



**Daffodil**  
*International*  
**University**

An Improved Zig Zag Pixel Selection Approach in LSB Based Secure  
Image Steganography

Submitted By

**Md Wasim**  
**201-35-2992**

**Dept. of Software Engineering**

Supervised By

**Md. Maruf Hassan**  
**Associate Professor**

**Department of Software Engineering, FSIT**

A thesis submitted in partial fulfillment of the requirement for the degree of  
Bachelor of Science in Software Engineering

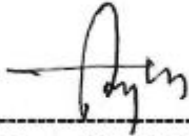
Fall 2023

©All right reserved by Daffodil International University

## APPROVAL

This thesis titled on “An Improved Zig Zag Pixel Selection Approach in LSB Based Secure Image Steganography”, submitted by Md. Wasim (ID: 201-35-2992) 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



-----  
**Dr. Engr. Abdul Kader Muhammad Masum**  
**Professor**

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

**Chairman**



-----  
**Md Khaled Sohel**  
**Assistant Professor**

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

**Internal Examiner 1**



-----  
**Fatama Binta Rafiq**  
**Lecturer (Sr. Scale)**

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

**Internal Examiner 2**



-----  
**Dr. Md. Liakot Ali**  
**Professor**

Institute of Information & Communication Technology (IICT)  
Bangladesh University of Engineering and Technology (BUET)

**External Examiner**

## 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



Md Wasim

ID: 201-35-2992

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

Steganography is a method that employs cryptographic techniques to encrypt sensitive information, thus facilitating the transmission of confidential data from the sender to the receiver over the transmission channel. Despite the fact that this data is not readily detectable, an intruder would have a difficult time capturing it. In this paper, investigates an innovative approach for image steganography that combines the Zigzag Pixel Selection technique with the Blowfish encryption algorithm in order to bolster the security and capacity of concealed data. The encryption procedure incorporates the Blowfish algorithm to ensure strong security of sensitive data, whereas the Zigzag Pixel Selection technique assures covert integration within the image. Blowfish is an exceptionally robust algorithm due to the variable length of its keys, which can vary between 32 bits and 448 bits. The previously mentioned flexibility empowers users to modify the key size in accordance with their particular security needs. Data security is enhanced and resistance to brute-force attacks is generally improved with an extended key. Zigzag patterns are often used in various algorithms for data traversal or manipulation. In the context of image processing, a zigzag pattern might be employed for pixel selection or scanning order. The basic idea is to traverse the pixels in a zigzag fashion rather than a simple left-to-right, top-to-bottom order. Our contribution is to improve the capacity of hidden data while embedding by using a 4-directional pixel selection technique.

**Keywords:** Image Steganography, Capacity, Blowfish Algorithm, XOR, LSB, Zigzag pixel selection technique.

# Table of Contents

<b>APPROVAL</b> .....	<b>i</b>
<b>DECLARATION</b> .....	<b>ii</b>
<b>ACKNOWLEDGMENT</b> .....	<b>iii</b>
<b>ABSTRACT</b> .....	<b>iv</b>
Chapter-1: Introduction .....	1
1.1 Background .....	1
1.2 Fundamental requirement for steganography.....	2
1.3 Problem Statement .....	3
1.4 Research Objective.....	3
1.5 Scope of works .....	4
1.6 Contributions .....	4
1.7 Solution Requirement.....	5
1.8 Thesis Outline .....	7
Chapter-2: Literature Review .....	8
2.1 Commencement of this 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 Analysis and Discussion .....	29

## Table of Figures

Figure: Block diagram of the proposed approach.....	5
Figure: General Steganographic System.....	18
Figure: Embedding Process of the proposed Approach.....	19
Figure: Retrieve process of the proposed approach.....	20
Figure: Block diagram of the proposed approach.....	21
Figure: Block diagram of Blowfish Algorithm.....	25
Figure: 4 Directional Pixel Selection of a Cover Image.....	27
Figure: Zigzag Pixel Selection of a Cover Image.....	28
Fig: Cover image.....	29
Figure: MATLAB Code Implementation.....	35
Figure: A Histogram comparison of the cover and stego pictures.....	32
Figure: Simulation Results using GUI.....	33

## **Lists of Table**

Table 1: Literature Review Table .....	17
Table 2: Metrics for measuring the quality of the suggested method using different standard-sized payloads. ....	31



# Chapter-1: Introduction

## 1.1 Background

The process of securely transmitting messages from a sender to a receiver is called steganography. It should demonstrate that conclusive conclusions concerning the sender and recipient's private communications are impracticable. The secret message is hidden confidential some cover media to reservation this level of concealment, making it improbable that a third party could find it. [1]

Data capacity and secure communication between unreliable organizations are fingered by cryptography. Various tactics are developed to address specific issues; a widely adopted tactic is the utilization of information encryption to obtain confidential data from enterprises. Other methods besides blowfish have become additional popular due to the growing petition for encryption techniques [2].

With the advancement of technology, more information can now be graphically transferred through communication, which has greatly benefited modern professions including commerce, medicine, the military, and others. It is therefore now required to create a protected association in order to transmit sensitive content via communication channels. Researchers have discovered that this significance can help keep unauthorized individuals from managing and accessing data [3]. This proposed solution additionally set up Zig Zag pixel selection mechanism to improve the Capacity of the hidden information. This suggested method aims to carefully balance installation limit and perceptual forthrightness by purposefully selecting pixels at picture boundaries, where visual alterations are less likely to be noticed. This ensures that the host picture maintains its visual integrity, increasing the security of the steganographic cycle and lowering the possibility of skepticism.[4]

As the digital world advances, there is a rising need for safe communication methods. This suggested method advances the state of LSB-based image steganography by fusing cutting-edge zigzag pixel selection algorithms with tried-and-true cryptographic principles. This thesis explores the development and implementation of the suggested remedy, illuminating its effectiveness, security, and potential applications in safeguarding confidential information in the rapidly expanding digital domain. [5] Not only does this suggested solution have excellent cryptography

skills, but it also has a pixel selection technique that is strategically based on image edges. The visual integrity of the host image may be compromised by standard LSB-based steganographic algorithms, which typically have to choose between hiding capacity and perceptual transparency due to embedded information. To circumvent this issue, the model groups pixels together on image edges, where alterations are less noticeable to the human eye. This novel method seeks to achieve an appropriate trade-off between allowing information to remain buried within the host image and minimizing any noticeable effects on its look.[6]

The proposed solution is important because of its potential influence on secure communication practices in addition to its technical complexity. This proposed solution offers a timely response to the growing demands of information security as the digital world develops and adversaries grow more cunning. The goal of this thesis is to shed light on the design, implementation, and performance evaluation of the proposed solution in order to advance knowledge of LSB-based image steganography and its uses for protecting confidential data in the ever-changing digital environment. [1].

## **1.2 Fundamental requirement for steganography**

A successful steganographic technique requires three essential elements: imperceptibility, capacity, and robustness. Being imperceptible is among them. Steganography's primary prerequisite, imperceptibility, emphasizes the hiding of secret data inside a carrier medium without causing appreciable changes. [7] Capacity in image steganography guarantees that the embedded data does not visually differ from the original content. In order to minimize the chance of detection, a high degree of capacity requires carefully choosing embedding locations, such as in the least important bits or areas less sensitive to human vision. The quantity of data that a steganographic method can encode into a particular carrier is measured by its capacity. Capacity is concerned with efficiency, whereas imperceptibility is seeking subtlety. It's critical to strike a balance between capacity and a significant hiding capacity. [8] Capacity optimization techniques frequently take advantage of redundant or less important carrier components, enabling more data hiding without sacrificing the overall visual integrity. Increased capacity is particularly important for situations where a significant amount of hidden data needs to be transmitted. Robustness is the capacity of a steganographic technique to fend off detection and attacks while preserving the confidentiality of the data that is being concealed. Capacity is improved by integrating cryptographic algorithms, as

demonstrated by the proposed solution application of the Blowfish algorithm. This cryptographic layer strengthens the concealed data against attempts at tampering and unauthorized access, enhancing the steganographic technique's overall resilience. For applications where the hidden information needs to be shielded from adversarial scrutiny or inadvertent distortions during transmission, robust steganography is crucial.

### **1.3 Problem Statement**

Problem 1: Unorder pixel selection makes stego image visible.

(“ A LSB Based Image Steganography Using Random Pixel” U. A. E. Ali (2021))

Problem 2: Unencrypted text data process a security risk.

(Bhaskar, Ketaki, Mitali Bakale, Priyanka Chaure, and Priti Shirke. "Image Steganography for data hiding Using Huffman code, Zigzag and OPAP." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 4, no. 6 (2015))

The problem statement Unorder pixel selection makes stego image visible. It implies that current steganographic strategies are vulnerable to unauthorized extraction and location of covered information due to the absence of robust safety measures affecting them. The ramifications include the potential for private information concealed in photos to be jeopardized as a result of flaws in existing protocols. In this case, the identification of the steganographic interaction itself raises potential concerns about data confidentiality in addition to the expected disclosure of hidden information by unauthorized parties. An alternative explanation centers on a particular method within image steganography, specifically approaches that utilize the Least Critical Piece (LSB). It claims that with commonly used LSB-based steganography, achieving optimal capacity is challenging. Subtleness is crucial to steganography because it guarantees that any changes made to the cover image (or implant stowed-away data) are invisible from the exterior. That's what the claim implies: the steganographic images exhibit observable artifacts as a result of the difficulty in maintaining subtlety brought about by LSB-based techniques. These old changes might have been inadvertent, raising questions about the procedure and possibly disclosing private data, which would undermine the steganographic cycle's effectiveness.

### **1.4 Research Objective**

The objective is to solve the weak security features of the currently used image steganography techniques, which make them susceptible to detection and unauthorized data extraction. This

entails creating a new model for image steganography that enhances data security. This underscores how inadequate the security measures in the currently in use image steganography techniques are and raises concerns about the privacy of hidden data. Here, the objective is to propose an orderly pixel selection technique to avoid easy detection. This might entail incorporating cutting-edge cryptographic methods, like the Blowfish algorithm that you mentioned in the title of your thesis. Strengthening steganography and making it more resilient to unauthorized data extraction and detection should be the main objectives of the new model. By doing this, the confidentiality of the data concealed within the steganographic images will be improved, assuaging concerns about possible security holes in current techniques. Commonly used LSB-based image steganography techniques have trouble reaching optimal imperceptibility, which causes observable artifacts. This emphasizes the necessity of creating a steganographic algorithm in the spatial domain that is in line with the techniques and focuses on enhancing capacity. The objective here is to design and develop a steganographic algorithm for the spatial domain. This algorithm should be specifically created to ensure that any modifications made during the data hiding process are practically invisible to the unaided eye in order to maximize capacity. Using techniques like zig zag pixel selection, which lessens perceptible artifacts and helps guarantee that hidden information is seamlessly integrated into the carrier image, can improve the overall visual quality of steganographic images.

## **1.5 Scope of works**

This paper will only address image steganography with the solution I will offer. It is not applicable to audio or video steganography. Right now, we are working on this paper on a small scale. I would advise future research on this topic to make use of audio or video.

## **1.6 Contributions**

Contribution of this paper is given as follows:

- The proposed approach come out from traditional pixel selection technique where 4 dimensional zig zag pixel selection technique is used that is difficult to attackers to recognize the presence of secret data.
- Both the Blowfish algorithm and XOR-based LSB provide good image quality as well as enhance the capacity of the image.

## 1.7 Solution Requirement

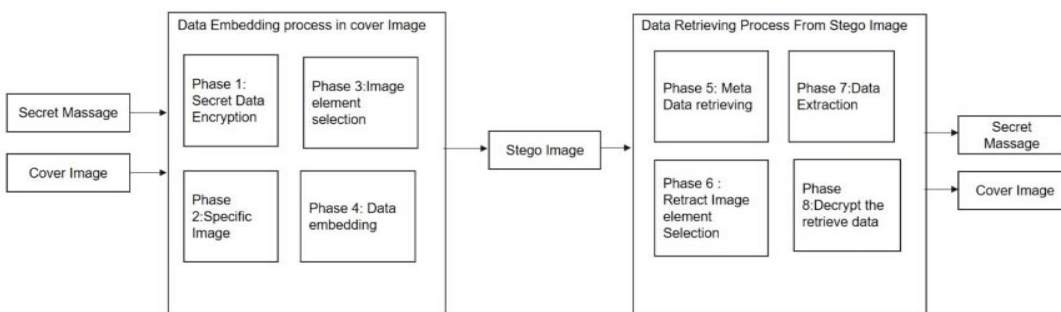


Figure: Block Diagram of the proposed image Steganography Approach

**Figure: Block diagram of the proposed approach**

To start with, we will discuss the Information Installing Interaction. The Stage 1: Restricted information Encryption by Blowfish: In this stage, the privileged information is encoded utilizing the Blowfish calculation. Blowfish is a symmetric key block figure known for its security and effectiveness. The encryption interaction guarantees that the delicate data is changed into a safe and indistinguishable configuration, shielding it from unapproved access during the installing system. Phase 2: Explicit Picture: A particular cover picture is chosen for the implanting system. This picture fills in as the transporter for the encoded privileged information. The decision of the cover picture is critical, as it decides how well the implanted information can be hidden inside the visual substance without drawing in doubt. Phase 3: Zig-Zag Pixel Selection for Image Element Selection: The Crisscross pixel determination procedure is utilized to pick explicit components inside the cover picture. This procedure efficiently chooses pixels in a crisscross example across the picture. The chose pixels will be utilized to implant the encoded information, guaranteeing a conveyed and subtle combination of the restricted data. Phase 4: Information Implanting: A secure and reversible method is used to embed the encrypted secret data into the selected image elements during this phase. The objective is to coordinate the information so that it becomes impalpable to the natural eye while keeping up with the trustworthiness of the cover picture. This stage requires cautious thought of the picture's qualities to keep away from visual relics. The Data Retrieval

Procedure will then be discussed: Phase 5: Obtaining Meta Data: The first move toward quite a while recovery includes extricating metadata related with the inserted information. This metadata incorporates data about the area and configuration of the implanted substance inside the cover picture. Understanding this metadata is critical for resulting steps in the recovery cycle. Phase 6: Withdraw Picture Component Choice: Like Stage 3, this stage utilizes the Crisscross pixel determination procedure to distinguish and choose the particular picture components that contain the implanted information. The crisscross example guarantees an orderly way to deal with finding the significant pixels for information recovery. Phase 7: Information Extraction: When the picture components containing the installed information are recognized, the information extraction process starts. The chose pixels are handled to recover the installed data while limiting any effect on the cover picture. This stage means to remove the encoded information with no misfortune or defilement. Phase 8: Unscramble the Recovered Information: The last stage includes unscrambling the recovered information utilizing the Blowfish calculation or a proper decoding technique. This step is fundamental to recuperate the first, delicate data from the encoded structure. The retrieved data will remain in their original, meaningful state if this phase is successfully completed. The entire method for embedding and retrieving data using the specified methods and algorithms is described by these eight phases taken together.

Image quality is the primary objective of the stenographic system. The most popular metrics for assessing image quality are Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) [9]. One metric to assess how much the embedding image has degraded in comparison to the cover image is PSNR.

$$MSE = \left(\frac{1}{MN}\right) \sum_{i=1}^M \sum_{j=1}^N (X_{ij} - X'_{ij})^2 \quad (1)$$

$$PSNR = 10 \log_{10} \frac{I^2}{MSE} \quad (2)$$

MSE measures the difference between two images. PSNR and MSE defined in equations 1 and 2. Where is the row and the column pixel in the original (cover) image, is the row and the column pixel in the reconstructed (Stego) image, and are the height and the width of the image, is the dynamic range of pixel values, or the maximum value that a pixel can be taken, for 8-bit images; I=255.

## **1.8 Thesis Outline**

The data being presented emphasizes how important secure communication is in the digital age and how sensitive data can be protected with LSB-based image steganography. It offers an incredible steganographic technique that boosts capacity by combining cryptographic principles with random pixel selection. Three essential components are necessary for steganography to be successful: robustness, capacity, and imperceptibility. This proposed solution integrates the Blowfish algorithm and makes deliberate pixel selections to address these issues. The problem statement draws attention to the drawbacks of current steganographic methods as well as the challenges faced by LSB-based strategies in maintaining optimal imperceptibility. The proposed solution is centered on utilizing state-of-the-art cryptographic methods to enhance data security for image steganography, specifically in the spatial domain.

## Chapter-2: Literature Review

### 2.1 Commencement of this Study

Image steganography is the process of hiding confidential information inside an image so that it is difficult to locate or decipher. While cryptography focuses on making a message unreadable for unauthorized users, steganography tries to conceal the embedded information itself, not the content. Using image steganography, secret data is embedded into the pixel structure of an image. Changing the pixel values' least significant bits (LSBs) is the most popular method. Little variations in these bits are less likely to be detected by the human eye because the LSBs contribute less to the perception of color or intensity overall. Digital watermarking, copyright protection, and secure communication are just a few of the uses for image steganography. It's crucial to remember that steganography is not infallible, and detection techniques have been created to recognize photos that have been tampered with during the steganography process. In a never-ending game of cat and mouse, researchers strive to continually improve both steganographic techniques and detection methods. Two key components of steganography are the type of carrier and the embedding technique. For steganography, different carriers are used as the cover message. Since images are the most commonly transferable messages over the Internet, image steganography is the widely used carrier medium. The field of image steganography has seen a great deal of research. There are essentially two categories of image steganography. [10], [11]:

**1) Spatial domain:** This approach embeds the data directly into the pixel intensity values. It is applied only to lossless compressed images. since embedding depends on the image's format. In the spatial domain, one often utilized strategy is the replacement of least significant bits (LSB).

**2) Transform domain:** This technique embeds information into the frequency domain of an image that has already undergone transformation. Different transformation methods, including the Discrete Cosine Transform, are used to conceal data in an image. This method works with lossy-compressed JPEG photos.



## 2.2 The history of image Steganography

The history of image steganography predates even the concept of information concealment, which dates back to antiquity. While the status of image steganography today has evolved in tandem with technical breakthroughs, the underlying principles have historical roots. Here is a brief overview of the history of image steganography: Historical reports state that the Greeks used a technique called "scytale" to hide messages. The message was written on a strip of parchment that was wound around a rod of a certain diameter. When unwound, the message would be garbled and seem unintelligible. The addressee might interpret the message with a rod of the same diameter. Throughout history, several kinds of invisible ink have been employed to conceal messages. These inks may be exposed to light through the use of chemicals, heat, or other methods. During World War II, steganography was used by both the Axis and Allied forces. For example, small pictures the size of a punctuation mark called microdots were used to hide information. Steganography was still used to encrypt letters, radio broadcasts, and other kinds of correspondence throughout the Cold War. Steganography moved into the digital sphere as computer use grew. Data hiding techniques were used in the past to conceal information in digital image and audio files' least significant sections. With the increasing popularity of digital steganography, scientists began developing more intricate methods. The popular image steganography algorithm F5 was made available during this period. With the rise in popularity of digital communication and the internet, steganography became more accessible. Researchers have developed many techniques to hide data from image, video, and audio recordings. Researchers investigated innovative methods to embed data while causing the least amount of harm to the carrier file as steganography tools and techniques advanced. Three applications of image steganography are secure communication, digital watermarking, and authentication. It developed into a tool for verifying the authenticity of internet material and protecting intellectual property.- Challenges: Alongside the development of steganalysis, or methods for locating hidden data, steganography gained popularity. Consequently, there has been an ongoing arms race between those searching for secret content and stenographers. To sum up, picture steganography has a long history that stretches from the primordial to the modern eras. The rapid advancement of communication technology has been driven by their need to communicate information in a secure and covert manner. During the picture steganography review process, the efficacy of steganographic techniques, the development of detection tools (steganalysis), and overall security are all assessed.

## **2.3 The evaluation of image Steganography over time**

An outline of the development of picture steganography evaluation is provided below:

Early studies on digital steganography focused on foundational techniques such as embedding LSBs (Least Significant Bits). These methods were simple and somewhat surreptitious, but they lacked robustness and security. Evaluation criteria included the imperceptibility of the steganographic alterations (i.e., how visually identical the Stego-image is to the original) and the capacity to conceal data without triggering red flags. The introduction of sophisticated steganographic algorithms like Out Guess and F5. The goals of these algorithms were to increase security and robustness while addressing the shortcomings of the earlier techniques. Metrics like resistance to steganalysis, payload capacity (the amount of data that could be hidden), and the capacity to survive standard image processing operations without losing the hidden information were taken into consideration by researchers. The focus shifted to strengthening steganographic algorithm security as steganalysis techniques advanced. This required creating defenses against steganalysis based on statistics and machine learning. More sophisticated embedding strategies, such as spatial domain techniques, transform domain techniques (like frequency domain techniques), and adaptive methods that change based on the properties of the cover image, were investigated by researchers. Researchers looked into combining cryptography and steganography to improve security. The goal of this combination—known as steganographic encryption—was to offer secret communication in addition to secrecy. The resistance to attacks like chosen-plaintext attacks, known-plaintext attacks, and adaptive steganalysis was added to the evaluation criteria. Steganalysis and steganographers are still engaged in an arms race. The problem for researchers is to create steganographic techniques that work and can withstand ever-more-advanced detection techniques. Current investigations investigate novel frameworks, like deep learning-driven steganography and steganalysis, in order to overcome the drawbacks of conventional methods. Steganographic techniques that can function in various and difficult environments are required for real-world applications like digital forensics and secure communication. Overall, from simple imperceptibility to more intricate considerations of security, robustness, and integration with cryptographic techniques, the evaluation of image steganography has progressed. With an emphasis on offering safe and discrete means of information exchange, the field keeps up with technological advancements and adapts to new opportunities and challenges.

## 2.4 Application of image Steganography

The following are some scenarios in which your suggested method can be applied:

Secure communication is essential for military and defense applications. Your method can be used to secretly transmit classified data by embedding sensitive information into images. Watermarking and Authentication: You can provide digital media tracking and authentication by watermarking digital files using your steganographic technique. This is particularly beneficial in stopping unauthorized dissemination and duplication. Digital Assets: The media and entertainment industries can use your method to prevent unauthorized use or distribution of digital images, videos, or audio files by adding ownership or copyright information. Ensuring the privacy of patient data in medical imaging is essential. You can utilize your steganographic technique to hide sensitive patient data from view without compromising the diagnostic data's accuracy. You can use your approach to safely transfer secret legal or commercial papers. Data that is contained within images is transferred with an extra layer of protection. Safe Information Transmission for Journalists: Journalists and whistleblowers can use your method to securely transmit proof or sensitive material without attracting attention to themselves. Secure cooperation: Researchers and academics working on sensitive projects or collaborative research can use your method of embedding information into photos for secure communication and cooperation. Private Messaging: Those who are worried about their privacy can use your private messaging service. When text is added to photographs, there is an additional layer of hiding. Protecting Digital information: Content providers can use your steganographic technology to embed data into photos as part of a DRM strategy to prevent unauthorized access or distribution of digital information.

10. Counter-Forensic Techniques and Anti-Forensics: You can talk about your approach in regard to counter-forensic techniques and anti-forensics, which are ways that people try to hide information from digital forensic investigation.

The author put forth a novel approach in [12]. This method conceals the secret message by searching for identical bits between the image pixel value and the secret message. One randomly chosen pixel separates the image into three layers (Red, Green, and Blue). Next, by searching for similar bits, two bits of the secret message are embedded in each layer's two least significant bits. A spatial domain technique is proposed in [10]. The proposed method uses the third least significant bit (LSB-3) of the cover picture to embed the message bits with the goal of minimizing the difference between the cover and the Stego-cover. Then, depending on the message bits, LSB

-1 and 2 can be changed. [13] For extra protection, the message bits have been permuted using a stego-key prior to embedding. However, the findings of the approach showed that the LSB -1 method had higher PSNR values than the recommended method, meaning that even if the capacity was the same, the LSB -1 image was of greater quality than the modified one.

The author has presented an image steganography method based on random pixel selection within the desired image area and LSB replacement [11]. After generating random numbers, it selects the region of interest where the required message is embedded along the random pixels. Increasing security in situations where the password is inserted using LSB pixels is the aim of this technique. Using a key for both data encryption and decryption, the Blowfish Encryption Algorithm is a straightforward, quick, and small encryption method. With an XOR operation and a function (F) in each round, it requires sixteen rounds. Since the Blowfish algorithm does not alter the key, it can be used in applications like file encryptors and communication lines where a key is not needed. But when it comes to supporting frequent key changes or using packet switching as a one-way hash function, Blowfish is inefficient. The algorithm is made up of a Feistel network that allows for key expansion and encrypted data encryption. [14]. The approach described by [15] splits the image data into blocks for encryption using a configurable key size of 448 bits. Because it produces more efficient results than the previous algorithm by increasing the number of rounds, the modified Blowfish algorithm is a noteworthy standard encryption algorithm. Because the algorithm can employ a variable length key, it performs better and more securely than symmetric encryption algorithms like AES and DES. Because it uses an extra block switching technique to scramble data, the improved Blowfish algorithm is more secure than the original Blowfish algorithm. The upgraded Blowfish method generates random numbers on image pixels.[16]

With image steganography, words and images can be concealed within images. Discrete Cosine Transform, Transform Domain, Spread Spectrum, Filtering and Noising, Masking, MSB, and LSB are a few of the methods applied here (Kamble et al., 2013). Because the MSB approach gives the steganographic image a suspicious appearance to humans, it is not a good alternative for steganography systems. Spatial and frequency domain steganographic techniques are the two primary categories [17]. With this method, a predefined secret key is used to disperse the secret message throughout each colour plane. Nagaraj et al. proposed a modified PVD-based steganography approach [18]. An embedding technique called the Pixel Value Difference Technique (PVD) was introduced in [9]. With this technique, data is embedded into each pixel

after the image is divided into randomly chosen non-overlapping blocks of nearby pixels. The amount of data embedded, or the number of last significant bits used, is directly related to the difference in brightness of adjacent pixels. This uneven embedding in PVD leads to unusual steps in the pixel difference histogram of the stego picture. A strengthened approach (IPVD), proposed in [19], has capitalised on this flaw. The adaptive edge LSB approach (AE-LSB) [20] has also removed this uneven pixel difference and increased capacity by including a readjusting phase. While there is a single fundamental flaw in all of these techniques, their ability to integrate additional data in regions with notable pixel variations makes them edge adaptable. These approaches look at pixel pairings at random instead than selecting based on larger differences. Consequently, they may end up with random data embedding and texture distortion in the LSB plane of the image. It is found that these methods are not very effective [21].

An ideal LSB substitution based on a genetic algorithm can assist obtain better stego-image quality than with the conventional LSB technique [22]. Furthermore, Chang et al.'s [23] efficient and fast optimum LSB approach, based on the dynamic programming strategy, allows Wang et al.'s scheme [14] to compute at a faster pace. Lin additionally introduced a simple LSB technique based on the modulus function [14] to enhance the stego-image quality. [24] presents a unique easy LSB approach based on optimal pixel correction. Wang has presented two novel techniques based on the modulo operator. A robust steganographic technique needs to be implemented in order to stop an attacker from getting access to private information both during transmission and receipt [25].

An edge-based picture steganography approach that utilises the Sobel Edge Detector and the 2k correction method was proposed by the author of "Steganography in images using Sobel Edge Detection with 2k Correction Method" [15]. Better imperceptibility is achieved by using the 2kmethod since the cover image and stego image are different. If there is a difference between the real and SPV values that is larger than  $2k-1$ , the Stego Pixel Value (SPV) is modified by either  $SPV+2k$  or  $SPV-2k$ . The Mean Square Error (MSE) and PSNR are calculated in an experiment. [26] This method offers greater embedding capacity and PSNR than the LSB approach.

The suggested method for image steganography takes a fresh approach to achieving capacity in the LSB-based space. By precisely integrating information into the least significant bits (LSBs) of pixel values using XOR-based embedding, the technique minimises visible changes in the host image. XOR procedures increase capacity without compromising the visual integrity of the cover image by making subtle changes that are difficult for the human eye to see. An extra degree of

security is also added by including the Blowfish algorithm during the embedding procedure. Blowfish ensures that the hidden data is encrypted to safeguard the privacy of the embedded data and stop unauthorised access. Because of this encryption, naturally occurring fluctuations in pixel values make changes to the LSBs less obvious. By utilising the edge's optical characteristics, where subtle alterations are less noticeable, the zigzag pixel embedding increases capacity. With careful pixel selection, information within image edges can be successfully hidden, and the influence on smooth sections is minimised. In summary, this method uses strategic LSB-based XOR embedding, Blowfish algorithm encryption, and selective pixel embedding in edge regions to accomplish capacity. Together, these methods guarantee that spectators cannot identify the steganographic changes.[27]

This problem statement addresses the issue of steganographic vulnerability in LSB-based secure image steganography caused by the use of an unordered pixel selection technique. It is expected that this technique will expand the perceptibility of the secret information, risking the steganographic interaction's security. In the second problem statement, security risk connected to processing unencrypted text data in image steganography is emphasized in this problem statement. It suggests that there might not be enough security protections in place for the way text data is currently handled, endangering the confidentiality and integrity of the hidden data.

## **2.5 Research Gap**

Problem 1: Unorder pixel selection makes stego image visible.

(“ A LSB Based Image Steganography Using Random Pixel” U. A. E. Ali (2021))

Problem 2: Unencrypted text data process a security risk.

(Bhaskar, Ketaki, Mitali Bakale, Priyanka Chaure, and Priti Shirke. "Image Steganography for data hiding Using Huffman code, Zigzag and OPAP." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) 4, no. 6 (2015))

The issue description A stego image can be seen by using an unordered pixel selection. It suggests that because there aren't enough strong safety precautions in place to protect them, existing steganographic techniques are susceptible to unauthorized extraction and location of covered information. The implications include the possibility that private information hidden in images could be compromised due to weaknesses in current protocols. In this instance, in addition to the anticipated disclosure of confidential information by unauthorized parties, the identification of the steganographic interaction itself raises possible concerns regarding data confidentiality. Another

explanation focuses on a specific technique in image steganography, namely techniques that apply the Least Critical Piece (LSB). It states that reaching optimal capacity with widely used LSB-based steganography is difficult. Subtleness is crucial to steganography because it guarantees that any changes made to the cover image (or implant stowed-away data) are invisible from the exterior. That's what the claim implies: the steganographic images exhibit observable artifacts as a result of the difficulty in maintaining subtlety brought about by LSB-based techniques. These old changes might have been inadvertent, raising questions about the procedure and possibly disclosing private data, which would undermine the steganographic cycle's effectiveness.

## 2.6 Research Objective

The unorganized pixel selection in RO1 makes the stego image more noticeable and discoverable, as it attempts to solve the linked issue in this problem. Offering a novel approach to pixel selection is the RO1's focus. This style will be distinguished by its neatness, ensuring that the pixel selection process is well-organized. Improving the cover image's security is the goal. The second research goal suggests incorporating a cryptographic algorithm into the picture steganography process in order to address PS2. This leads to the creation of a double-layered model, which boosts security. Reducing security risks associated with processing unencrypted text data and enhancing the overall security of the steganographic system are the main objectives.

RO1: To propose an orderly pixel selection technique to avoid easy detection.

RO2: To propose secure a model by including Cryptographic algorithm in image Steganography.

Mapping:

1. RO1 → PS1
2. RO2 → PS2

This mapping demonstrates the direct alignment between the acknowledged problem statement (PS1) and the associated research objective (RO1). Stated differently, the intended solution aims to address the issue of stego images emerging due to unordered pixel selection. The issue will be fixed and the security of LSB-based secure image steganography will be reinforced by mapping PS1 to RO1 and using an orderly pixel selection technique. The idea is to create a technique that avoids easy detection by purposefully selecting pixels in a more organized manner.

This mapping creates a relationship between the research objective (RO2) and the second problem statement (PS2). The processing of unencrypted text data poses a security risk, as highlighted by

PS2, and the corresponding RO2 seeks to address this issue by presenting a double-layered model. To address the identified security risk, this model combines image steganography with a cryptographic algorithm. The goal of mapping PS2 to RO2 is to build a more reliable and secure steganographic system that can manage unencrypted text data efficiently while preserving the integrity and confidentiality of the hidden data.

## **2.7 Closure of this study**

For the purpose of developing the proposed thesis paper, "An Improved Zig Zag Pixel Selection Approach in LSB Based Secure Image Steganography" a thorough review of the body of literature on image steganography has been conducted. The literature research has revealed important insights into the current status of steganographic techniques and has brought attention to the need for enhanced data security and capacity in the spatial realm. The reviewed investigations have consistently shown the shortcomings in traditional LSB-based steganography techniques, emphasising the need for developing alternative approaches to address these issues. Data hidden in image files may be made more secure by combining the XOR procedure and the Blowfish algorithm. By carefully balancing data concealment and visual fidelity, the creative integration of zigzag pixel selection significantly enhances the recommended 4 dimensional approach capacity. The significance of developing steganographic approaches to guard against modern dangers and evolving detection methods has been underlined by the literature review. Through the synthesis of insights from many sources, this review has positioned the technique as a unique solution that not only enhances data security but also focuses on boosting capacity within the spatial domain. As we move on with the thesis, the literature study has laid the foundation for a detailed investigation of the intricacies of XOR-based LSB steganography, the stability of the Blowfish algorithm, and the efficacy of zigzag pixel selection. The combined data that was taken from the literature study serves as a very useful road map that guides the research in the direction of developing a cutting-edge steganographic methodology.



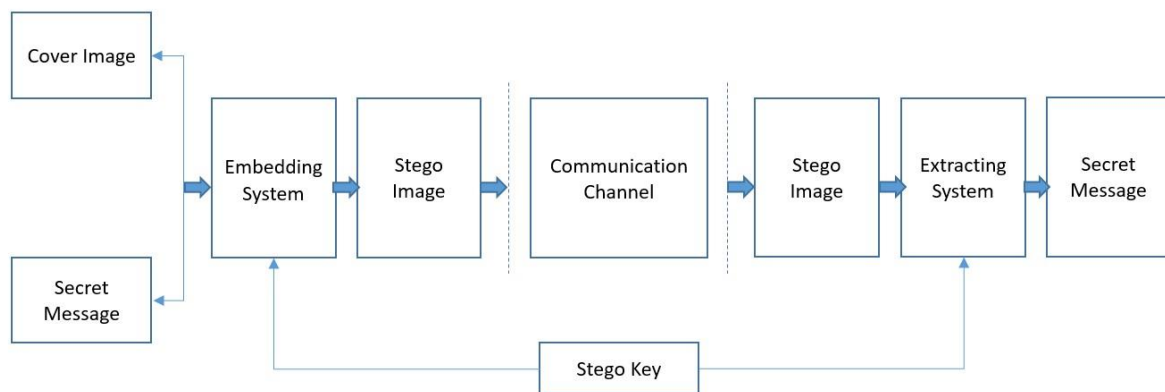
Researcher Name	Year	Technique	Capacity	Limitation	PSNR
Pratiksha Sethi	2018	LSB based image steganography	N/A	Improving algorithm efficiency for larger data while enhancing cipher strength against brute force attacks.	73%
Kamaldeep Joshi	2020	The mixture of the YCbCr Color Model, 2-bit XOR LSB substitution 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

In actuality Steganography can be divided into five kinds based on the cover media: image, audio, video, text, and network steganography. Image steganography conceals secret communications by using an image as the cover object. The pixel intensities of the cover image are used in this method to conceal the secret data. Information can be embedded in the cover image using a variety of techniques, most broadly classified as spatial domain and transform domain techniques. Singular value decomposition, LSB substitution, pseudorandom method, distortion method, Discrete Fourier transformation method (DFT), Discrete Cosine transformation method (DCT), Discrete Wavelet transformation method (DWT), etc. are some of these methods. These methods can be broadly categorized into spatial domain and transform domain techniques.[28]



**Figure: General Steganographic System**

In Figure the general steganographic system is displayed. The cover image has the secret information implanted into it using the appropriate procedure and stego key in the embedding system. The message is then extracted from the stego image by the recipient using the stego key and the method that was used after receiving the stego image across the communication channel. Two fundamental prerequisites for image-based steganography are thought to be crucial to the concealing process by researchers.[29], [30] First, parts of a secret message can be hidden in an image using a steganography technique so that the original image and the stego-image are identical

to each other, making the secret message invisible. Second, a substantial amount of secret data should be able to be incorporated into the cover image using the method without sacrificing imperceptibility. Because the link between these two objectives needs to be balanced, attention should be taken while choosing the settings of the digital steganography technique. For instance, imperceptibility will be impacted if we raise the capacity above a certain level, and so forth.

### 3.2 Proposed Method

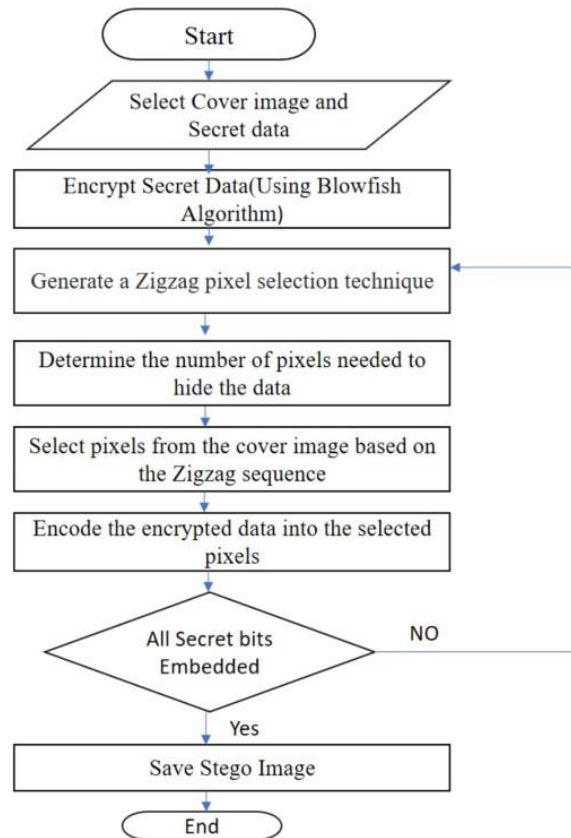


Figure :Embedding process of the proposed Approach

**Figure: Embedding Process of the proposed Approach**

The choice of a cover image and secret data, which is then encrypted in Step 3 using the Blowfish technique, kicks off the embedding process. The secret data is first secured by the Blowfish encryption before being incorporated into the cover image. The Zigzag pixel selection technique, which is generated in Step-4, offers a better way to choose pixels in a particular order. In order to ensure a reliable and effective steganographic strategy, this sequence is used in Step 6 to calculate the amount of pixels required to conceal the encrypted data. Step 6 introduces a novel method of

geographically distributing the hidden information by selecting pixels from the cover image according to the Zigzag sequence. Step 7 then completes the concealment process by embedding all of the secret bits into the chosen pixels. Step 8 then saves the stego picture that contains the hidden data. The final stego image, which represents the cover image with smoothly integrated secret data, is the result of the embedding procedure. Step-9 signifies the completion of the embedding phase and the method. The total security and efficacy of LSB-based secure image steganography are increased by this all-inclusive methodology, which combines encryption, an enhanced Zigzag pixel selection approach, and effective embedding techniques.

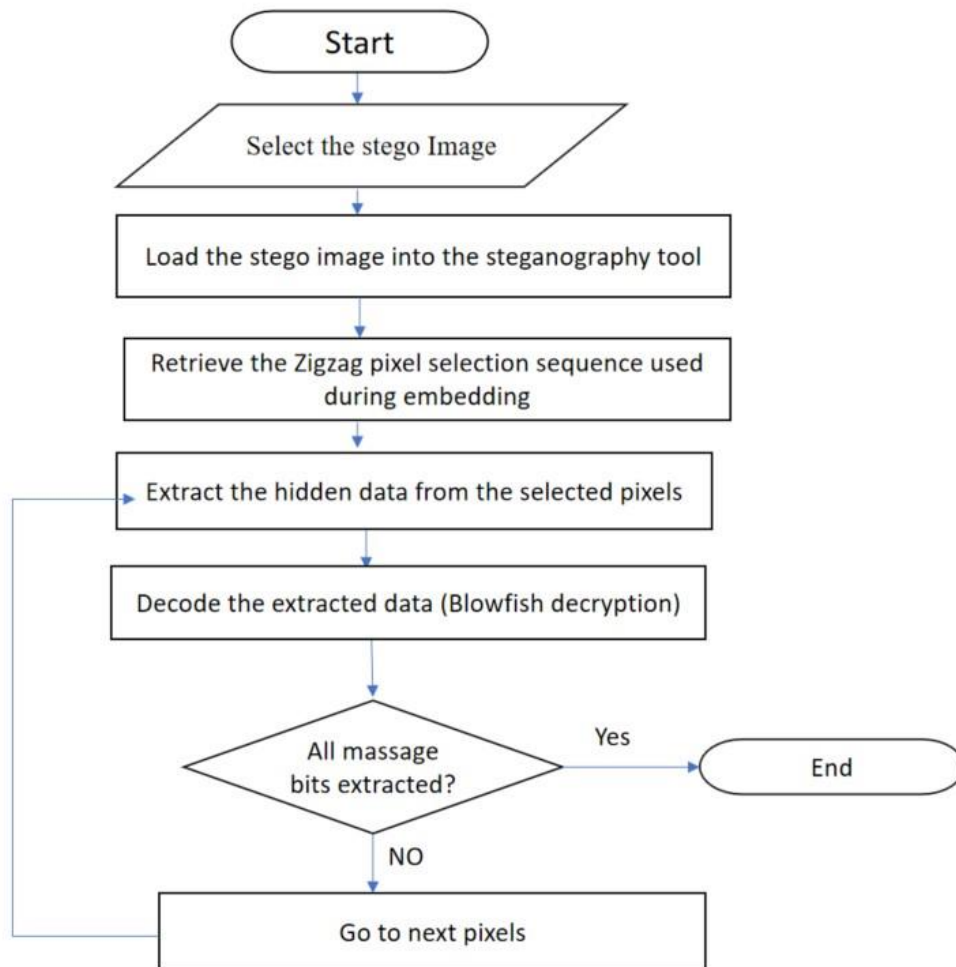
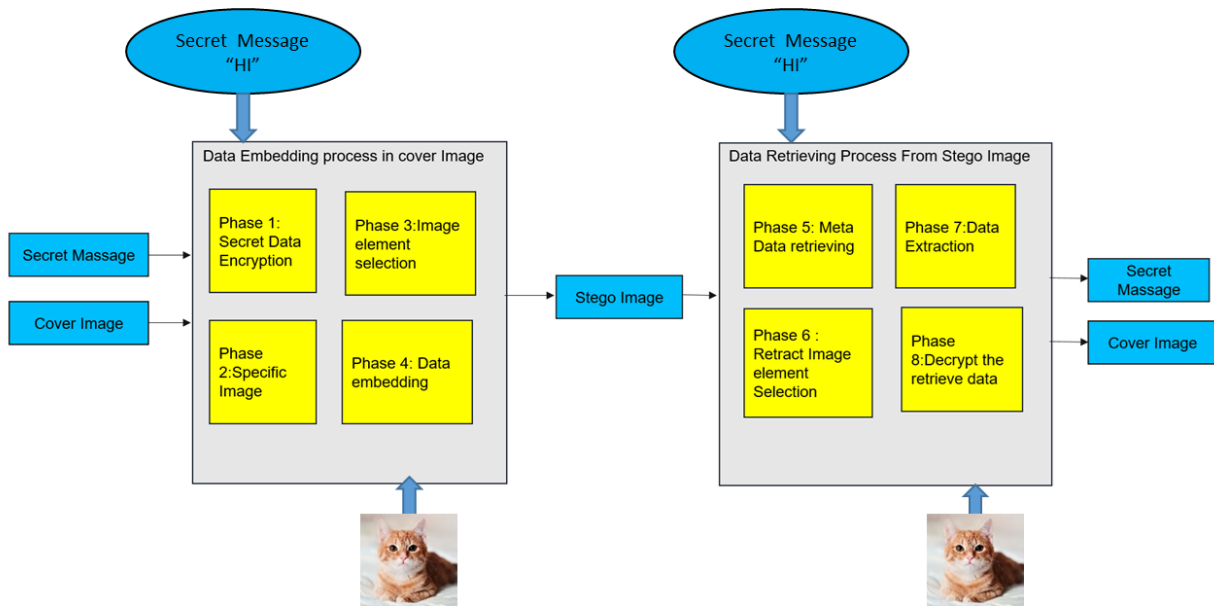


Figure : Retrieve process of the proposed Approach

**Figure: Retrieve process of the proposed approach**

Selecting the stego image in Step 2 and importing it into the steganography tool in Step 3 initiate the extraction process. Step 4 involves retrieving the Zigzag pixel selection sequence that was used throughout the embedding procedure. For the purpose of precisely locating the pixels holding the hidden data, this order is essential. In Step 5, the information that has been steganographically embedded is kept intact by extracting the hidden data from the chosen pixels using the Zigzag sequence that has been obtained. Step 6 then involves decoding the recovered data using Blowfish decryption, which reverses the encryption that was used during embedding. The procedure verifies in Step-7 whether every message bit has been correctly extracted. If not, Step-8's subsequent pixels are extracted as part of the extraction procedure, guaranteeing a complete and exhaustive recovery of the hidden data. The completion of the extraction process is ensured by using this repeated strategy until all message bits are successfully extracted. Zigzag pixel selection, iterative bit extraction, and Blowfish decryption are combined to improve the extraction process's accuracy and dependability in safely obtaining the original secret data from the stego image. For a reliable and secure picture steganography system, the methodology makes sure that encryption and steganographic techniques are seamlessly integrated throughout both the embedding and extraction stages.



**Figure: Block diagram of the proposed approach**

Certainly! Let's delve into Phase-1. Generate a secret key (e.g., a random sequence of bits) to be used for both encryption and decryption. This key must be kept confidential as it is crucial for the security of the encryption process. If the secret message "ff09" is not of the required block size for Blowfish (64 bits), pad it to meet the block size. For example, "ff09" can be padded to "ff09000000000000" to match the 64-bit block size. Use the Blowfish algorithm to encrypt the padded secret message with the generated key. Blowfish operates on 64-bit blocks and uses a series of key-dependent S-boxes and a complex key expansion process. The result of the Blowfish encryption is the encrypted version of the secret message. This encrypted data is now ready to be embedded into the cover image. Certainly! Let's delve into Phase-2. Select the cover image for steganography. In this case, the chosen cover image is "Dog.png." Optionally, perform any necessary preprocessing on the cover image. This may include resizing the image, converting it to grayscale, or applying other modifications based on the requirements of the steganography method. Analyze the chosen cover image to determine its characteristics, such as dimensions (width and height in pixels), color depth, and other relevant features. This analysis is essential for ensuring compatibility with the steganography algorithm and determining the available capacity for data hiding. Estimate the capacity of the cover image to determine how much data can be embedded without significantly altering the visual quality of the image. This estimation is crucial for determining the amount of information that can be hidden without raising suspicion. Confirm that the selected cover image meets the requirements for the steganography process, including size, format, and any other specifications dictated by the chosen algorithm and technique. Certainly! Let's delve into Phase-3. Start traversing the pixels of the cover image in a zigzag pattern. This traversal can start from the top-left corner or any other predetermined location. Use a zigzag pattern to visit pixels in a sequence that alternates between moving horizontally and vertically. The pattern could look like this:

This pattern ensures that pixels from different areas of the image are selected, providing a diverse set of locations for data embedding. For each position in the Zigzag pattern, select the corresponding pixel in the cover image. These selected pixels will be candidates for data embedding. Depending on the capacity estimation from Phase-2, adjust the number of pixels to be selected. Ensure that the selected pixels have sufficient capacity to embed the encrypted data without causing noticeable visual changes. Record the coordinates of the selected pixels (e.g., (x1, y1), (x2, y2), ...) for later use during the data embedding process. Certainly! Let's delve into Phase-

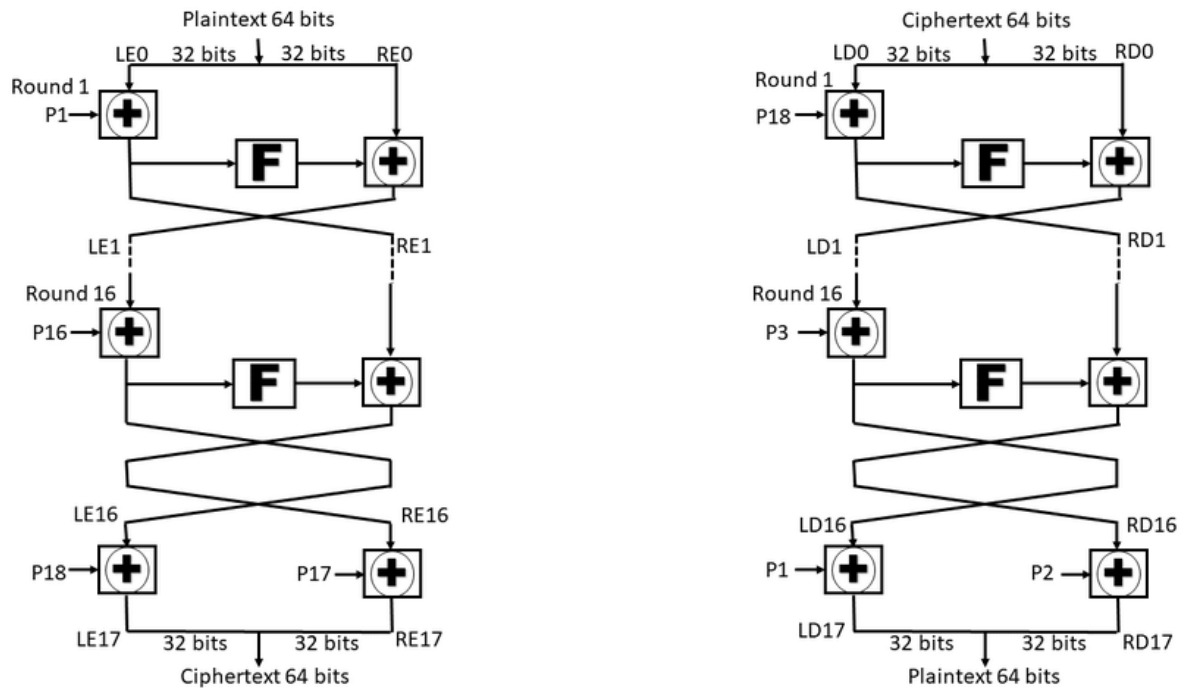
4. Obtain the encrypted data generated in Phase-1 using the Blowfish algorithm. Convert the encrypted data (in hexadecimal or any other format) to its binary representation. This is necessary for the XOR LSB embedding, which modifies the least significant bit of the cover image pixels. For each selected pixel obtained in Phase-3, perform the XOR LSB embedding. This involves replacing the least significant bit of the pixel's color values (e.g., Red, Green, or Blue in the case of an RGB image) with the corresponding bit from the binary representation of the encrypted data.

For example, if the least significant bit of the Red channel is '0101' and the corresponding bit in the binary representation of the encrypted data is '1', then replace the least significant bit with '0101 XOR 1 = 0100'. Repeat the embedding process for all the selected pixels obtained through the Zigzag Pixel technique in Phase-3. Save the modified image after embedding the encrypted data. This new image now contains the hidden information. Optionally, visually inspect the stego-image to ensure that the changes are imperceptible to the human eye. The goal is to hide the data without causing noticeable visual artifacts. Certainly! Let's delve into Phase-5. During the embedding process in Phase-4, essential information such as the encryption key, Zigzag Pixel Selection pattern, and any other relevant parameters should be saved as metadata within the stego-image. This information is necessary for the correct extraction of the hidden data. Define a specific format for storing metadata within the stego-image. This format should be structured and easily interpretable during the extraction process. It may include fields for the encryption key, Zigzag Pixel Selection parameters, and any other necessary details. Embed the metadata information into the stego-image using a secure and consistent method. This could involve modifying specific pixels or regions within the image to store the metadata without causing noticeable changes. Before proceeding with data extraction, ensure that the metadata retrieval process is well-documented and that the necessary information can be easily accessed from the stego-image. Certainly! Let's delve into Phase-6. Extract the metadata stored in the stego-image, specifically the information related to the Zigzag Pixel Selection technique. This information is necessary to reconstruct the pattern used during data embedding. Using the information retrieved from the metadata, reconstruct the Zigzag Pixel Selection pattern that was applied during the embedding process in Phase-3. Perform a reverse Zigzag traversal on the stego-image using the reconstructed pattern. This means visiting the pixels in the reverse order of the Zigzag pattern to identify the pixels that were originally selected during embedding. Record the coordinates of the pixels identified during the reverse Zigzag traversal. These are the pixels that were originally selected for data embedding in Phase-3.

Validate the integrity of the Zigzag Pixel Selection process by comparing the recorded coordinates with the metadata information. Ensure that the reconstruction process accurately reflects the original pixel selection. Certainly! Let's delve into Phase-7. Use the recorded coordinates of the selected pixels obtained during Phase-6 to identify the pixels in the stego-image that were originally chosen for data embedding. For each selected pixel, extract the least significant bit (LSB) of the color values (e.g., Red, Green, or Blue in the case of an RGB image). These LSBs contain the embedded data. Concatenate the extracted LSBs to reconstruct the binary representation of the embedded data. If necessary, perform any additional decoding or processing based on the steganographic method used in Phase-4. This step ensures that the extracted data is in a suitable format for decryption. Validate the integrity of the extracted data by comparing it with the metadata information. Ensure that the extracted data matches the original data embedded in Phase-4. Certainly! Let's delve into Phase-8. Obtain the extracted and possibly decoded data obtained from Phase-7. This data was originally encrypted using the Blowfish algorithm in Phase-1. Retrieve the Blowfish encryption key from the metadata. This key was used to encrypt the original secret message in Phase-1. Use the Blowfish algorithm with the retrieved key to decrypt the extracted data. This involves reversing the encryption process applied in Phase-1. Validate the decrypted data by comparing it with the original secret message. Ensure that the decryption process was successful and that the original message has been accurately recovered. The final output of Phase-8 is the decrypted and extracted secret message. This message should match the original secret message that was initially encrypted and embedded into the cover image.

LSB-based picture steganography requires careful consideration of multiple criteria, such as application kind, security, and performance, when choosing the Blowfish algorithm for data concealing. Blowfish is widely recognized for its safe symmetric key block cypher. With a maximum key size of 448 bits, it is impervious to brute-force attacks. To avoid unwanted retrieval of the hidden data, the security of your steganography approach is crucial. Speed and efficiency are key features of Blowfish's design. Since its encryption and decryption speeds are quick, it is ideal for real-time or resource-constrained applications. Especially when dealing with large image datasets, the effectiveness of the method is critical in steganography. Because Blowfish makes effective key management feasible, steganography programs cannot function without it.





**Figure: Block diagram of Blowfish Algorithm**

Blowfish is the symmetric block cipher algorithm and it encrypts the block data of 64-bits at a time. It follows the Festal network and the working process of this algorithm is divided into two parts.

#### A. Key-expansion

This section will break down the key, which consists of a maximum of 448 bits, into many sub key arrays, totaling 4168 bytes.

#### B. Data-Encryption

We will loop over the network 16 times while encrypting the data. Moreover, there is the key-dependent permutation and the key-and data-dependent substitution in every round. The algorithms do additions on 32-bit words or XORs on such words. Four indexed array data lookup tables must be created for each iteration of this process.

Key Generation:

- Blowfish uses large number of sub keys. These keys are generating earlier to any of the data encryption or the decryption.

- The p-array consists of 18, 32-bit sub keys:

P1,P2,.....,P18

• Four 32-bit S-Boxes consists of 256 entries each:

S1,0, S1,1,..... S1,255

S2,0, S2,1,..... S2,255

S3,0, S3,1,..... S3,255

S4,0, S4,1,..... S4,255

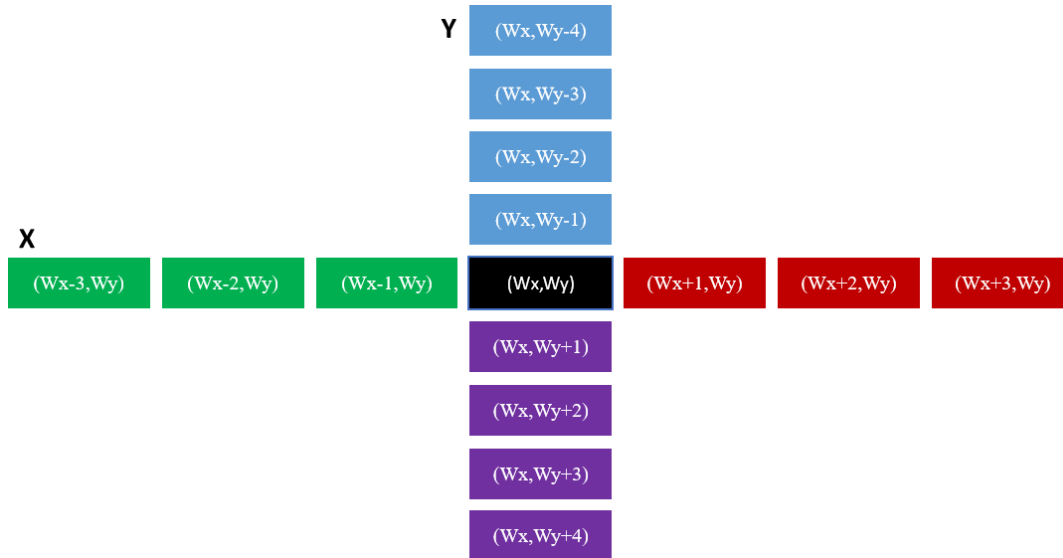
Steps to Generate Sub Keys:

1) Initialize each of the four S-boxes with a fixed string after setting up the P-array initially. Additionally, this string also contains the pi hexadecimal digits (without the first three).

2) Perform an XOR with P1 using the first 32 bits of the key, P2 using the second 32 bits of the key, and so on until all bits of the key (potentially up to P14) are obtained. Until the complete P-array has been XOR with key bits, cycle over the key bits repeatedly. (For example, if A is a 64-bit key, then AA, \AAA, etc., are equivalent keys.) There is at least one equivalent longer key for every short key.

Decryption is exactly the same as encryption, except that P1, P2 ..... P18 are used in the reverse order. [19]

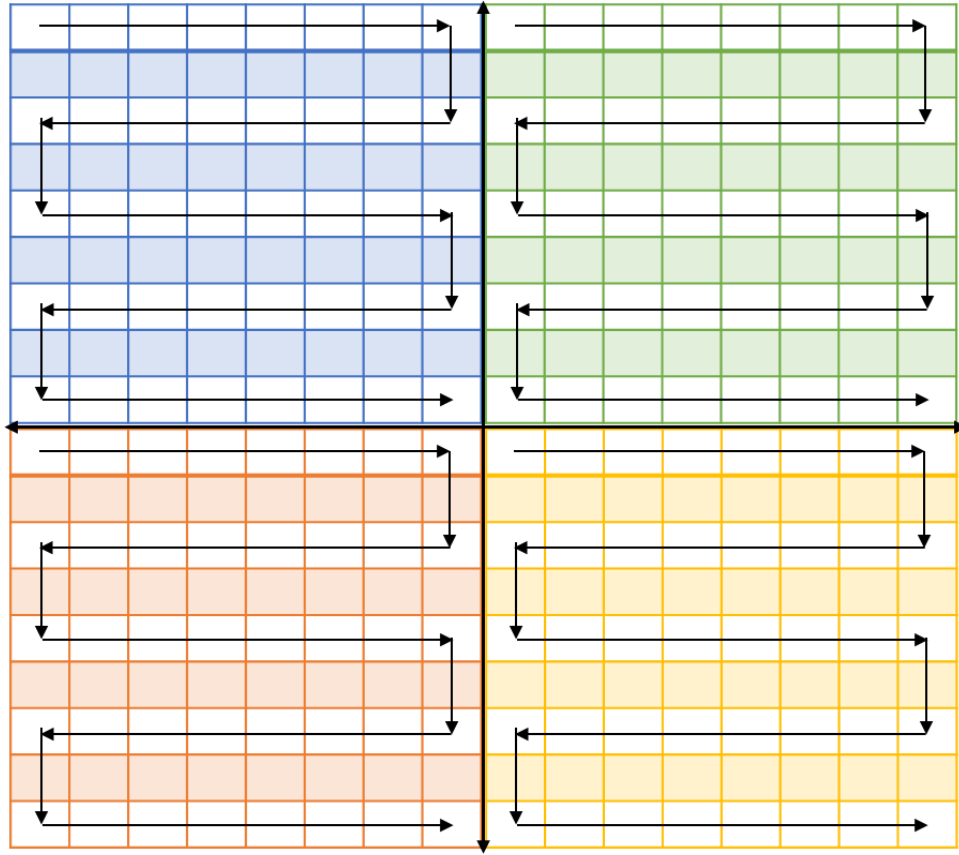
"4 directional Pixel Selection" most likely alludes to a process or methodology that involves choosing or processing pixels in four distinct ways. The cardinal directions—left, right, up, and down—are frequently connected to these directions.



**Figure: 4 Directional Pixel Selection of a Cover Image**

Here's an overview of how this may function: Direction Upward Commence at a particular pixel. Choose or handle pixels that are rising from the origin. In the downward direction, begin at a particular pixel. Choose or handle pixels that are descending from the origin. Starting from a certain pixel, move leftward. Choose or handle pixels that are traveling from the beginning position to the left. In the direction of the right, begin at a particular pixel. Pixels that are going rightward from the beginning location can be chosen or processed.

"Zigzag" usually describes a pattern that alternates between multiple directions, frequently creating a zigzag shape. A "4 directional Zigzag Pixel Selection" technique in computer graphics or image processing could choose pixels in a zigzag pattern in four separate directions. There are four possible directions: left, right, up, and down.



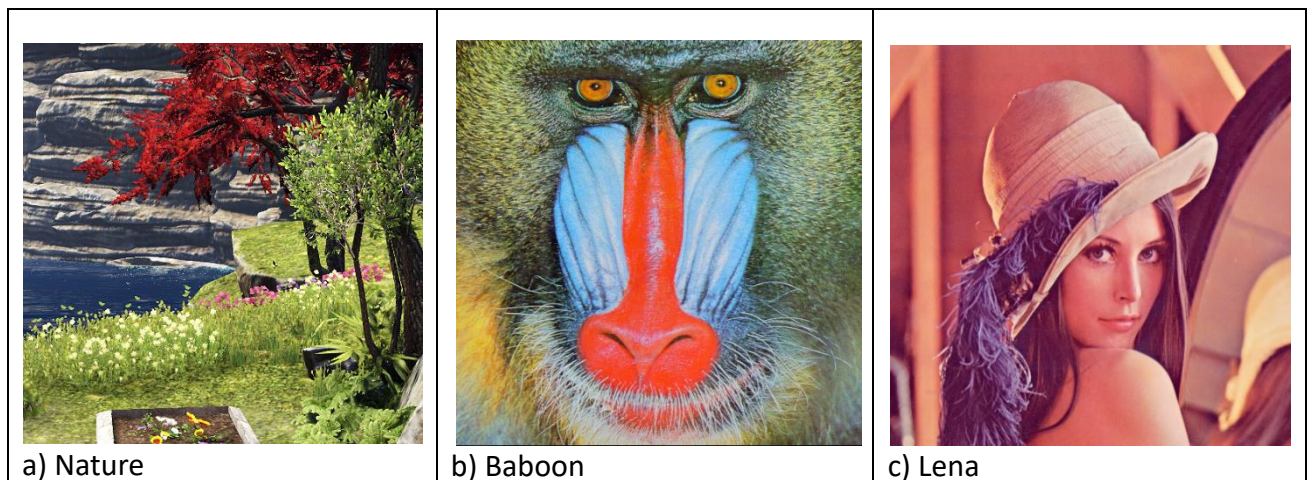
**Figure: Zigzag Pixel Selection of a Cover Image**

Here's a straightforward example: Commence at a particular pixel. Proceed to the right and pick zigzag-patterned pixels. Proceed downwards, picking out zigzag-patterned pixels. Proceed to the left and pick zigzag-patterned pixels. Pick up pixels in a zigzag pattern as you go. This method could be applied to any application where choosing pixels in a certain sequence or pattern is advantageous, including picture reduction and data encoding.

## Chapter-4: Result Analysis and Discussion

In this part, the results are shown in terms of how they look and how they compare to the cover and stego picture. The suggested method's results are also compared with those of other known methods to make sure they work. We used four quality measurement tools for the study's statistical analysis: Mean-Square Error (MSE), Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), and Capacity Ratio (C).

Three pictures, Nature, Baboon and Lena which can be seen on the cover of the figure, were used to test the suggested method. In this case, 512x512 images are used for the analysis because that is the most usual size used in the study. The choice was made because these figures are used a lot in steganography works.



**Fig: Cover image**

The mathematical definition for the given 4 quality measurement matrices (i.e. MSE, RMSE, PSNR and CR) are presented ...

The Mathematical definition for MSE is

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

The mean squared error (MSE) finds the difference between the pixels in the source and stego images. Lower MSE numbers show that imperceptibility has improved.

$a$  = The number of rows of pixels that make up the frame's height.

$b$  = The frame's width, shown as the number of columns of pixels.

$X(i, j)$  = The pixel value of the first frame at  $i^{\text{th}}$  row and  $j^{\text{th}}$  column.

$(i, j)$  = The pixels' brightness in the stego frame at  $i^{\text{th}}$  row and  $j^{\text{th}}$  column

The Mathematical definition for PSNR is

$$\text{PSNR} = 10 \log_{10} \frac{\text{MAX}_X^2}{\text{MSE}}$$

PSNR figures out how good a picture is by comparing the original to a version that has been stretched or distorted. In picture steganography, it is used to figure out how hard it is to tell the difference between the stego image and the original image. The PSNR is found by taking the mean squared error (MSE) and the highest pixel value, which is usually 255 for 8-bit images.

MAX denotes the maximum value that an 8-bit image can have assigned to a pixel (255 (11111111)).

MSE is the mean square error.

A PSNR value exceeding 30 dB signifies increased robustness and imperceptibility.

The Mathematical definition for CAPACITY RATIO is

Capacity Ratio = Number of Embedding Units / Total Number of Units in the Cover Image

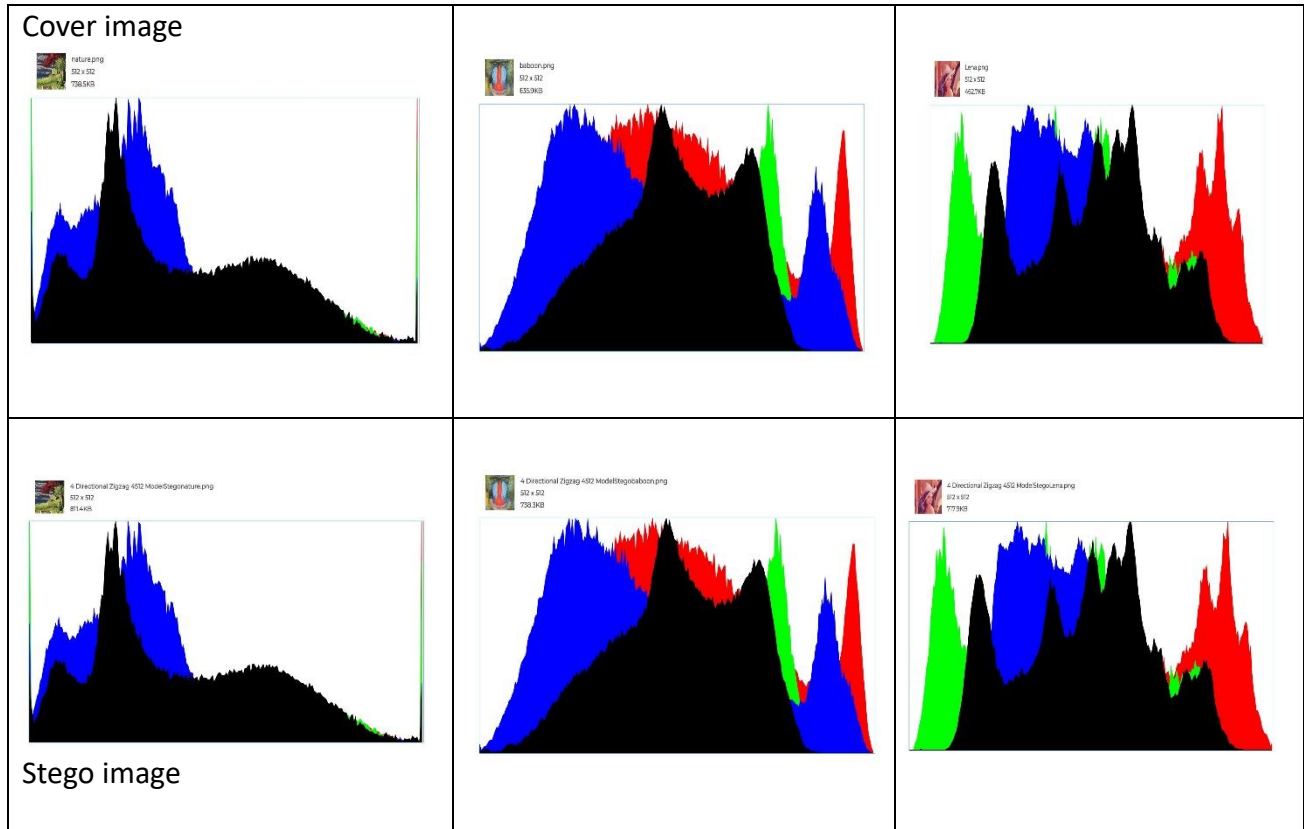
In the given context, "Number of Embedding Units" and "Total Number of Units in the Cover Image" denote the quantity of units (e.g., pixels or blocks) that are accessible for the purpose of concealing information.

Image	Size	Payload	MSE	RMSE	PSNR	CAPACITY RATIO
Nature	512*512	512bytes	0.00767898559570313	0.0876298213834944	69.0277650793092	0.00513203812
		256 bytes	0.00385665893554688	0.0621020042796275	72.0186912722857	0.00260416412
		128 bytes	0.00212860107421875	0.046136764886788	74.5998608388199	0.00130207062
Baboon	512*512	512 bytes	0.0076904296875	0.0876950950025143	69.0212975504608	0.00513203812
		256 bytes	0.00392532348632813	0.0626524020794744	71.9420490805714	0.00260416412
		128 bytes	0.00197982788085938	0.0444952568355255	74.9145292497111	0.00130207062
Lena	512*512	512 bytes	0.00795364379882813	0.0891832035689912	68.875142235098	0.00513203812
		256 bytes	0.00400543212890625	0.0632884833828893	71.8543098374963	0.00260416412
		128 bytes	0.00195693969726563	0.0442373111441646	74.9650291770776	0.00130207062

**Table 2: Metrics for measuring the quality of the suggested method using different standard-sized payloads.**

This table with the dimensions  $512 \times 512$  was used for Nature, Baboon, and Lena, with payload sizes of 512 bytes, 256 bytes, and 128 bytes, respectively. For Nature, the suggested method had MSE values of 0.00767898559570313, 0.00385665893554688, and 0.00212860107421875; for Baboon, they were 0.0076904296875, 0.00392532348632813, and 0.00197982788085938. It was 0.00795364379882813, 0.00400543212890625, and 0.00195693969726563 for Lena in a row. Another important way to judge the quality of a picture is to look at the RMSE. For Nature, the RMSE values were 0.0876298213834944, 0.0621020042796275, and 0.046136764886788. For Baboon, they were 0.0876950950025143, 0.0626524020794744, and 0.0444952568355255, and for Lena, they were 0.0891832035689912, 0.0632884833828893, and 0.0442373111441646. Nature had PSNR values of 69.0277650793092, 72.0186912722857, and 74.5998608388199, while Baboon had values of 69.0212975504608, 71.9420490805714, and 74.9145292497111. The PSNR values for Lena were 68.875142235098, 71.8543098374963, and 74.9650291770776. Another important thing that data embedding in the stego picture is Capacity. The capacity ratios

for Nature were 0.00513203812, 0.00260416412, and 0.00130207062, and for Baboon they were 0.00513203812, 0.00260416412, and 0.00130207062. Lena's each Capacity score was 0.00513203812, 0.00260416412, and 0.00130207062.

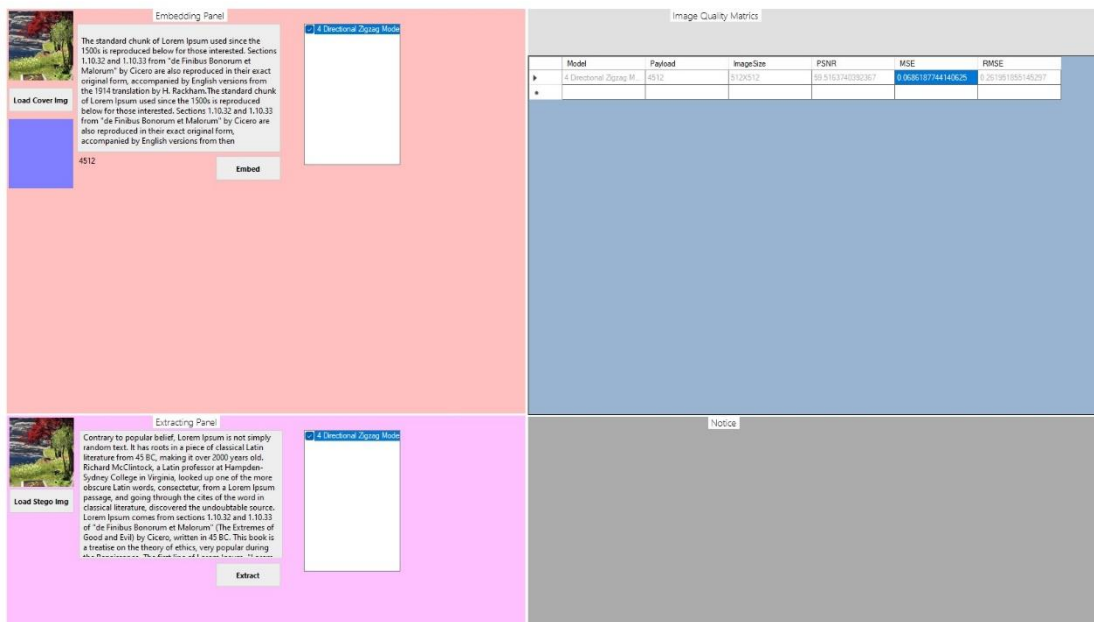


**Figure: A Histogram comparison of the cover and stego pictures**

Take a look at the 512x512 pixel cover images, which are nature.png, baboon.png, lena.png, and Lena.png. After a secret message is inserted into the steganographic and cover histograms, it becomes evident that there is no discernible difference. Histograms visually represent the dispersion of pixel intensities within an image. These visual aids facilitate the understanding of the tonal variations and overall composition of an image. Constraints on the pixel values that introduce discernible fluctuations to the histogram are commonly observed when a secret message or data point is encoded within an image. However, the absence of such distinctions in the comparative analysis gives rise to thought-provoking discussions. The histograms' lack of disparity could potentially be attributed, in part, to the efficacy of the steganographic technique employed. By encapsulating data within a cover medium, such as an image, steganography reduces the visibility



of the concealed data. Advanced steganographic methodologies ensure that alterations performed on the cover image elude both statistical algorithms such as histograms and human visual inspection. Consideration should also be given to the capacity of the cover images to retain the embedded data. Placing additional data behind cover images that feature a wide spectrum of pixel intensities and color variations facilitates the concealment process without significantly impacting the overall histogram. Evidently, the steganographic process effectively maintained the visual integrity of the cover images, as evidenced by the absence of significant fluctuations in the histograms of the stego and cover images. Additionally, it highlights the challenges that individuals encounter when attempting to decipher concealed information using pixel intensity distribution analysis in isolation.



**Figure: Simulation Results using GUI**

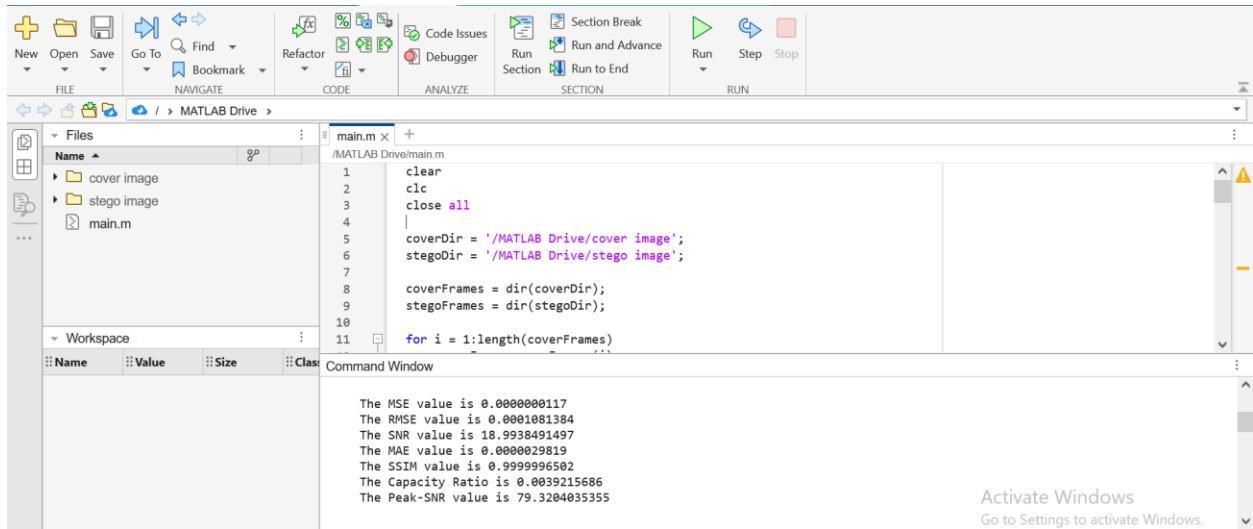
The C# code for our proposed model was implemented using the Visual Studio Code Editor. In essence, this represents the graphical user interface (GUI) of the model we have put forth. We intend to delineate the comprehensive workflow of this model. The model includes an embedding and extracting panel, with PSNR, MSE, and RMSE calculations for our model displayed on the right. We obtain an input box for embedding the secret message in the embedding panel. Here, the Blowfish algorithm is implemented. Diverse online blowfish encryption tools are available for encrypting sensitive data. Using these tools, we encrypt four pieces of data or a message. We then

enter the encrypted data into the input box and select the embed button. Once the cover image has been embedded with the confidential data, it is converted to a steganographic image. The right-hand side of our graphical user interface will display PSNR, MSE, and RMSE calculations when we unexpectedly embed secret data within image pixels. Those values are retrievable from this panel. Our method is implemented on the four steganographic images. The following is a synopsis of the embedding procedure. We shall now discuss the extraction process. In the downstream panel, which is essentially the extraction panel, we will observe that when we load the steganographic images individually and select the extract button, confidential data will become suddenly visible using the proposed model. With the aid of our proposed solution, data will be transmitted in a secure manner over a transmission channel, and a secret message will be extracted.

The implementation procedure incorporated a colored image of Mysore Palace, which measured  $800 \times 600 \times 3$  pixels and was saved in JPEG format. The character count for the secret message is 4054, while the bit count is 28378 bits [31].

From the author's paper [31], they use  $800 \times 600 \times 3$  pixels images and was save in JPEG format. The character count was 4054 as they mention. But my proposed 4 directional pixel selection technique performs better than that solution because we use  $512 \times 512$  pixels PNG format images, and my data capacity is 4512 means I can input 4512 characters for embedding which is more than 4054. So, we can say that our proposed technique can efficiently works better than that solution. Last of all, we can successfully increase the hidden data capacity by using our technique.

We implemented our result in the MATLAB. Here is the overview:



**Figure: MATLAB Code Implementation**

As seen in this figure, we primarily tested the PSNR, MSE, RMSE, and capacity ratio values in MATLAB for the single image baboon.png. We can see that the values for the capacity ratio, PSNR, MSE, and RMSE for this image are, respectively, 79.52, 0.000017, and 0.004. Even looking at the histogram, we can see that there is less of a difference between the cover and Stego image histograms. Our combination model performs exceptionally well, as demonstrated by the figure 3 that shows the results of prior researchers' comparative analysis. In order to improve image imperceptibility, we measure PSNR and MSE. We have excellent capacity for this model because we can embed more data using the suggested technique.

## Chapter-5: Conclusion

In conclusion, the mixture of XOR LSB encoding, the Blowfish algorithm, and the innovative Zigzag Pixel Selection approach presents a robust and sophisticated framework for secure image steganography. The synergy of these techniques not only enhances the embedding capacity but also fortifies the overall security of the steganographic process. The utilization of XOR LSB encoding provides a subtle and imperceptible means of embedding information within the least significant bits of pixel values, ensuring a high level of visual fidelity in the stego images. The integration of the Blowfish algorithm adds an additional layer of encryption, safeguarding the hidden data from potential attacks and ensuring confidentiality. Moreover, the novel Zigzag Pixel Selection approach introduced in this research significantly contributes to optimizing the storage capacity without compromising the visual quality of the cover image. By strategically selecting pixels in a zigzag manner, we achieve a more efficient use of available space, leading to an increased payload capacity for hidden data. The experimental results presented in this thesis validate the effectiveness and superiority of the proposed approach over existing methods. Refine and optimize the Zigzag Pixel Selection algorithm to further minimize the impact on visual quality. Future research can explore alternative pixel selection strategies or hybrid approaches that combine multiple selection algorithms to achieve a balance between increased capacity and imperceptibility.

## References

- [1] N. D. Lynn, A. I. Sourav, and A. J. Santoso, "Implementation of Real-Time Edge Detection Using Canny and Sobel Algorithms," *IOP Conf Ser Mater Sci Eng*, vol. 1096, no. 1, 2021, doi: 10.1088/1757-899x/1096/1/012079.
- [2] D. A. Huffman, "A Method for the Construction of Minimum-Redundancy Codes," *Proceedings of the IRE*, vol. 40, no. 9, 1952, doi: 10.1109/JRPROC.1952.273898.
- [3] A. A. Arab, M. J. B. Rostami, and B. Ghavami, "An image encryption algorithm using the combination of chaotic maps," *Optik (Stuttg)*, vol. 261, 2022, doi: 10.1016/j.ijleo.2022.169122.
- [4] I. Kich, E. B. Ameer, and Y. Taouil, "Image steganography based on edge detection algorithm," in *2018 International Conference on Electronics, Control, Optimization and Computer Science, ICECOCS 2018*, 2018. doi: 10.1109/ICECOCS.2018.8610603.
- [5] 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.
- [6] N. Jain, S. Meshram, and S. Dubey, "Image Steganography Using LSB and Edge – Detection Technique," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 2, no. 3, 2012.
- [7] "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.
- [8] 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.
- [9] H. W. Tseng and H. S. Leng, "A steganographic method based on pixel-value differencing and the perfect square number," *J Appl Math*, vol. 2013, 2013, doi: 10.1155/2013/189706.

- [10] I. Almomani, A. Alkhayer, and W. El-Shafai, "A Crypto-Steganography Approach for Hiding Ransomware within HEVC Streams in Android IoT Devices," *Sensors*, vol. 22, no. 6, 2022, doi: 10.3390/s22062281.
- [11] M. Kalita, T. Tuithung, and S. Majumder, "A New Steganography Method Using Integer Wavelet Transform and Least Significant Bit Substitution," *Computer Journal*, vol. 62, no. 11, 2019, doi: 10.1093/comjnl/bxz014.
- [12] J. J. Roque, "SLSB: Improving the steganographic algorithm LSB," in *Security in Information Systems - Proceedings of the 7th International Workshop on Security in Information Systems - WOSIS 2009 In Conjunction with ICEIS 2009*, 2009. doi: 10.5220/0002169700570066.
- [13] N. A. Kofahi, "An empirical study to compare the performance of some symmetric and asymmetric ciphers," *International Journal of Security and its Applications*, vol. 7, no. 5, 2013, doi: 10.14257/ijisia.2013.7.5.01.
- [14] S. G. Mallat, "A Theory for Multiresolution Signal Decomposition: The Wavelet Representation," *IEEE Trans Pattern Anal Mach Intell*, vol. 11, no. 7, 1989, doi: 10.1109/34.192463.
- [15] F. Marcelloni and M. Vecchio, "A simple algorithm for data compression in wireless sensor networks," *IEEE Communications Letters*, vol. 12, no. 6, 2008, doi: 10.1109/LCOMM.2008.080300.
- [16] R. A. A S and S. Gopalan, "Comparative Analysis of Eight Direction Sobel Edge Detection Algorithm for Brain Tumor MRI Images," in *Procedia Computer Science*, 2022. doi: 10.1016/j.procs.2022.03.063.
- [17] M. A. Saleh, "Image Steganography Techniques - A Review Paper," *IJARCCCE*, vol. 7, no. 9, 2018, doi: 10.17148/ijarccce.2018.7910.
- [18] V. Nagaraj, V. Vijayalakshmi, and G. Zayaraz, "Color Image Steganography based on Pixel Value Modification Method Using Modulus Function," *IERI Procedia*, vol. 4, 2013, doi: 10.1016/j.ieri.2013.11.004.

- [19] X. Zhang and S. Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security," *Pattern Recognit Lett*, vol. 25, no. 3, 2004, doi: 10.1016/j.patrec.2003.10.014.
- [20] C. H. Yang, C. Y. Weng, S. J. Wang, and H. M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, 2008, doi: 10.1109/TIFS.2008.926097.
- [21] W. Luo, F. Huang, and J. Huang, "Edge adaptive image steganography based on lsb matching revisited," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, 2010, doi: 10.1109/TIFS.2010.2041812.
- [22] M. Hussain and M. Hussain, "Information hiding using edge boundaries of objects," *International Journal of Security and its Applications*, vol. 5, no. 3, 2011.
- [23] J. G. Yu, E. J. Yoon, S. H. Shin, and K. Y. Yoo, "A new image steganography based on 2k correction and edge-detection," in *Proceedings - International Conference on Information Technology: New Generations, ITNG 2008*, 2008. doi: 10.1109/ITNG.2008.101.
- [24] V. Singhal, D. Singh, and S. K. Gupta, "A Novel Approach for Enhancement of Blowfish Algorithm by using DES, DCT Methods for Providing, Strong Encryption and Decryption Capabilities," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 7 S, 2023, doi: 10.17762/ijritcc.v11i7s.7008.
- [25] T. Sanida, A. Sideris, and M. Dasygenis, "A Heterogeneous Implementation of the Sobel Edge Detection Filter Using OpenCL," in *2020 9th International Conference on Modern Circuits and Systems Technologies, MOCASST 2020*, 2020. doi: 10.1109/MOCASST49295.2020.9200249.
- [26] H. A. W. Jasim Albayati and S. A. Ali, "A Comparative Study of Image Steganography Based on Edge Detection," in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/1818/1/012032.
- [27] S. K. Salim, M. M. Msallam, and H. I. Olewi, "Hide text in an image using Blowfish algorithm and development of least significant bit technique," *Indonesian Journal of*

- Electrical Engineering and Computer Science*, vol. 29, no. 1, 2023, doi: 10.11591/ijeecs.v29.i1.pp339-347.
- [28] 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.
- [29] R. Tian, G. Sun, X. Liu, and B. Zheng, "Sobel edge detection based on weighted nuclear norm minimization image denoising," *Electronics (Switzerland)*, vol. 10, no. 6, 2021, doi: 10.3390/electronics10060655.
- [30] L. Han, Y. Tian, and Q. Qi, "Research on edge detection algorithm based on improved sobel operator," *MATEC Web of Conferences*, vol. 309, 2020, doi: 10.1051/mateconf/202030903031.
- [31] 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.