at random to hide information.

Every pixel in a 24-bit color picture is made up of three 8-bit prime colors (R, G, and B). One byte of information is embedded into each of the R, G, and B values of a pixel using second PRNG. As a result, the message byte is split into three groups of two, three, and three bits, representing the pixel's R, G, and B values, respectively. To embed the first bit of the first group into the red value, the PRNG randomly chooses a bit from each of the five MSBs. Next, the outcome of an Exclusive-OR operation on the message bit and the randomly chosen bit replaces the third LSB of the red value. Second and third message bits of the first group are transformed and embedded into the second and first LSB of the red value using this procedure.

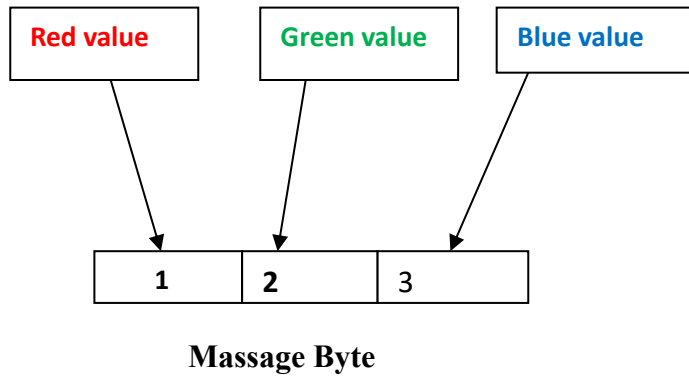


Fig 3.8: Each pixel's byte of text to be embedded (Red, Green, Blue)

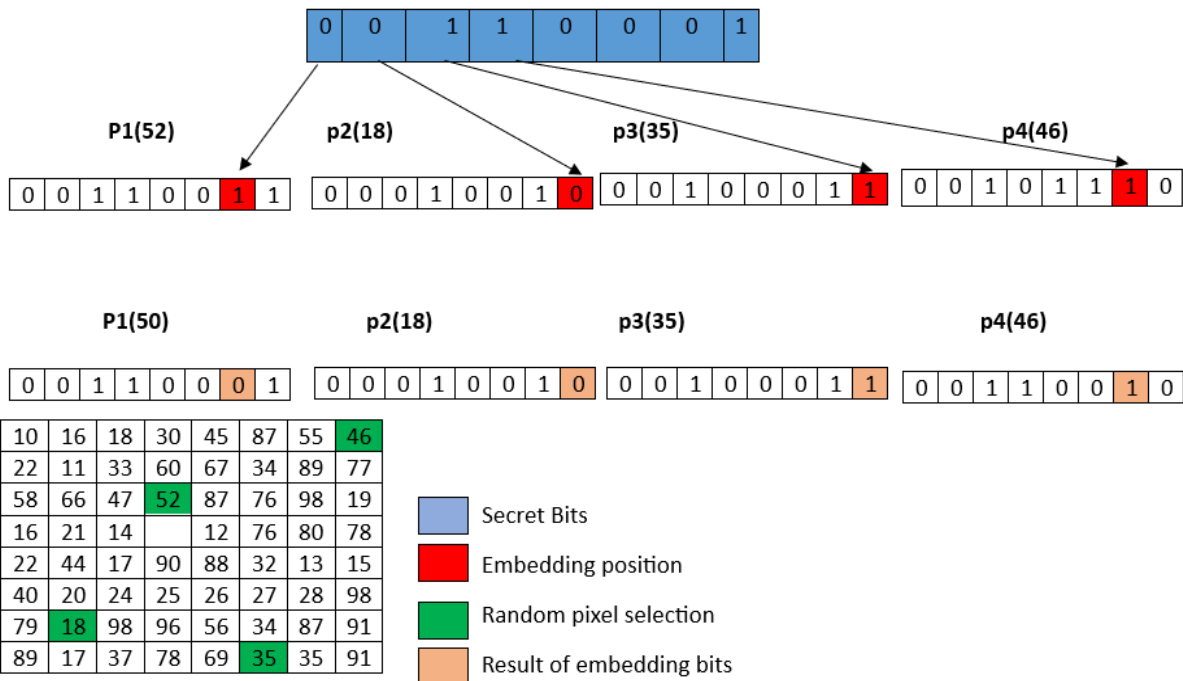


Fig 3.9: Random pixel selection

Through the suggested approach, the second purpose of this study is achieved, which is to incorporate the Least Significant Bit layer's secret data such that the quality of the original image is maintained.

Following presumptions can be used to apply the embedding procedure:

When the first bit of 0 and P1's second bit in the LSB is 0, the second LSB layer remains unaltered. In the case of the second pixel P2, substitution will be made in the initial level of the LSB, which,

in the event that the bit is 0 and the second bit in the Least Significant Bit layer is 1, is 0. The second LSB layer for the third pixel P3 stays unchanged when the bit is 1 and the second bit in the Least Significant Bit layer is 1. When the second bit in the LSB layer is 0 and the bit is 1, substitution occurs in the first layer of the Least Significant Bit in the case of the fourth pixel P4. Thus, the stego image generates the pixels P1', P2', P3', and P4'. In this case, the randomly selected pixel is represented by a green color, but the subsequent embedding is represented by a red color. Additionally, yellow serves as an illustration of the hidden details.[26] The process of data embedding involves the transformation of the Least Significant Bits.

Random pixel selection is a technique used in image steganography to change the color values of selected pixels to incorporate concealed information within an image. Random pixel selection introduces an unpredictable element to the embedding process, which makes it more secure and difficult to detect, as opposed to adhering to a predetermined pattern. Imagine the image as a grid of pixels, each with its unique RGB (Red, Green, and Blue) color values, to accomplish this without using code. To encode the concealed information, pick a set of pixels at random from the image and slightly alter their color values[27]. This procedure guarantees that the changes are evenly applied over the picture, making it difficult for anyone examining the picture to identify an identifiable pattern. Although this explanation gives conceptual knowledge, the method needs to be put into code by selecting particular pixels, adjusting their color values, and making sure the modifications are not noticeable to the unaided eye.

Random pixel selection introduces an element of unpredictability in the steganographic process, contributing to the hidden data's imperceptibility within the image. The randomness can enhance concealment to the embedded information, making it more challenging for adversaries to detect.[28] By selecting pixels randomly for data embedding, the resulting steganographic image is less likely to exhibit discernible patterns that could be exploited by visual analysis techniques. This helps in creating a more visually seamless integration of hidden data[29]. This technique can enhance the robustness of the steganographic technique by reducing vulnerability to attacks that target specific patterns or regions in the image. This randomness adds a higher level of safety against statistical pattern-based steganalysis approach.

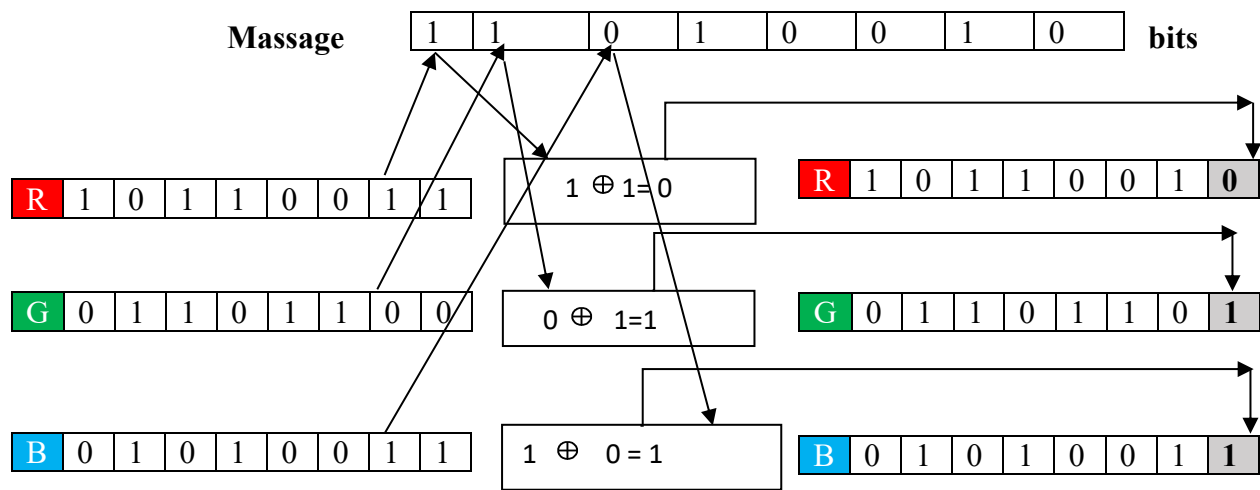


Fig 3.10: XOR Embedding Process

I'll now demonstrate how to use XOR embedding in picture steganography. Assume that the RGB color model will XOR a secret message bit, 11010010, into a single pixel. The decimal equivalent of the red binary value, 10110011, is 179. The decimal equivalent of 01101100, or 108, is the Green binary value. The decimal value of 01010011, which is the Blue binary value, is 83. But 8 is the number of the hidden message. I'll labor here for only one pixel to protect the seventh bit, or 1, of the red binary value. As we all know, $1 * 1 = 0$. The eighth bit value of the red binary will now have that XORed bit "0" substituted. The value of the eighth bit was previously 1, but after being XORed, it abruptly changed to 0. The second bit of the secret message, which is 1, will be XORed with the seventh bit of the Green binary value in the following phase. The eighth bit of the Green binary value will be used in place of the XORed $1 \oplus 0 = 1$ value. The value, which is 1, will shift. The third phase will include repeating the same procedure. The third bit (0 in the secret message) will be XORed with the seventh bit (7 in the Blue binary value). The eighth bit of the blue binary value will be used to replace the XORed $0 \oplus 1 = 1$ value. The value of one will be overwritten. This document describes the working method of XOR embedding.

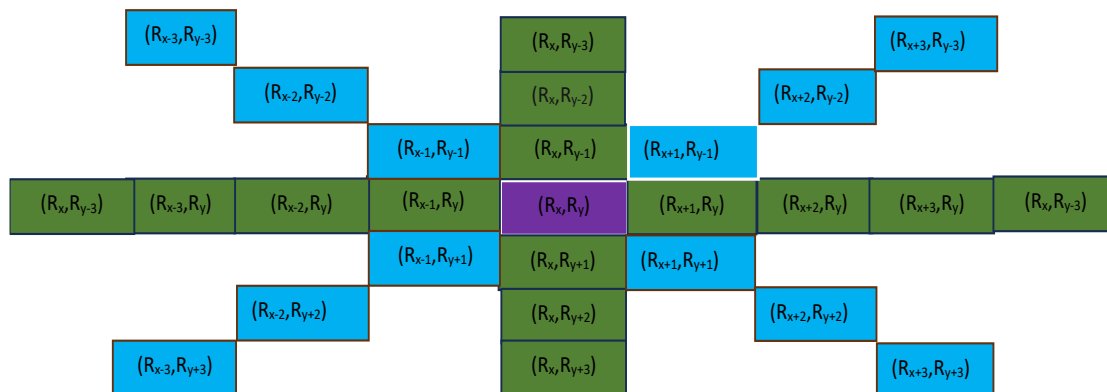


Figure 3.11: 8 Directional pixel Selection

In order to choose pixels for the 8-directional pixel selection approach, a predetermined pattern must take into account North, northeast, east, southeast, south, southwest, west, and northwest are the eight different directions. This all-encompassing method guarantees that the concealed data is dispersed throughout the picture in a manner that reduces detection vulnerability and strengthens defense against different kinds of image processing assaults. The recommended approach involves embedding the message in the (C_x, C_y) center pixel first, then locating and embedding the pixels in the remaining eight directions. Every embedding direction will adhere to the given the equation in straight lines. y is equal to mx plus c . In this case, y stands for the vertical axis' length, x for the horizontal axis' length, m for the straight line's slope, and c for the y value at $x = 0$. The suggested method's eight-directional pixel selection strategy is shown in Fig.

Peak Signal to Noise Ratio (PSNR):

PSNR compares a picture original against a deformed or compressed rendition to determine how good the picture is. It is used to assess how imperceptible the stego picture is in relation to original picture when it comes to image steganography. The mean squared error (MSE) and the highest value of a pixel —typically for 8-bit, 255 images—are used to determine the PSNR.

$$PSNR = 10 \log_{10} \frac{MAX_X^2}{MSE} \dots \dots \dots (3.1)$$

- MAX= the highest value that may be assigned to a pixel in an image (255 (11111111) for an 8-bit picture).
- MSE= Mean Square Error

Greater robustness and imperceptibility are indicated by a higher PSNR value (over 30 dB).

Mean Square Error (MSE):

(Maximum inaccuracy between the original and compressed picture)

The mean squared error (MSE) calculates the differences between the original and stego pictures' corresponding pixels. Improved imperceptibility is shown by lower MSE values.

$$MSE = \frac{1}{a * b} \sum_{i=0}^{a-1} \sum_{j=0}^{b-1} [X(i, j) - Y(i, j)]^2 \dots \dots \dots (3.2)$$

a = The number of rows of pixels in the frames.

b = The frame width, or the number of pixel columns.

The original frame's pixel intensity at row i^{th} and column j^{th} is equal to (i, j) .

The lower Mean Squared Error (MSE) value indicates the smallest error between the stego and original picture, suggesting more dependability. $Y(i, j)$ = Pixel intensity of the stego frame at i^{th} row, and j^{th} column

Structured Similarity Index Measurement (SSIM):

(This statistic is based on structural substance. SIM is a metric that considers the brightness, contrast, and structure of pictures. It verifies the resemblance between the stego-image and the cover picture. In contrast with PSNR and MSE, it provides a more complete indicator of image quality. The range of SSIM values is -1 to 1, with 1 denoting perfect similarity.

$$SSIM(X, Y) = \frac{(2\mu_X\mu_Y + C_1)(2\sigma_{XY} + C_2)}{(\mu_X^2 + \mu_Y^2 + C_1)(\sigma_X^2 + \sigma_Y^2 + C_2)} \dots \dots \dots (3.3)$$

- The respectability average pixel values of frames X and Y are denoted by μ_X, μ_Y .
- The relative variations in pixel values for frames A and B are denoted by σ_X^2 and σ_Y^2 .
- The covariance of pixel values between frames A and B is denoted by σ_{XY} .
- Constants are C_1, C_2 .

The SSIM ranges from 0 to 1, and a video is considered high quality if its value is close to 1. These measures are frequently used to assess picture steganography methods; greater PSNR and SSIM values and lower MSE indicate superior stego image imperceptibility.

Chapter 4: Result and Discussion





image	payload	Image Size	PSNR	MSE	RMSE
	32	512x512	85.8816760633	0.0000000026	0.0000508061
	32	512x512	89.6055351053	0.0000000011	0.0000330920
	32	512x512	85.6886245114	0.0000000027	0.0000519480
	12	512x512	85.7840776904	0.0000000026	0.0000513802

Table 2: Table of results for the stego image analysis

The experimental data presented in this part provide a description of the performance of our proposed method. Our steganography makes use of well-known LSB-based embedding methods. To conduct our experiments, we used our Random pixel selection technique and LSB embedding to a range of typical photos at different sizes, including baboon.png, fruit.png, lena.png, and so on. These test Pictures are shown in Table 1. The quality of a stego image is usually assessed from two perspectives. First, we analyze the difference between the stego and cover photos using the Peak Signal-to-Noise Ratio (PSNR) measurement. The Mean Square Error (MSE) is located between the cover and stego pictures. The MSE is described as follows with a cover image with m and n for width and height, a stego image designated by K, and a cover image indicated by I. Here is how the MSE and PSNR is defined:

$$MSE = \frac{1}{a*b} \sum_{i=0}^{a-1} \sum_{j=0}^{b-1} [X(i, j) - Y(i, j)]^2 \dots (4.1) \quad PSNR = 10 \log_{10} \frac{MAX_X^2}{MSE} \dots (4.2)$$


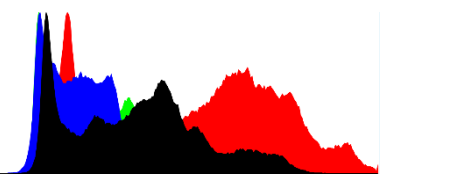
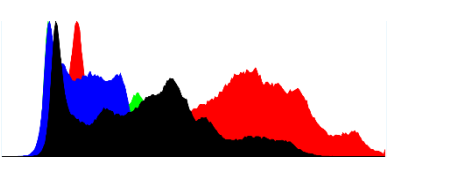




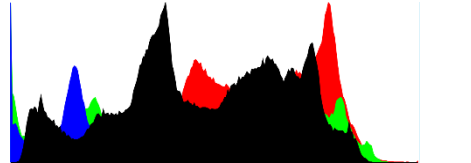
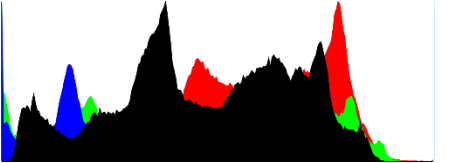
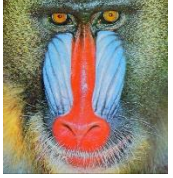
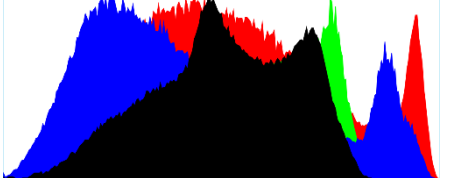
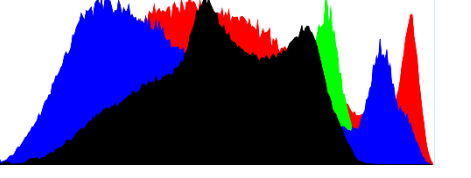

Image	Cover image histogram	Stego image histogram
		
		
		
		

Table 3: A comparison between the Stego image histogram and the cover image

Look at the four 512x512 pixel cover images: nature.png, baboon.png, fruit.png, and lena.png. After adding a hidden message to the photographs, it becomes evident that the histograms showing cover and stego picture are not significantly different from one another. Histograms display the distribution of pixel intensities in a picture. They serve as a visual tool to help understand an image's overall composition and tone variations. Generally, if a secret message or other piece of information is implanted inside a picture, the histogram will noticeably alter due to variances in the pixel values. However, the absence of such variances in the comparative study raises some intriguing considerations. One possible explanation for the absence of disparity in the histograms might be the effectiveness of the steganographic technique employed. Steganography aims to conceal information within a covering, like that a picture, without calling attention to itself. Advanced steganographic methods ensure that the alterations done to the cover picture are imperceptible to both the human eye and statistical instruments such as histograms. Another consideration is the cover pictures' capacity to store the encoded data. A wide range of pixel intensities and color changes in the cover pictures makes it simpler to hide more data without

noticeably changing the overall histogram. The fact that the histograms of the stego and cover photos do not significantly differ from one another indicates that the steganographic process was effective in maintaining the visual integrity of the cover images. It also highlights the challenges that face anybody attempting to unearth concealed information using only pixel intensity distribution analysis.

Embedding Panel



Load Cover Img


U2FsdGVkX18n4n5CPF4R105AnKVpoj2u

Proposed Model
 8 Directional Model
 XOR Sub Model

32

Embed

Extracting Panel



Load Stego Img

U2FsdGVkX18n4n5CPF4R105AnKVpoj2u

Proposed Model
 8 Directional Model
 XOR Sub Model

Extract


Image Quality Metrics

	Payload	ImageSize	PSNR	MSE	RMSE
▶	32	512x512	80.7325779072432	0.00054931640625	0.0234375
•					

Notice

Activate Windows
Go to Settings to activate Windows.

Embedding Panel



Load Cover Img


U2FsdGVkX1/iAqz1PADWVSP/gfazWRWw

Proposed Model
 8 Directional Model
 XOR Sub Model

32

Embed

Extracting Panel



Load Stego Img

U2FsdGVkX1/iAqz1PADWVSP/gfazWRWw

Proposed Model
 8 Directional Model
 XOR Sub Model

Extract

Image Quality Metrics

	Model	Payload	ImageSize	PSNR	MSE	RMSE
▶	Proposed Model	32	512x512	81.1104635161372	0.0005035400390625	0.022439697
•						

Notice

Activate Windows
Go to Settings to activate Windows.

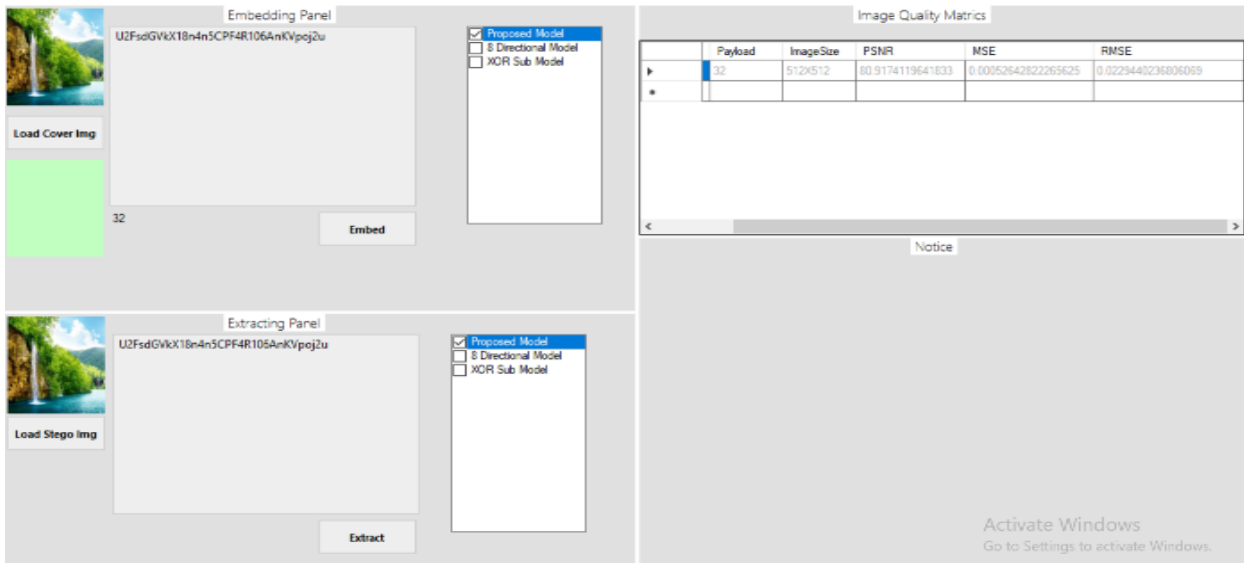
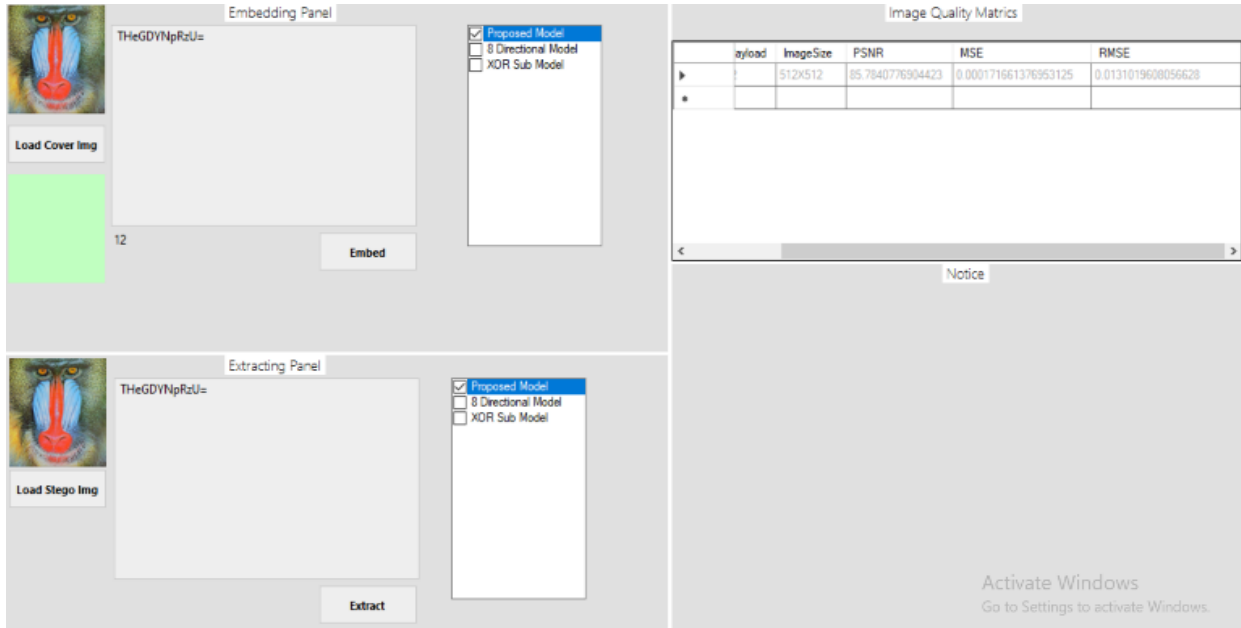
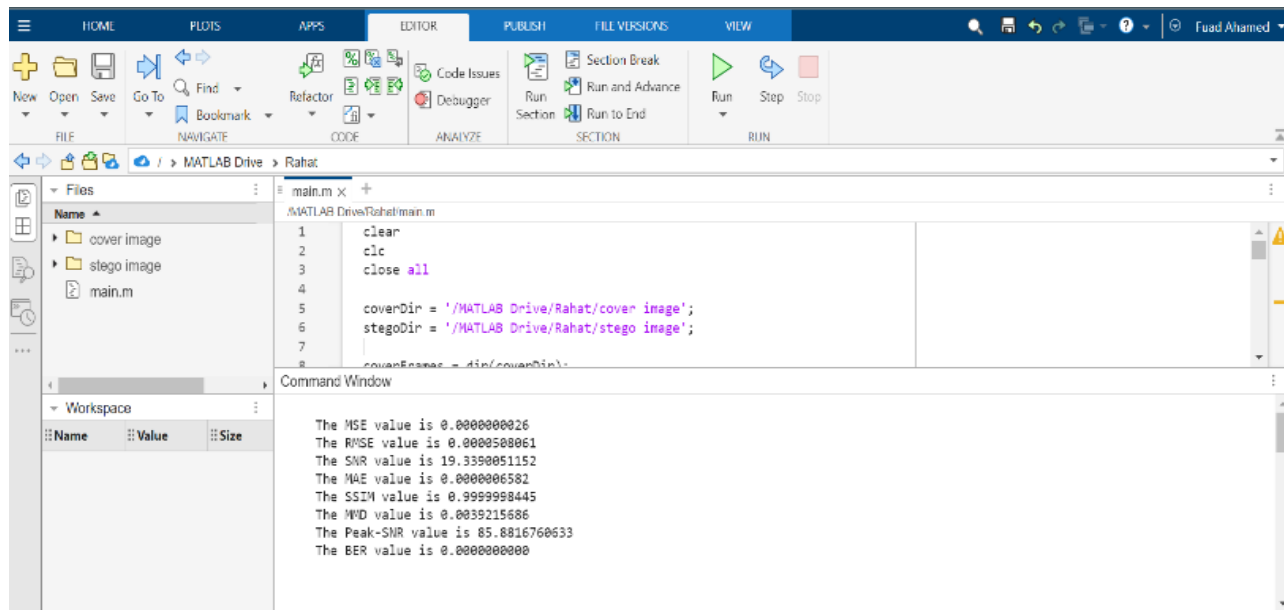


Fig 4.1: GUI Of the Proposed method Implementation

We used Visual Studio Code Editor to implement C# code for our suggested model. In essence, this is our suggested model's GUI or interface. We want to explain this model's whole workflow. The model has an embedding and extracting panel, and the PSNR, MSE, and RMSE calculations for our model are on the right side. We now have an input box for embedding the hidden message in the embedding panel. Here, we use the 3DES algorithm. To encrypt our confidential data, there are several online 3DES encryption tools available. Using these tools, we encrypt four pieces of data or messages. We next input the encrypted data into the input box and choose "Embed." The cover picture is implanted with the secret data once it has been embedded, and it is then converted to the stego image. The right side of our GUI will display the PSNR, MSE, and RMSE calculations when we abruptly implant hidden info into certain picture pixels. We can obtain those values from this panel. We use the four stego pictures in this manner. This is how the embedding process is summarized. Let's discuss the extraction procedure. Confidential data will appear here by default if we import the Stego photos one at a time and hit the extract button on the bottom, which is essentially the extraction panel.



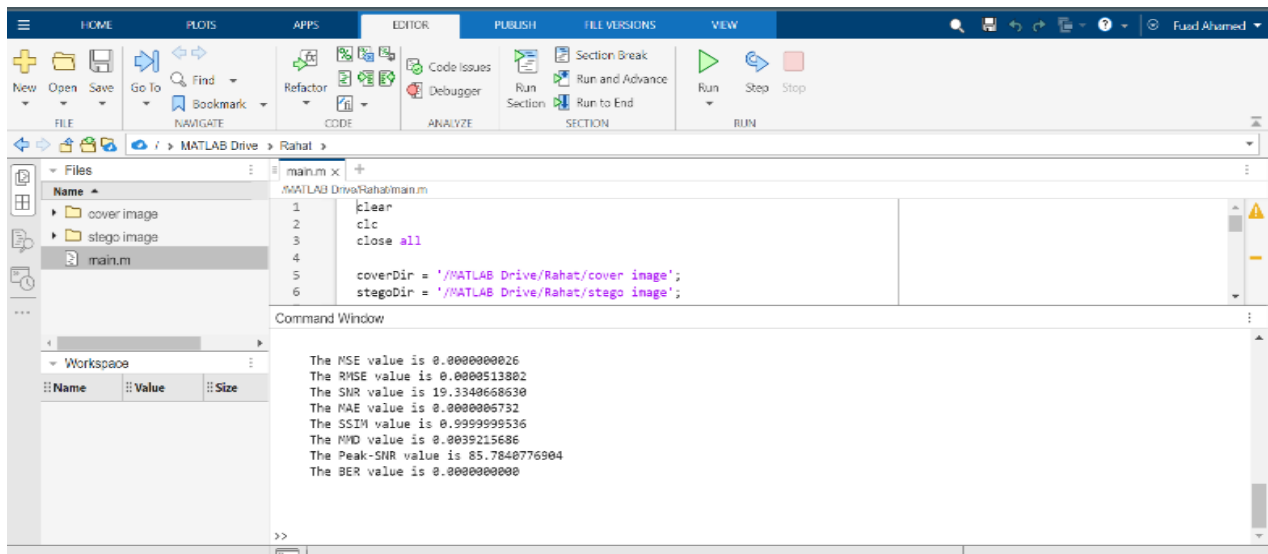
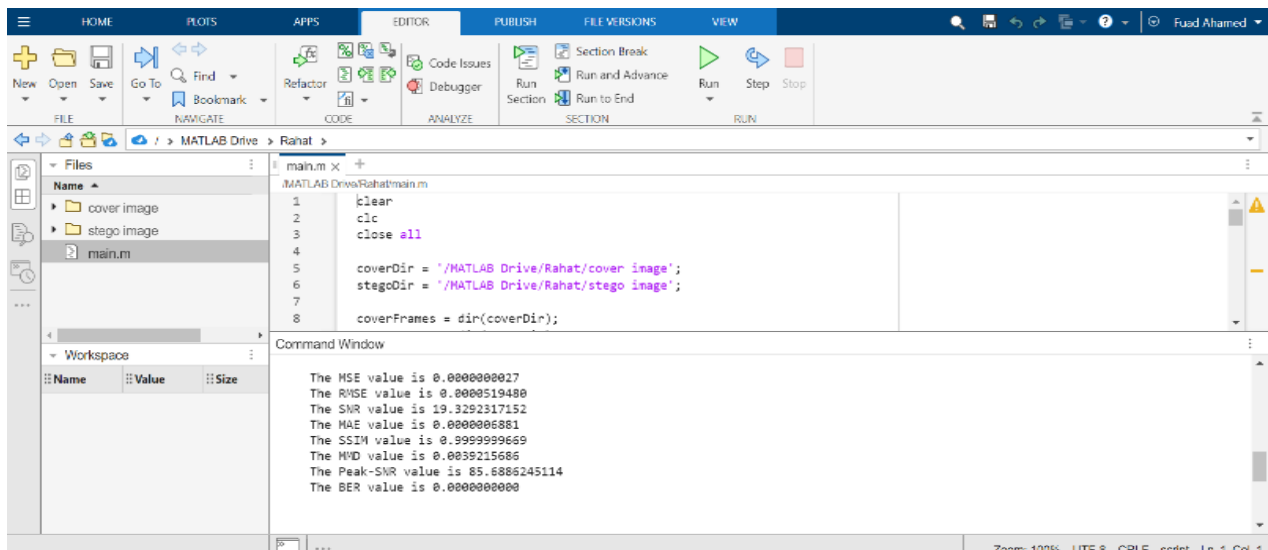
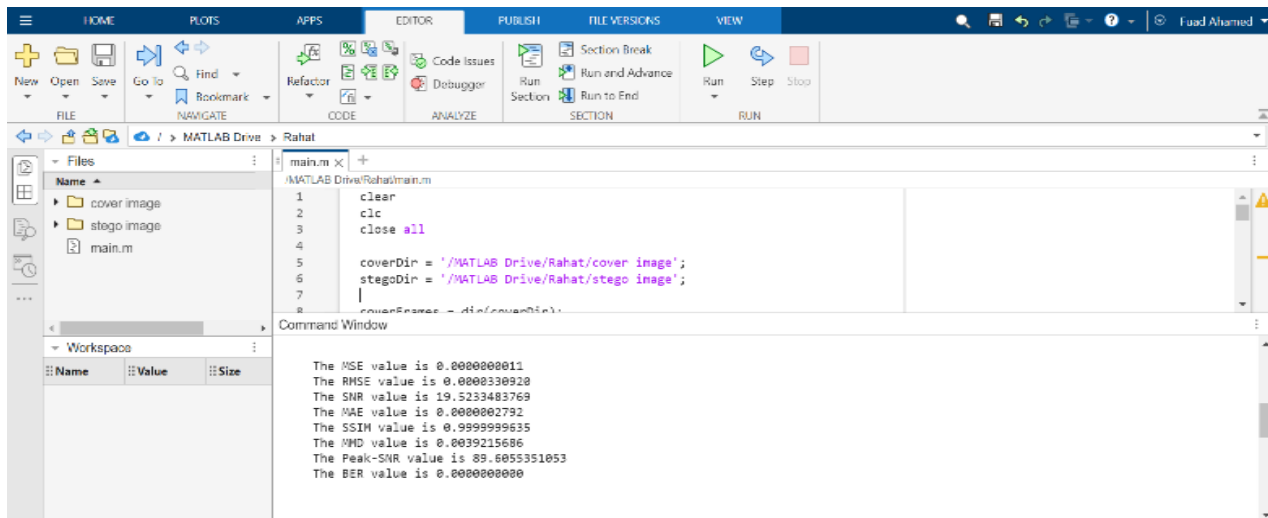


Fig 4.2: Implementation of MATLAB Code

Figure 13 illustrates how we primarily checked the PSNR, MSE, and RMSE values in MATLAB for the four photos, which are titled nature.png, baboon.png, fruit.png, and lena.png. It is evident from the first image that the corresponding PSNR, MSE, and RMSE values are 85.8816760633, 0.0000000026, and 0.0000508061. As we can see, the values for the second picture are 89.6055351053, 0.0000000011, and 0.0000330920 in terms of PSNR, MSE, and RMSE. As we can see, the third picture yields the following values for PSNR, MSE, and RMSE: 85.6886245114, 0.0000000027, and 0.0000519480. Regarding the fourth picture, as we can see, the values for PSNR, MSE, and RMSE are 85.7840776904, 0.0000000026 and 0.0000513802, respectively. Even in Figure 2, the cover and stego image histograms show less of a difference, as can be seen. Our combination model performs exceptionally well, as demonstrated by the figure 3 that shows the results of prior scholars' comparison investigation. In order to improve picture imperceptibility, we assess PSNR and MSE. We observed that all picture PSNR values were up to 80, indicating that our model might become less noticeable after embedding. This is a huge improvement, indicating that our model is far superior. We are aware that a PSNR of 40 or above is highly indicative of a less visible picture. However, when we tested it in MATLAB, we had a result of 80

Image	References [19],[30]	References [31]	References [32]	Our Work
Lena	54.82	-	77.90	85.8816760633
Baboon	72.48	72.62	78.49	85.7840776904
Peppers	54.88	-	76.39	85.6886245114

Table 4: Comparison PSNR of our proposal with other researchers

We compare three image's PSNR value with other existing technique. When we compare, we see that in the Lena image, the PSNR value found was 54.82 and another researcher found was 77.90. But our model performs better than others because we find the result 85.88. Similarly, from the Baboon image, the PSNR value was found consequently 72.48, 72.62, 78.49 whether our model's result is found 85.7840776904 which is obviously better than other's. At the last Peppers image, the previous researcher's result was consequently 54.88 and 76.39 whether our model's result is found 85.68 which is great. So, from the discussion we can say that our model performs far better than others. The PSNR value is increased when we embed hidden text in the image.

Image	References [30]	References [33]	References [19]	Our Work
Lena	0.002893	0.0032	0.4268	0.0000000026
Baboon	0.002825	0.0031	0.4253	0.0000000026
Peppers	0.002712	0.0037	0.4243	0000000027

Table 5: Comparison MSE of our proposal with other researchers

Here we compare MSE values with other existing techniques. We know that low MSE is associated with better perceptual quality. We added three researchers gathered MSE result from their papers. From the Lena image we found MSE value was 0.002893, 0.0032 and 0.4268. But our MSE value we get 0.0000000026 that is very best. Consequently, from the Baboon image, we get MSE value from the previous researchers that was 0.002825, 0.0031 and 0.4253. But our model performs well here because our value is 0.0000000026. From the 3rd image Peppers, the value was 0.002712, 0.0037 and 0.4243 but our value is we get 0.0000000027 that is cool. It's important to note that a low MSE is a common goal in image steganography. So, our model is working better than other existing techniques.

Chapter 5: Conclusion and Future Scope

In conclusion, the mixture of XOR LSB, Triple DES encryption, and random pixel selection in image steganography has proven to be a robust and innovative approach to secure data hiding. The utilization of XOR LSB ensures efficient embedding of hidden information into the least significant bits of the image pixels, thereby achieving imperceptibility while maintaining a high level of security. The incorporation of the Triple DES algorithm adds an additional layer of protection, enhancing the overall encryption strength of the concealed data. The integration of random pixel selection further fortifies the security aspect by introducing unpredictability in the steganographic process. This not only mitigates the risk of detection by potential adversaries but also contributes to the concealment of the embedded data within the vast visual space of the image. The synergy of these techniques results in a sophisticated and resilient image steganography method, suitable for safeguarding sensitive information in diverse applications. The experimental results and performance evaluations validate the efficacy of the proposed approach, demonstrating its superiority in terms of both security and imperceptibility when compared to traditional methods. The current research successfully addresses the imperceptibility aspect in image steganography through the integration of XOR LSB, Triple DES, and random pixel selection. However, to further advance the field, future researchers are encouraged to focus on enhancing both capacity and robustness within this technique.

References

- [1] W. M. Abdulllah, A. M. S. Rahma, and A. S. K. Pathan, "Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach," *Computers and Electrical Engineering*, vol. 40, no. 4, 2014, doi: 10.1016/j.compeleceng.2014.02.007.
- [2] B. Wei, M. Yu, K. Chen, and J. Jiang, "Deep-BIF: Blind Image Forensics Based on Deep Learning," in *2019 IEEE Conference on Dependable and Secure Computing, DSC 2019 - Proceedings*, 2019. doi: 10.1109/DSC47296.2019.8937712.
- [3] P. Ganesan and R. Bhavani, "A high secure and robust image steganography using dual wavelet and blending model," *Journal of Computer Science*, vol. 9, no. 3, 2013, doi: 10.3844/jcssp.2013.277.284.
- [4] P. Andriotis *et al.*, "On Two Different Methods for Steganography Detection in JPEG Images with Benford's Law," *Security and Protection of Information*, 2013.
- [5] A. Almohammad, "Steganography-Based Secret and Reliable Communications : Improving Steganographic Capacity and Imperceptibility," *Doctor thesis*, 2010.
- [6] J. K. Mandal, "Colour Image Steganography based on Pixel Value Differencing in Spatial Domain," *International Journal of Information Sciences and Techniques*, vol. 2, no. 4, 2012, doi: 10.5121/ijist.2012.2408.
- [7] G. Ardiansyah, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm," in *Proceedings - 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2017*, 2017. doi: 10.1109/ICITISEE.2017.8285505.
- [8] S. Nirenjena and M. Jayapriya, "A Novel Triple Layer Method to Hide Secret Image Using Steganography," in *2020 International Conference on System, Computation, Automation and Networking, ICSCAN 2020*, 2020. doi: 10.1109/ICSCAN49426.2020.9262406.
- [9] D. C. Wu and W. H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognit Lett*, vol. 24, no. 9–10, 2003, doi: 10.1016/S0167-8655(02)00402-6.
- [10] M. S. Taha, M. S. Mohd Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in *IOP Conference Series: Materials Science and Engineering*, 2019. doi: 10.1088/1757-899X/518/5/052003.
- [11] Y. Yigit and M. Karabatak, "A stenography application for hiding student information into an image," in *7th International Symposium on Digital Forensics and Security, ISDFS 2019*, 2019. doi: 10.1109/ISDFS.2019.8757516.

- [12] O. Elharrouss, N. Almaadeed, and S. Al-Maadeed, "An image steganography approach based on k-least significant bits (k-LSB)," in *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies, ICIoT 2020*, 2020. doi: 10.1109/ICIoT48696.2020.9089566.
- [13] X. Zhou, W. Gong, W. Fu, and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," in *2016 IEEE/ACIS 15th International Conference on Computer and Information Science, ICIS 2016 - Proceedings*, 2016. doi: 10.1109/ICIS.2016.7550955.
- [14] S. D. Muyco and A. A. Hernandez, "A modified hash based least significant bits algorithm for steganography," in *ACM International Conference Proceeding Series*, 2019. doi: 10.1145/3335484.3335514.
- [15] J. Guru, M. Srivatsava, and M. R. Sheeja, "Implementation of Triple DES ALGORITHM in Data Hiding and Image Encryption Techniques," *International Journal of Advanced Science and Technology*, vol. 29, no. 3, 2020.
- [16] S. Sugathan, "An improved LSB embedding technique for image steganography," in *Proceedings of the 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology, iCATccT 2016*, 2017. doi: 10.1109/ICATCCT.2016.7912072.
- [17] R. Amirtharajan, R. Subrahmanyam, J. N. Teja, K. M. Reddy, and J. B. B. Rayappan, "Pixel indicated triple layer: A way for random image steganography," *Research Journal of Information Technology*, vol. 5, no. 2, 2013, doi: 10.3923/rjit.2013.87.99.
- [18] A. Gutub, A. Al-Qahtani, and A. Tabakh, "Triple-A: Secure RGB image steganography based on randomization," in *2009 IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009*, 2009. doi: 10.1109/AICCSA.2009.5069356.
- [19] M. M., A. A., and F. A., "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 3, 2016, doi: 10.14569/ijacsa.2016.070350.
- [20] S. Dash, M. N. Das, and M. Das, "Secured Image Transmission Through Region-Based Steganography Using Chaotic Encryption," in *Advances in Intelligent Systems and Computing*, 2019. doi: 10.1007/978-981-10-8055-5_48.
- [21] D. Vadlamudi, R. J. Kumar, and C. N. Sai, "Image Encryption using Reverse Data Hiding Algorithm with Triple DES," in *5th International Conference on Inventive Computation Technologies, ICICT 2022 - Proceedings*, 2022. doi: 10.1109/ICICT54344.2022.9850838.
- [22] S. Karakus and E. Avci, "A new image steganography method with optimum pixel similarity for data hiding in medical images," *Med Hypotheses*, vol. 139, 2020, doi: 10.1016/j.mehy.2020.109691.

- [23] H. Zheng, C. Zhou, X. Li, Z. Guo, and T. Wang, "A Novel Steganography-Based Pattern for Print Matter Anti-Counterfeiting by Smartphone Cameras," *Sensors*, vol. 22, no. 9, 2022, doi: 10.3390/s22093394.
- [24] J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," *Signal Process Image Commun*, vol. 29, no. 3, 2014, doi: 10.1016/j.image.2014.01.003.
- [25] O. M. Al-Shatanawi and N. N. El-Emam, "A New Image Steganography Algorithm Based on MLSB Method with Random Pixels Selection," *International Journal of Network Security & Its Applications*, vol. 7, no. 2, 2015, doi: 10.5121/ijnsa.2015.7203.
- [26] N. A. F. Abbas, N. Abdulredha, R. K. Ibrahim, and A. H. Ali, "Security and imperceptibility improving of image steganography using pixel allocation and random function techniques," *International Journal of Electrical and Computer Engineering*, vol. 12, no. 1, 2022, doi: 10.11591/ijece.v12i1.pp694-705.
- [27] M. M., A. A., and F. A., "A Modified Image Steganography Method based on LSB Technique," *Int J Comput Appl*, vol. 125, no. 5, 2015, doi: 10.5120/ijca2015905908.
- [28] A. A. A. Gutub, "Pixel indicator technique for RGB image steganography," *Journal of Emerging Technologies in Web Intelligence*, vol. 2, no. 1, 2010, doi: 10.4304/jetwi.2.1.56-64.
- [29] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," in *CCNC 2018 - 2018 15th IEEE Annual Consumer Communications and Networking Conference*, 2018. doi: 10.1109/CCNC.2018.8319263.
- [30] M. Damrudi and K. J. Aval, "Image steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and blowfish," *Int J Eng Adv Technol*, vol. 8, no. 6 Special Issue 3, 2019, doi: 10.35940/ijeat.F1033.0986S319.
- [31] M. Damrudi and K. J. Aval, "Two stage steganography on compressed and encrypted message," *International Journal of Circuits, Systems and Signal Processing*, vol. 15, 2021, doi: 10.46300/9106.2021.15.54.
- [32] "A Development of Least Significant Bit Steganography Technique," *Iraqi Journal of Computer, Communication, Control and System Engineering*, 2020, doi: 10.33103/uot.ijccce.20.1.4.
- [33] J. Chandrasekaran, G. Arumugam, and D. Rajkumar, "Ensemble of logistic maps with genetic algorithm for optimal pixel selection in image steganography," in *2nd International Conference on Electronics and Communication Systems, ICECS 2015*, 2015. doi: 10.1109/ECS.2015.7124769.