AN IMPROVED 4-DIMENSION PIXEL SELECTION METHOD TO ENHANCE CAPACITY IN IMAGE STEGANOGRAPHY

Submitted by

TAYEBA BINTE HAIDER

241-56-019

Department of Software Engineering

Daffodil International University

Supervised by

Dr. S M Hasan Mahmud

Associate Professor

Department of Software Engineering

Daffodil International University

A thesis submitted in partial fulfillment of the requirements for the Degree of Master of Science in Cyber Security.

© All rights Reserved by Daffodil International University

APPROVAL

This thesis titled on "**An Improved 4-Dimension Pixel Selection Method to Enhance Capacity in Image Steganography**", submitted by **Tayeba Binte Haider (ID: 241-56-019)** 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 Master of Science in Cyber Security and approval as to its style and contents.

BOARD OF EXAMINERS

.....

Prof. Dr. A. H. M. Saifullah Sadi
Professor
Director of M. Sc. in Cyber Security
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Chairman

.....

Dr. Marzia Ahmed
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

.....

Dr. Rubaiyat Islam
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 2

.....

Md. Rezaul Islam
CISA

External Examiner

© Daffodil International University

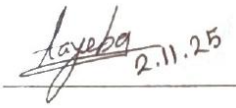
DECLARATION

I, hereby declare that, this thesis report is done by me under the supervision of Mr, Dr. S M Hasan Mahmud, 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 Masters or any degree.

Supervised By

Dr. S M Hasan Mahmud
Associate Professor,
Department of Software Engineering,
Daffodil International University

Submitted By



Tayeba Binte Haider
ID: 241-56-019
Department of Software Engineering,
Daffodil International University

© Daffodil International University

ACKNOWLEDGEMENT

First and foremost, I express my gratitude to the Almighty Allah for bringing me to the completion of this thesis. I wish to indicate my appreciation to my supervisor, Dr. S M Hasan Mahmud, Associate Professor, Department of Software Engineering, for his unflagging support throughout my research work. His supervision has always directed me toward solving my thesis-related queries. Thanks to all my friends, seniors, and juniors who directly or indirectly contributed to this research. Finally, I thank my family, my parents, and all the dear ones who have supported me by all means throughout my life.

© Daffodil International University

ABSTRACT

The use of social media and the internet has been rising and a lot of data is being exchanged as well. Vulnerability increases with the amount of data shared. It is essential and required that shared data be secure and private. Techniques like watermarking and cryptography are employed to ensure security. However, the ciphertext's accessibility instantly raises suspicions and attracts the attention of malicious people. This brings us to yet another technique steganography. The primary goal of steganography is to conceal the existence of secret communication rather than the content of it. Image steganography, which helps protect sensitive information, is similar to concealing secret messages in common photos. As a way to improve data concealment within images, an improved method for image steganography is introduced in this study. There are limits to how much data can be hidden using conventional methods like LSB substitution without sacrificing image quality. A 4-directional pixel selection method is proposed as a solution, methodically embedding data outward from the image center. By incorporating encryption more specifically, the RSA cryptosystem the technique improves data security. As experimental evaluations with Lena, Lake, and pepper images show, the suggested technique is developed by discretely embedding important data while preserving image quality. With its foundation for safely hiding significant amounts of data inside images, this technique offers a potential development in image steganography. Analysis has been used to measure the quality, and the value of the quality assessment matrices has produced improved results and retains a maximum of 1256 bytes of hidden data.

Keywords

Image steganography, Pixel selection technique, RSA, XOR, Least Significant Bit (LSB), RGB

 © Daffodil International University

Table of Contents

APPROVAL i
DECLARATION ii
ACKNOWLEDGEMENT iii
ABSTRACT iv
CHAPTER 1: INTRODUCTION 1
1.1 Background 1
1.2 Beginning of Steganography 2
1.3 History of Digital Steganography 3
1.4 Fundamental Requirements 4
1.4.1 Imperceptibility: 4
1.4.2 Capacity: 5
1.4.3 Robustness: 5
1.5 Reason to select Image as cover 6
1.6 Domains of Image Steganography 7
1.7 Problem Statement 9
1.8 Research Objective 9
1.9 Scope of work 9
1.10 Contribution 11
1.11 Thesis organization 11
CHAPTER 2: LITERATURE REVIEW 12
2.1 Introduction 12
2.2 Spatial domain-based embedding techniques 13
2.3 LSB-based techniques 13
2.4 Literature Review 15
2.5 Research Gap 16
2.6 Summary 17
CHAPTER 3: RESEARCH METHODOLOGY 19
3.1 Introduction 19
3.2 Block Diagram 19
3.3 RSA Encryption Techniques 22
3.4 Proposed Model and Equation 23

© Daffodil International University

3.5 XOR-Based Image Steganographic Techniques 26
3.6 Embed and Retrieve Technique 28
3.7 Embedding and Retrieving Algorithm 30
3.8 Evaluation 32
3.8.1 Equations of Quality Metrics 32
3.8.1.1 Mean-square error (MSE) 32
3.8.1.2 Peak Signal to Noise Ratio (PSNR) 33
3.8.1.3 Capacity Ratio 33
CHAPTER 4: EXPERIMENTS AND RESULTS 34
4.1 Introduction 34
4.2 Test Data 34
4.3 Result 36
4.5 Comparison with Existing Model 37
4.6 Comparative Visual Analysis 38
CHAPTER 5: CONCLUSION 40
REFERECES 41

© Daffodil International University

List of Figures

Figure 1.1: Relationship of cryptography, steganography, and watermarking. 2
Figure 1.2: Simple behavior of steganography 4
Figure 1.3: Basic fundamental requirement of steganography 5
Figure 1.4: Domain of steganography 8
Figure 3.1: Block Diagram of the Proposed Model 21
Figure 3.2: RSA Techniques 22
Figure 3.4: Embedding technique XOR. 27
Figure 3.5: Embedding technique 28
Figure 3.6: Retrieving technique 29

© Daffodil International University

List of Tables

Table 2.1: Literature review. 15

Table 4.1: Cover Image for Proposed Model Implementation. 35

Table 4.2: Quality Measurement Metrices for the Proposed Model. 36

Table 4.3: Quality Measurement Metrics (capacity ratio) 36

Table 4.4: Comparison among techniques. 37

Table 4.5: Comparative analysis between cover image and stego image based on Histogram. 38

© Daffodil International University

CHAPTER 1: INTRODUCTION

1.1 Background

Due to the changes in time, the use of the Internet and social networks has increased and there is also a huge amount of data exchange going on. The more data is exchanged, the more vulnerable it is made. Security and privacy of shared data are necessary and mandatory. To make communication and data secure on the internet, cryptography and steganography techniques are used to ensure high security. Cryptography and steganography are used for secret/hidden writing. In cryptography, it is converting raw information or plain text to unreadable code text. It uses an encryption algorithm with a key. The message must be hidden in a way that makes it meaningless to the unauthorized. The original data are unreadable in this process, so that confidentiality is maintained. However, the availability of the code text raises suspicion and draws the attention of evil people very quickly that something secret is hidden. Here comes another technique called steganography. Steganography is the procedure to hide data to prevent exploration in a regular and regular file or message. It protects data in a way that no one is really able to understand its existence. Steganography does not generate indicators that can be seen by humans, this technique seems more appropriate and has attracted much more attention lately. Steganography's main objective is to mask the existence of secret communication rather than its content. It works because the secret information is embedded in a media that can be any digital content. Another technique is also used to hide data The technique of adding a brand or piece of information to digital signals (such as paper, audio, video, or photos) that can be used to indicate who owns the item, confirming its legitimacy, or providing further information is known as watermarks The protection of intellectual property rights, the discouragement of unlawful use or distribution, and the provision of a way to track the source of content are the main objectives of watermarks. The primary distinction between steganography and watermarks is that it is always invisible while watermarks are sometimes visible.(Dalal & Juneja, 2021; Qin et al., 2019; Shehab & Alhaddad, 2022)

© Daffodil International University

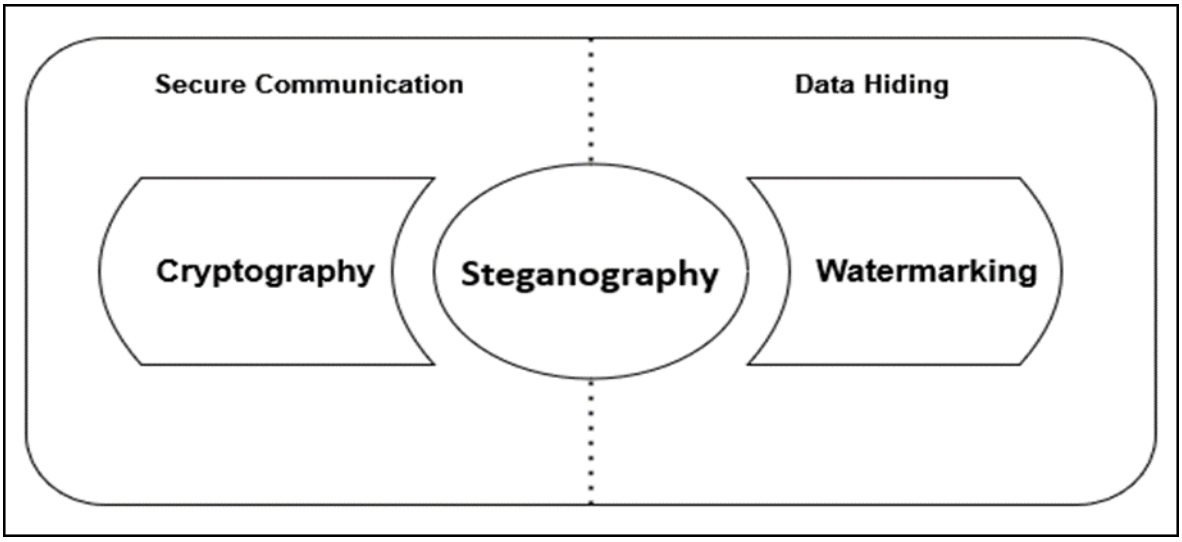


Figure 1.1: Relationship of cryptography, steganography, and watermarking.

The history of steganography extends back thousands of years. People have been concealing messages or information within seemingly innocuous objects or information since ancient times.(Borse et al., 2008)

1.2 Beginning of Steganography

One of the earliest known uses of steganography is from Greek historian Herodotus, who called a technique used by the Greeks in the fifth century BC. During the Persian era, a nobleman named Hittites wanted to contact his supporters. He had shaved the head of a trusted slave, tattooed a message on the slave's scalp, and waited for the hair to grow again before he sent the slave to deliver the message.

Another well-known historical example of steganography is the work of the Roman Empire of invisible ink. Information can be hidden in what seemed to be an empty piece of parchment by using materials to write secret messages that only became apparent when exposed to specific chemicals or heat. Different cultures and civilizations have developed their ways to hide information over time. Examples are placing secret compartments in things, posting messages in artwork, using microdots in times of conflict, or using different linguistic or numerical codes.

(Edmead, 2007; Jamil, 1999; Qin et al., 2019)

© Daffodil International University

1.3 History of Digital Steganography

Digital steganography is a relatively new technology unlike the old tradition of encrypting communication or physical things with information. With the development of computers and digital technologies came the rise and evolution of digital steganography. The early history of digital steganography dates back to the 1980s and 1990s, a time when digital data transmission and computer accessibility increased. Originally, communications were hidden in image and audio files using the least significant bit (LSB) technique, which buries information in audio samples or pixels that are usually undetectable to the human eye or ear. The revolutionary digital steganography method known as F5 was developed in the late 1990s by Westfield and Boltzmann. It focuses on inserting data into JPEG images through manipulation in the quantization tables. In parallel, the S programs allowed the user to hide text in image files effortlessly. However, technology did not standstill; where there was once only audio and photographic files, steganography has grown to include other kinds. It can now be practiced on executable files, multimedia files, and even network protocol implementation. With all of this came some refinements to the algorithms and methods—sophisticated ones, such as those involving spread spectrum techniques, transform domain methods, and those incorporating artificial intelligence and genetic algorithms. Their later 21st-century applications included the less serious cybercrime and espionage uses but also controversial applications like digital watermarking for copyright protection. As evidenced by having undergone further development owing to the infusion from deep neural networks and machine learning, their techniques now appear rather rudimentary in comparison.

© Daffodil International University

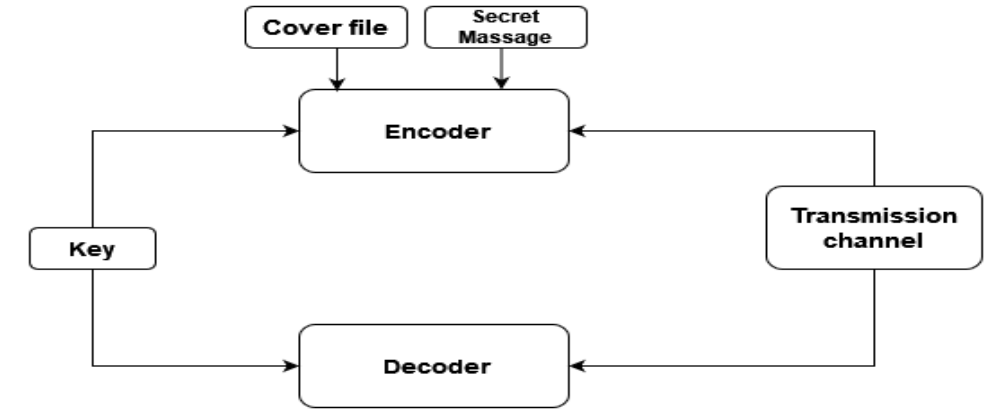


Figure 1.2: Simple behavior of steganography

In the last third of the 20th century, scientific interest was taken in ways of processing text, music, and image data in digital files. The main aim was to conceal colors or hide information in the least meaningful parts of images. In parallel with this, improvements in computing power led to the production of specialized software and techniques that simplified embedding and extracting hidden information from digital files. These developments helped make steganography more accessible to the average user. Digital steganography methodologies have been under development since that time, with researchers looking at new directions such as embedding data into multimedia files and network communication protocols and even machine learning. In other words, within the general theme of cybersecurity, there is a substrate for further research and development in the area of digital steganography. It takes much skill to unearth such hidden information, and even then, only when one possesses specific skills or tools. Among techniques that maintain imperceptibility are changes in frequency domains, hiding information within redundant parts of a file, and embedding in the least significant bit.

1.4 Fundamental Requirements

Three basic characteristics characterize the efficiency and functionality of steganography as a covert communication method in different settings.

1.4.1 Imperceptibility: The embedded data must be concealed from unauthorized observers in order for steganography to function. There shouldn't be any noticeable or audible changes to the

© Daffodil International University

carrier or cover medium (such as a picture, audio file, or video) once the secret data has been added. It is very difficult for anyone else to find out about the existence of hidden information without specific training or tools. Techniques like frequency domain modification, data concealment within redundant parts of a file, and LSB (Least Significant Bit) embedding help to maintain imperceptibility by minimizing observable changes to the carrier file.

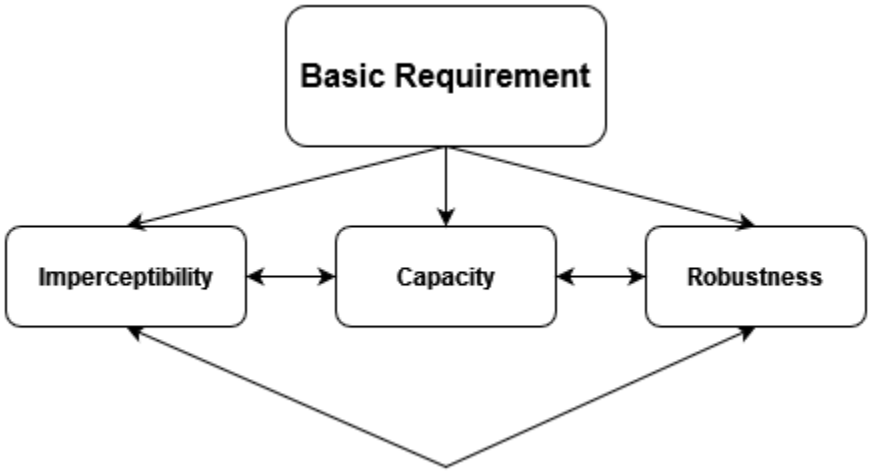


Figure 1.3: Basic fundamental requirement of steganography

1.4.2 Capacity: The capacity is a property that describes how much secret information can be hidden inside the cover. This kind of imperceptibility is always at odds with carrying information. Therefore, it appears that imperceptibility requires less alteration of the carrier file, while capacity allows larger amounts of data to be embedded. High-capacity embedding techniques and using multiple carriers can achieve high-level capacity at the expense of little imperceptibility. However, increased capacity very often implies increased vulnerability to detection.

1.4.3 Robustness: Robustness is the step of the steganographic technique to survive many attacks, manipulations, or modifications of the carrier file without loss of the hidden data. For instance, embedded data must be recoverable from a cover medium that has been cropped, compressed, or even converted to another format. Inversely, flexible steganography methods

© Daffodil International University

apply complex algorithms and redundancy or error correction codes that make hidden data invulnerable to every kind of modification of the carrier file.

1.5 Reason to select Image as cover

Steganography is embedding information inside a carrier in such a way that its existence is undiscovered, and in this regard, digital images become very versatile and efficient media. Photos have numerous advantages over other formats and hence are widely used to carry information in their process of sending secret messages and hiding data.(Liu et al., 2020) In this digital world, the huge use of images makes them important in transmitting secret messages. The growing popularity of digital images across different platforms, applications, and devices makes their use for confidential communication less evident and more easily intercepted in today's connected world. Images are also so common and represent an untypical file type, hence decreasing suspicion whenever trying to send confidential data without inspections.(Duan, Guo, et al., 2020; Subramanian, Cheheb, et al., 2021; Wang et al., 2022) Due to their large size and complex structure, such properties make it possible to hide several amounts of information in an image without the least sacrifice to its aesthetic quality. Because of its large storage capacity, information can be embedded in it with negligible or no perceivable change in the image. (Liao et al., 2022) On the other hand, the degree of imperceptibility has to be optimized such that the data is hidden within the picture; without visible changes, the quality of the image is disturbed, thus making such a process balanced. Due to this peculiarity, modern techniques of steganography exploit the insensitivity of human vision to certain image alterations, thereby embedding data inside images while retaining their original state. Very diverse industries utilize image steganography, indicating the power it generates across different fields. For example, in the domain of cybersecurity, it represents one of the most valuable tools to ensure the safe transmission of data, whereby it would transport several critical pieces of information concealed inside images to outside parties.(Ghoul et al., 2023; Saad et al., 2021; P. Wu et al., 2018)

Furthermore, techniques such as digital watermarking employ visual steganography to encode data and, therefore, seek to prevent unauthorized use or copying of copyrighted material so as to safeguard intellectual property rights. Digital image steganography has been used in digital forensics and, by extension, in law enforcement to enable clandestine information exchange

© Daffodil International University

between investigating agencies, which is an important aspect of the security and resolution of cases. In addition, it provides an effective channel for the anonymous dissemination of information; by hiding crucial photographic evidence, it guarantees the confidentiality and security of individuals making sensitive disclosures, thus playing an important role in journalism and whistleblowing.(Alam et al., 2020; Subramanian, Elharrouss, et al., 2021) Image steganography is indeed very applicable in cases involving the protection of intellectual property, anonymity, law enforcement, and modern communication. Hence, it is powerful and very useful in many industries and uses where stealthy communication is required because it is very easy to embed information within images and covertly transfer information given the innate characteristics and omnipresence of images. The embedding carrier used in our research is images which has been used by many other researchers. (Kadhim et al., 2019; Sahu & Sahu, 2020; Setiadi, 2021, 2022) (Hussain et al., 2018; Shah & Bichkar, 2021; Tayyeh & Al-Jumaili, 2022)

1.6 Domains of Image Steganography

Based on the methods and strategies used for encrypting images, image steganography is classified into several categories. Spatial domain techniques embed data in pixel values without significant changes to the appearance of the images. The least significant bit (LSB) insertion is one of the earliest techniques used to achieve this. Frequency domain techniques, such as Discrete Fourier Transform and Discrete Cosine Transform, embed information in the frequency coefficients after the altered image data has been transformed. Transform domain techniques modify image transforms, such as wavelet or curvelet transforms, to enable more efficient data hiding in image subbands. Finally, hybrid systems combine several methods to enhance the security and capability of data hiding within images, sometimes even achieving a balance between the imperceptibility and resilience of the hidden information. These categories provide a range of techniques for concealing information in images, each with special benefits and drawbacks concerning robustness, imperceptibility, and attack resistance.

© Daffodil International University

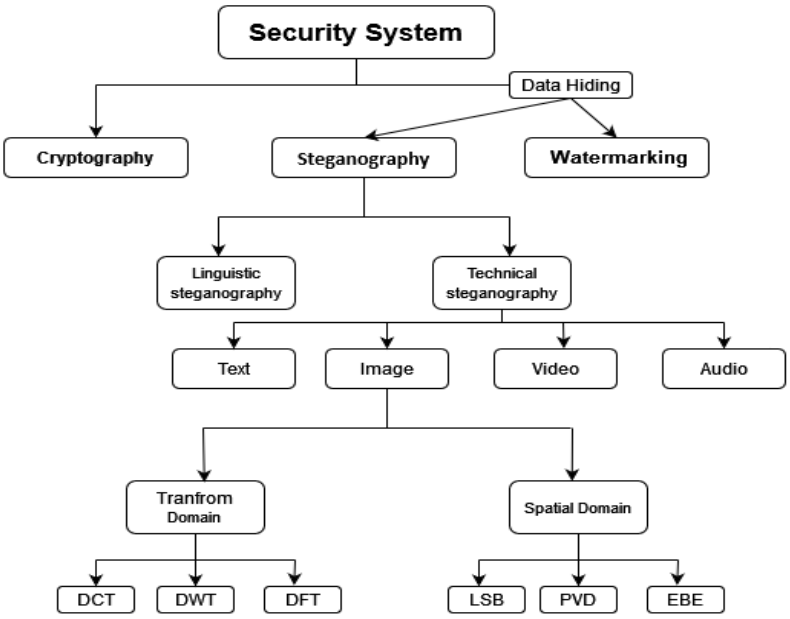


Figure 1.4: Domain of steganography

This study examines LSB-based visual steganography. LSB-based picture steganography alters the least significant portions of image pixels in order to embed secret data. Because human vision is less sensitive to changes in the least important parts, changes in these parts are often visually indistinguishable, maintaining the quality of the cover image. In the divided cover image, the least important parts of selected pixels are replaced with the hidden message. This technique removes a lot of information from an image without causing noticeable distortion. LSB embedding is the simplest and most popular method among researchers because it carries less useful information and permits embedding without causing perceptual distortion.(Dalal & Juneja, 2021) Additionally, in order to increase payload capacity, information can be concealed by using multiple LSBs of a pixel; however, this may degrade the visual quality of the stego image.(Chan & Cheng, 2004) The previous study's techniques followed odd and erratic pixel patterns, which made data recovery challenging for the recipient. The lack of a distinct pattern complicates the extraction process, requiring the recipient to be aware of the exact technique or embedding key. (Ehsan Ali et al., 2021) In contrast, even though a sequential pattern is relatively easy for the recipient to identify, it raises concerns about the security of the hidden information. Steganalysis or statistical analysis would easily detect it since it follows a pre-determined route or phase within the image. If enemies use this predictability for a faster identification of the embedded data; this will result in leaking

© Daffodil International University

the secret message. The key problem is that conventional and chaotic pixel area selection can reveal stego images.

1.7 Problem Statement

Security challenges of steganographic techniques facing as attackers becoming more adept. Recent advances in steganalysis make it possible to decode hidden messages in pictures. These deep neural networks are being used in sophisticated machine learning. Statistical techniques help to find small changes or errors made to any product or data. (Fu et al., 2020)

PS-1: This refers to the data quantity that can be hidden and the carrier medium's protection. Compromises are often made to maintain original look or quality. It becomes more difficult to embed or hide more information within a medium without changing its original appearance, which could make the hidden data easier to find. (Kordov & Zhelezov, 2021)

PS-2: Another problem is Imperceptibility and capacity frequently have an inversely proportional connection, which means that imperceptibility tends to increase as capacity decrease that create a problem capacity low. (Maji et al., 2021) (Setyono & Ignatius Moses Setiadi, 2019)

1.8 Research Objective

The proposed model's primary goal is to solve the issues that were previously discussed. The core objective is:

OBJ 1→ To embed data in an organized manner with a sample retrieval process. (PS-1)

OBJ 2→ To improve capacity with maintainable imperceptibility. (PS-2)

1.9 Scope of work

Ensemble steganography is a powerful sor of combining stenography and cryptography. It uses the strengths of both fields to enhance embedded information security. This combination the strength of cryptography is used in this technology to provide robust encryption abilities. Hiding data using steganography inside some cover medium. Combining the two methods allows ensemble. Applying steganography to encrypt the concealed information not only complements its hiding but also enhances the security posture of data embedding. A multilayered security

© Daffodil International University

paradigm is formed by steganography and cryptography. Steganography is the aspect where hidden stego data is embedded inside some medium, while cryptography encrypts the secret message that only those authorized can understand. Thus, a two-layer protection approach is developed, increasing the complexity of resisting threats from hackers trying to access or uncover any of the secret data. Besides, the individual weaknesses can only be exploited when the ensemble then is subjected to steganographic or cryptographic methods. Combined methods thus eliminate weaknesses that may exist in either, hence, when statistical analysis could have been applied to steganography, some specific attacks were to test some cryptographic methods. If properly applied, the hidden and encrypted data is well protected against discovery and decryption. That is to say, Steganography and Cryptography are like two walls of a castle, standing side by side and impervious to intrusion. Therefore, the ensemble approach generally gives added security, confidentiality, and integrity. The exposed data is similarly retained unto any hidden source from being uncovered and decoded. Especially when one does not want the strengths and weaknesses of either method to be presented either alone or in combination, ensemble steganography overcomes such deficiencies. Steganography is followed by cryptography and vice versa. Individual approaches entail apparent disclosure through steganography when the embedded information is extracted, while cryptography yields the opposite effect. Several other undesirable results emanate when the single technique is used. By this technique, however, the level of assurance he requires is said to attain it by overlapping. Several studies have proportionally placed their emphasis on the fact that cryptography is first followed by steganography to arrive at the same result regardless of the order of execution; only the order of application differentiates cryptographic techniques. The protection against detection reduces; however, it becomes necessarily dependent upon how robust the cryptography, steganography, and cover medium used are.Currently, implementing digital steganography in various areas has been done quite cutting-edge, from marketing to security and academic. paper For example: It applies in digital media watermarking and, by doing so, secures evidence, copyright, and similar issues; online advertisement-oriented text, image, and video manipulation; and e-learning providing online material using web pages and taking online examinations. These examples discuss implementing steganography in many socially relevant matters. However, they have many relations to other aspects of society. However, in other areas of social life, implementing such technology has also been evidenced.Combining the two approaches lessens the potential for individual flaws, even

 © Daffodil International University

though steganography could be detected by statistical analysis and cryptography could be the subject of attacks that target encryption techniques. When integrated skillfully, the hidden and encrypted data becomes increasingly resistant to being found and cracked. Steganography and cryptography work together to create a powerful method that is perfect for protecting sensitive information and sensitive communication. Better security, confidentiality, and integrity are offered by this combination technique, which also ensures that the conveyed data will stay confidential even in the unlikely event that the hidden information is found and decrypted. Cryptography and ensemble steganography Cryptography and steganography can be used together to increase embedded security. (Dalal & Juneja, 2021) Although not much research has been done on this, more must be done.

1.10 Contribution

Through capacity enhancement, the suggested method marks a significant advancement in steganographic procedures. This work presents an improved method for image steganography: the 4-Dimension Pixel Selection Method, which is specifically designed to increase the image's ability to conceal data. This is utilized by the method to significantly boost the data-hiding ability of photos. By effectively utilizing image redundancies in various dimensions, the approach can conceal a greater amount of information without sacrificing visual quality or creating noticeable abnormalities.

- Focus on capacity enhancement.
- Maintainable imperceptibility.

1.11 Thesis organization

The first chapter of the thesis acts as an introduction, establishing the background and goals. An in-depth discussion of the literature, including current theories and research, is covered in Chapter 2. The methodology is described in Chapter 3, the results and discussions will be presented in Chapter 4, and the study's conclusions are presented in Chapter 5. All of this will be backed up by a reference section in Chapter 6 that lists the materials and sources that were used in the research.

© Daffodil International University

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

A Classical steganography is based on the premise that a carrier medium, such as an image, is necessary to hide data or information within. However, this notion leads to various methods of hiding information, especially in images. Based on current technological advancements and modern techniques, one of the most widely accepted methods involves several classification dimensions based on their characteristics, compression, spatial, and transform domains. A reversible process can return the carrier medium to its original state without any distortion, while an irreversible process cannot. In the view of classical techniques, the process involved was reversible. That is, any information embedded within the original medium can export without trace or distortion of the added cover of the medium. This has been defined over the years as a key area of the steganographic process; it is instrumental in ensuring confidentiality regarding embedded data. Noteworthy in this regard, information relating to anything personally sensitive has involved a rising number of applications in this specific field, but it might not necessarily be easily related to images. In other words, it is a modern computer vision technique employing knowledge of image processing and multimedia systems, which finally serves the purpose of data hiding or steganography.(Abikoye & Ogundokun, 2021; Chefranov & Oz, 2022; Jebur et al., 2023)

This becomes very significant whenever the cover image undergoes the process of losing its integral visual characteristics. Reversible methods can achieve accurate recovery without loss or distortion of cover images. For instance, replacement of LSB in formats of raw or uncompressed data is such a technique. Another aspect of detection is explained by the classification based on compression. Uncompressed or raw data formats, that is, in the spatial domain, display the image in its original pixel format. (Kuyoro et al., 2022) The benefit of reversible steganographic techniques regarding this issue is that they are applied directly to raw pixel data, allowing for accurate embedding and extraction of hidden information. The integrity of the original image in the uncompressed domain makes it an excellent option for reversible techniques due to smooth extraction and concealment processes.(Ghoul et al., 2023; Mahmoud & Elshoush, 2022; Rustad et al., 2022) We will also call it the "spatial domain" in our work, referring to the original uncompressed domain or the pixel data format. For the sake of consistency and clarity, the terms are sometimes used interchangeably. This intentional choice stresses that reversible technique

© Daffodil International University

matters are the dominant markets where, in case any image is modified, there always exists a difference between modified and original image formats. Many researchers have used reversible techniques, which involve accurate recovery for the case when cover video remains unchanged without any visual distortion, while secret data gets extracted. (Song et al., 2015)

2.2 Spatial domain-based embedding techniques

Working directly with raw data or managing pixel values is referred to as "spatial domain."(Hussain et al., 2018) LSB (Least Significant Bit) substitution is the most basic technique for embedding in the spatial domain. In the spatial domain, image steganography requires direct embedding to the image's pixel intensity values. (X. Wu et al., 2022) To encode the secret data bit in LSB, the least significant parts of cover videos are swapped out; other researchers have also employed LSB replacement. (Bhattacharyya et al., 2010) An LSB's robustness and data-hiding capabilities are limited, despite the fact that replacing one is simple and quick. Because the changes in the least significant bits are predictable and statistically noticeable, embedded data using LSB replacement is vulnerable to a variety of attacks and steganalysis techniques. Despite its shortcomings, LSB substitution is still a crucial method in spatial domain steganography because it can be used as a standard to evaluate and compare more intricate or sophisticated embedding strategies. The methods that are described in this section have been used in a number of studies.

2.3 LSB-based techniques

While LSB (Least Significant Bit) embedding has so far gained widespread recognition for hiding small data within digital images, it is, however, suitable for use in steganography within other digital mediums. The core technique, which images pixels also undergo, comprises modifications made to their least significant parts of data representation. Subsequently, optimal balancing between data capacity and perceptual distortion permits broadening LSB embedding beyond picture steganography. A method particularly important in its applying is the embedding of information without, in any substantial way, compromising the perceptual qualities of the carrier medium. Since the LSB modifications are imperceptible, the impact on the integrity of the original data is minimal. This method is preferred by researchers and professionals from a variety of areas because it can covertly add information but still preserve the original content's integrity. (Al Maki et al., 2023; Degadwala et al., 2024; Mohamed et al., 2023; Because it can discreetly add

© Daffodil International University

information while preserving the original material's integrity, researchers and practitioners across a range of fields prefer this approach.(Abood et al., 2022; Celik et al., 2005; Chan & Cheng, 2004; Moore et al., 1999)

The ability to embed LSB (Least Significant Bit) is a key factor that affects how well hidden information is protected in digital media, especially in the areas of data hiding and steganography. It tells you how much secret information can be added to a digital cover media without changing its quality too much or making people think it has been tampered with. (M. Khan & Rasheed, 2023; A. Yang et al., 2023; J. Yang et al., 2023) Capacity is crucial because it is correlated with the number of LSBs that can be slightly altered without affecting the auditory fidelity or authenticity of the host medium, which could be an image, audio file, or other digital content.

A number of variables unique to the cover material and the intended level of concealment affect capacity. By showing how many bits are used to represent each pixel's color or grayscale value, the bit depth of an image establishes its potential capacity. Depending on the image's resolution, altering the least significant bit in an 8-bit image can conceal one bit of data per pixel, which changes the overall capacity. (Cheddad, Condell, Curran, & Mc Kevitt, 2010; Duan, Gou, et al., 2020) It involves a scale of balancing the degree of data invisibility against that of perceptual distortion. The more LSBs used, in principle, increases the hidden bits, which causes an increased probability of observable changes that tend to be deleterious to the integrity of the audibility or visibility of the embedding. In that respect, it is important to find an acceptable compromise between maximizing the amount of information concealed and ensuring convincing the cover medium's integrity since exceeding imperceptibility limits may compromise hidden data's concealment. The capacity for LSB embedding thus represents and limits the capability for hiding information, providing a context in which due care and precision become essential for embedding information securely into digital carriers.(Duan, Nao, et al., 2020) It acts as a basic guideline for the skill of striking a balance between the ability to conceal information and the imperceptibility of changes, making sure that the hidden data is safe, secure, and undetectable to adversaries or uninvited recipients in the digital environment. Here is an example of embedding any letter "M" with ASCII (American Standard Code for Information Interchange) code 77 in decimal and "1001101" in binary, for instance, each pixel in a 24-bit color frame will have 8 bits. The letter

© Daffodil International University

"M" is required in the 24-bit block of three pixels. Considering these three successive pixels: 00101000 10010010 00101010 01000101 11110000 10110110 01100101 10001111.

When "1001101" is embedded, some pixels will change. The altered pixels are 10001111 00101010 01000100 00101001 10010011 11110000 10110111 01100101.(Dalal & Juneja, 2021; Rahman et al., 2022)

2.4 Literature Review

Table 2.1: Literature review.

Author	**Paper**	**Techniques**	**Average Capacity**	**PSNR**	**Limitation**
SOLAK & ALTINIŞIK, 2019	New Approach for Steganography: Bit Shifting Operation of Encrypted Data in LSB (SED-LSB)	LSB	N/A	51.63	Not robust
Setyono & Ignatius Moses Setiadi, 2019	Securing and Hiding Secret Messages in Image using XOR Transposition Encryption and LSB Method	LSB & XOR	518.4 KB	63.236 : 57.132	Low capacity, Less robust
Abdel-Aziz et al., 2021	Improved data hiding method for securing color images	MSB	2-bit/8-bit	77.16: 53.68	Computational complexity, Less imperceptible
Maji et al., 2021	Cover independent image steganography in spatial domain using higher order pixel bits	XOR	90%	57.475 :51.629	Use of public key to exchange

© Daffodil International University

Rahman et al., 2020	A Novel Approach of Image Steganography for Secure Communication Based on LSB Substitution Technique	LSB	60%	38.322 : 41.695	Not imperceptible
Alam et al., 2020	A New 8 Directional Pixel Selection Technique of LSB-Based Image Steganography	LSB8 directional Pixel selection	maximum 765 bytes	76	Hides only 512x512 image
Kordov & Zhelezov, 2021	Steganography in color images with random order of pixel selection and encrypted text message embedding	LSB	16,000 bits	69.1: 82.73	Low Capacity

This section presents an overview of previous works on LSB image steganography. The authors who have used LSB-based steganography on images for secret message embedding are cited. This brings about the following merits: LSB greatly improves the quality of image steganography, increasing imperceptibility with rising PSNR and MSE. The largest obstacle to using LSB methods lies within the size and payload of hidden data. (Huang et al., 2019) Advantages: Advanced defense against intrusion. Data transmission is securely recommended. Used for protecting personal data and image copyrights. Disadvantages: Difficult for third parties to extract embedded information. (Aslam et al., 2022; Molato et al., 2022) Advantages: LSB can generate an invisible stego image resistant to statistical attacks. Disadvantages: Since the algorithm itself is simple, it can easily be broken down by an adversary. According to (Suresh & Kamalakannan, 2022), the proposed method provides fairly good quality and strong security.

2.5 Research Gap

Research gaps in steganography and data concealment must be addressed to improve the efficacy and security of the field. The simple hiding of data in digital media suffers greatly by these gaps, especially the ones related to lack of capacity.(Setyono & Ignatius Moses Setiadi, 2019) However, there are promising solutions that have the potential to revolutionize the field of data concealment

© Daffodil International University

techniques.Poor capacity in data hiding strategies has been the main focus of research for a long time.(Kordov & Zhelezov, 2021) To surpass this challenge, traditional embedding algorithms need to be reimagined. Indeed, the data storage capability with digital cover media can massively scale due to the ever-increasing complexity of creating an embedding algorithm. Traditionally, such enhanced algorithms have aimed to increase hidden data while minimizing perceptual distortion by maximizing the use of LSBs. Any such modification results in a thin line between maintaining perceived integrity of the digital cover media and increasing data capacity. (SOLAK & ALTINIŞIK, 2019) The very second main limitation, besides pixel selection in guaranteeing secure and efficient data concealment, is the orderliness in pixel selection. So far, pixel selection has proved to be one of the most promising trends. The recent pixel selection involves methods that have developed a sensitivity for detection concerning the amount of data visible. Therefore, careful selection and alteration of pixels allow for increased data security. By making sophisticated pixel selection modules part of data concealment, resilience and performance may be increased several times over. Another positive way through which the secrecy of data is assured involves the application of cryptography in all communication pertaining to the embedding or covering media. This added layer of security first encrypts the hidden data using different cryptographic methods, making it inaccessible or even intercept by any third party.

2.6 Summary

A three-dimensional, in-depth thinking process is now required to break through such traditional barriers and fill the gaping chasms of open research in data hiding and steganography. Low capacity and poor pixel selection techniques form practical roadblocks for introducing and securing private information in digital contexts. All these have relative promise; however, success depends on the art of merging sophisticated techniques and elaborate algorithms. Therefore, an increase in the embedding algorithms' understanding and application associated with the fundamental problem involves insufficient capacity within data hiding techniques. There is also a requirement for the development and application of embedding techniques. Algorithms for increasing the capacity of digital cover media for hiding data are relevant, with maximal participation of least significant bits. Therefore, optimization in embedding balances an increase in data volume against perceptual degradation of the cover medium. To this end, improper pixel selection methods have been found to provide the simplest solutions. Because of advanced and strategically planned pixel selection methods, the future looks bright. Enhanced by advanced

© Daffodil International University

algorithms, these purposely look for and change pixels to embed data, improving security and making detection challenging. Incredibly pixel selection procedures could completely modify the transference and value of data concealment techniques. Indeed, a very promising way of enhancing data secrecy is the encryption of messages before their embedding through careful integration of cryptographic encryption methods. This practically enhances the security architecture by embedding the information against unauthorized access or interception. Indeed, such an approach at an overall strategy has covered several research gaps, including pixel-selecting methods, embedding algorithms, and cryptographic encryption techniques. Indeed, such an overall strategy would bring methods far beyond what may be understood of their current horizon to a brand-new era of secret data techniques. These methods have, indeed, made far potential groundbreaking implications for how covert communications typically occur, especially in embedding data, strengthening process security, and further contributing to innovative implications in information security. From the perspective of research into hiding data, there exists an attractive future for its researchers and practitioners in the name of security, creativity, and effectiveness, which almost equidistantly sounds par excellence.

© Daffodil International University

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

Image steganography is a primary method in the spatial domain, hidden behind the practice of embedding secret or confidential information into digital images. The embedded data into an image using this technique is derived from a change in pixel intensities, yet it imparted no significant change in the image's overt appearance. Other than LSB substitution, which is relatively simple and quite effective, many techniques exist within spatial domain steganography. The main intention of LSB substitution is to embed secret information in the cover image while concealing the image's visual likeness by altering the least significant pixel values. The popularity of LSB substitution comes from its simplicity and efficiency in hiding information without significantly affecting the visual quality of the images. Through substitution of the least significant bits by portions of the secret message, data is covertly embedded into the image, and the information becomes practically invisible to the naked eye. The LSB substitution method has been widely studied and applied by researchers and information security practitioners as a general approach to embedding private data within digital images. Indeed, the characteristic that makes the LSB substitution method pragmatically useful and attractive is that it can keep the contained data private while maintaining the integrity and aesthetic quality of the cover image. Since human visual perception is relatively insensible to even considerable changes in the least significant bits of a pixel's value, modifications attained through the LSB substitution process are easily overlooked. Based on this condition, the LSB substitution method allows data hiding and secure communication by embedding relatively small secret information amounts into the host digital image. Although this technique is simple, it has several drawbacks, among which the limitation of embedding a large volume of information into images stands out. It limits embedding information without compromising the quality of the images since it modifies only the least significant part of the image.

3.2 Block Diagram

Encryption is a basic answer to security, one where plaintext data is converted into ciphertext using complex, algorithmic-based formulas to protect sensitive data. This process involves various

© Daffodil International University

mathematical computations and keys needed to make the data readable only to authorized people or systems. Encryption techniques include hash functions, several cryptographic protocols, symmetric, and asymmetric encryption, among others. The method of encryption best used would then depend on the type of data one wants to protect and its bearing concerning security. Choosing an appropriate image in steganography is critical. It must be neither too simple nor too complicated for the modification due to hidden information to be undetectable. Data embedding capabilities depend on parameters such as format, resolution, and color-depth image. Candidate selection methods are statistical analysis-based; therefore, the selected image should be capable of hiding data with a minimum degradation in visual quality. This involves finding specific areas in the selected image where data will be hidden. Choosing an appropriate image in steganography is critical. It must be neither too simple nor too complicated for the modification due to hidden information to be undetectable. Data embedding abilities necessarily involve factors such as the image format, resolution, and color depth. Candidate selection methods based on statistical analysis will thus find an image capable of hiding data with minimal degradation in visual quality. This will, however, get to find specific areas in the selected image where data will be hidden. Geographically, pixel selection can be done on the domain techniques basis, on the pixel intensity features, color channels, and location.

Advanced algorithms can, of course, use region-based or adaptive pixel selection techniques to minimize visual effects while maximizing capacity for data. Algorithms also consider human vision models, which guarantee imperceptibility. There are several ways of data embedding; mostly, they depend on what visual components are selected. LSB-based methods modify the least significant bits of the pixels to contain data, while transform domain methods—singularly, the DCT—modifies frequency coefficients. The spread spectrum techniques embed the information within the spectrum of the images so mildly that it cannot be detected. All these methods aim to

© Daffodil International University

achieve statistical insignificance concerning the inherent complexities of the images or noise.

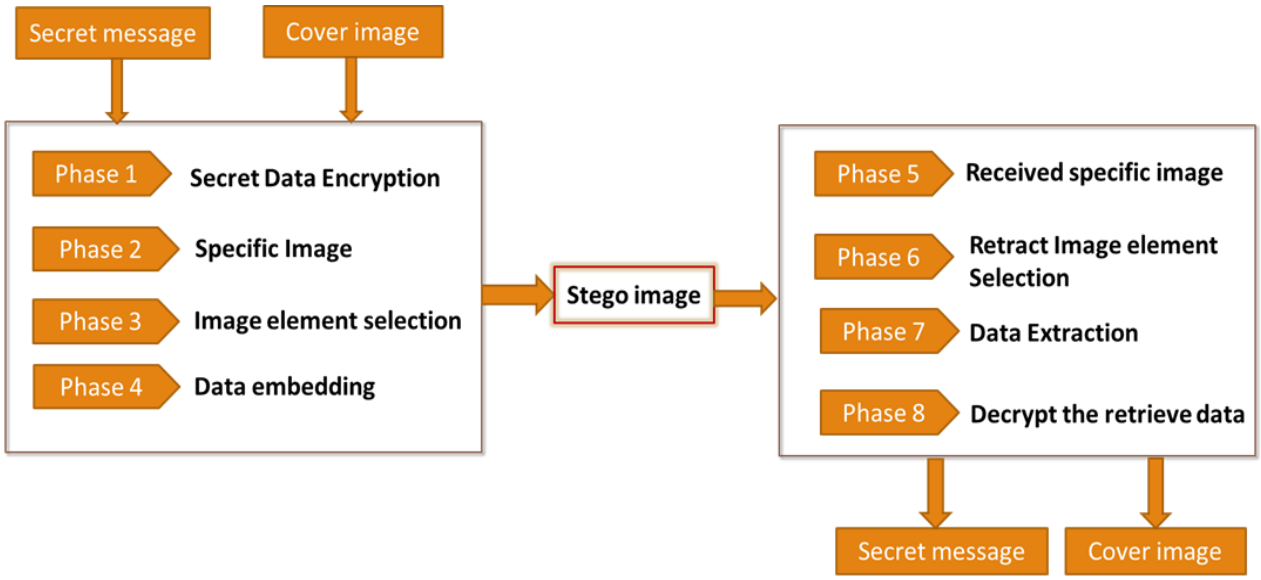


Figure 3.1: Block Diagram of the Proposed Model

The image after data embedding looks similar to the one in which data has been embedded. During this phase, the changes made while embedding data have to be ensured that they are well imperceptible to the human eye. This phase involves statistical analysis, allowing the altered image to be visually valid while having hidden data. This is followed by a change in the location of the altered image, which serves to search well for the efficient method of data extraction. Knowledge of the altered areas in the image is important and thus easily provided by reverse engineering based on the embedding procedure. For accurate detection and designation of these areas for data extraction, sophisticated algorithms and statistical analysis are performed. The extraction procedure is executed by reversing data embedding starting from its embedding phase. Robust algorithms that can recognize and extract the concealed information from the carrier image are necessary to precisely isolate the embedded data from the image without any loss or distortion. Reversing the encryption that was applied to the data before embedding is necessary to decrypt the data that was recovered. By using particular keys or algorithms, the decryption process restores the retrieved ciphertext to its original plaintext form, making it once more comprehensible and functional.ss

© Daffodil International University

3.3 RSA Encryption Techniques

Strong encryption technology For the most part, RSA has endured. In part, the difficulty of factoring large integers serves as the foundation for the security of RSA, a public-key cryptosystem that permits "digital signatures" and secure communications. Even though the authors invite anyone to try, whether or not they used factorization techniques, no one seems to have been able to crack their code.(Rivest et al., 1978) This has successfully certified RSA and will maintain its security guarantee for as long as it is resistant to these kinds of hacks. (Jain et al., 2016)

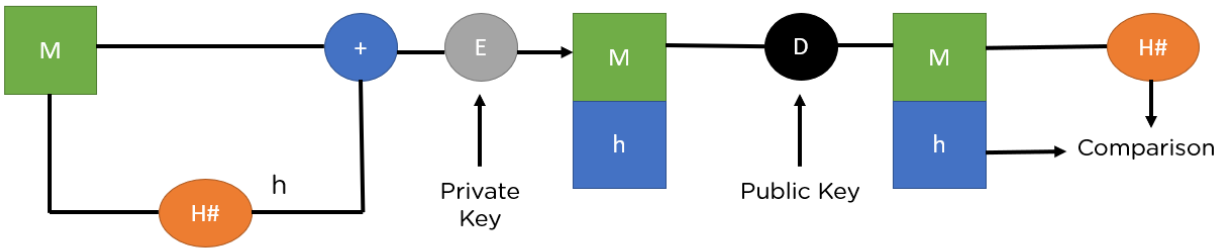


Figure 3.2: RSA Techniques.

A public key and a private key are used in RSA. Mathematically, these keys are connected. While the private key is kept private and used for decryption, the public key is used for encryption and made public. The first step in a key generation is to choose two big prime numbers, p and q. Since n is a part of both the private and public keys, someone could derive it from their product: n = p × q. Then, to find φ(n), where φ is Euler's totient function, one calculates it as φ(p - 1)(q - 1). Next, an integer 'e' must be chosen such that 1 < e < φ(n) and e is coprime with φ(n). e is known as the public exponent. For the private exponent 'd', compute the modular multiplicative inverse of 'e' modulo φ(n). "d" is not made public. The sender encrypts the message 'M' using the receiver's public key. It should be noted that "M" is an integer that has to be smaller than n. The ciphertext 'C' can be computed using the formula C ≡ M^e (mod n). It implies that the letter "C" is the encrypted message that only the intended recipient can receive securely. The ciphertext 'C' is decrypted using the private key of the recipient. The original 'M' is multiplied by n. From the decrypted ciphertext 'C,' the recipient obtains the original message "M." The RSA algorithm relies on the security of factoring large composite numbers formed by two prime numbers. Factoring the product of two large prime integers to crack RSA encryption is computationally impossible for big

© Daffodil International University

enough keys. The basis for RSA's security is the complexity of the RSA problem, which involves performing mathematical operations that are believed to be one-way functions. How secure RSA is depends on the size of the keys used. Longer key lengths offer more protection against brute-force attacks. Strong pseudo-random number generators are necessary for key generation.(Kuppuswamy et al., 2023; Setyono & Ignatius Moses Setiadi, 2019)(Abid et al., 2023; Lin & Li, 2021; Lokhande, 2014; S. Singh & Saurabh, 2012)

3.4 Proposed Model and Equation

This initial stage marks the beginning of the retrieval process, the beginning of the actions to extract the secret message concealed in the stego image. The stego picture, which serves as the carrier of the buried data, starts the retrieval process. The hidden message is encoded in this image's pixels using steganographic techniques. The first thing involved in retrieving the secret message hidden in a stego image is obtaining the encryption key, which works as follows: it is vital in reversing the embedding process' encryption. It is through this key that the locations of the specific pixels containing the hidden message within the stego image are identified. Thus, in this case, the pixel location key would indicate the changes made to the pixel in the stego image during embedding to hide the secret message. The focus here is to obtain maximum information from these specific pixels. The pixel data extraction process intends to extract the data residing within the chosen pixel(s). More specifically, this operation comprises decoding the hidden sequence or bits belonging to the secret message and subsequently extracting that message. The review process goes on with the stego image until a certain pixel is located that possibly holds part(s) of a secret message. Once located, selection and data extraction are accomplished with that specific pixel. Once a bit has been retrieved, all the fetched data are sorted and arranged into bytes. This will facilitate further processing and decryption of the data, which will be further explained logically. The previously acquired encryption key is used to decrypt the returned data, which is now organized into bytes. This allows the data to be read and understood as it was originally hidden since the embedding encryption method is reversed. Finally, this indicates that the encrypted message has been successfully recovered from the stego image. From pixel selection until decryption, this is the final stage of the process. This step involves systematically applying a flowchart to extract the secret message hidden within a stego image. Each step's primary objectives

© Daffodil International University

are precise pixel selection, data extraction, conversion, and decryption, ensuring the safe and accurate recovery of the original hidden data from the stego image. This suggested steganography method hides secret information in an image using a 4-directional pixel selection mechanism. Prior to moving in the left, right, up, and down cardinal directions, the data is first embedded in the middle pixel. This process then splits once more into left, right, up, and down directions. Unlike the zigzag pixel selection technique, this method uses the center point of the image, which is determined by the width and height.

The proposed 4-directional pixel selection technique would use the binary value of each character to determine the Total Number of Secret Message Bit Lengths (SL), to achieve its purpose. Next, it will use Equation (1) to determine the Total Number of Pixels (TP) for embedding.

Total Number of Pixels,

$$TP = SL/3 \quad \text{(3.1)}$$

It will use Tp as a focus value and use Equation (2) to obtain the value of the pixel number for Each Direction (Pd).

Pixels number for each direction,

$$PD = TP/4 \quad \text{(3.2)}$$

After that, the method will begin embedding the Center Pixel's hidden message (Tx, Ty). Equation (3) must be used to determine the Height (H) and Width (W) of the cover picture to compute (Tx, Ty).

Center Pixel,

$$(T_x, T_y) = |(\frac{H}{2}, \frac{W}{2})| \quad \text{(3.3)}$$

in this case stands for the ceil function. After the fraction value is provided by the H/ 2 and/or W/ 2 in Equation (3), || will only consider the upper limit value.

The suggested method would insert the message in the center pixel (Tx, Ty), then identify the pixel in each of the four directions to insert the remaining message. Every direction embedding will adhere to the straight-line equation found in Equation (4).

© Daffodil International University

Straight line equation,

$$y = mx + c \quad [where, m = -1,0,1] \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.4)$$

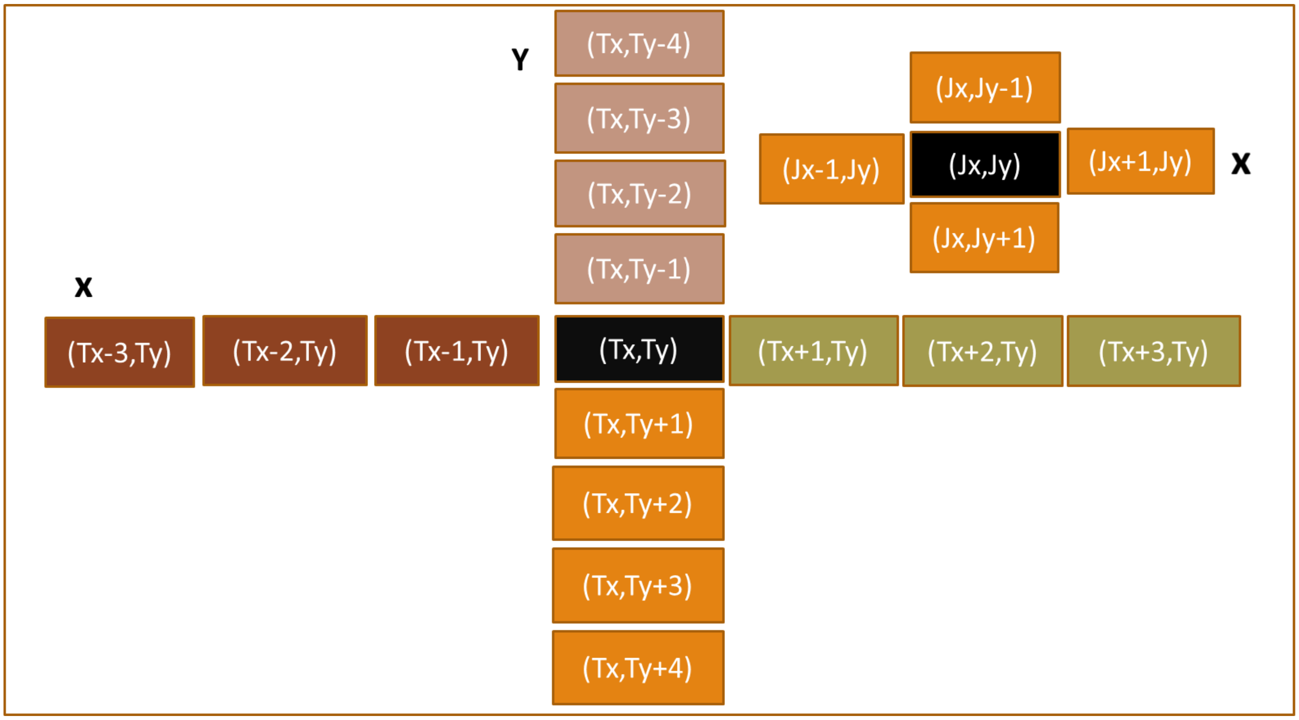


Figure 3.3: Proposed 4 directional Pixel selection of a cover image

Diagonal value of square,

$$D = \frac{H}{2} * \sqrt{2} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.5)$$

The 4-directional Pixel Position (F) can be determined using equation (6).

Pixel position,

$$F = \left(\frac{D_x}{2}\right) \pm a, \left(\frac{D_y}{2}\right) \pm a \quad \text{[where, a = 0 to pd]} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.6)$$

Equation (7, 8, 9, 10) is utilized to determine the location of the four pixels in which this method will insert the bit size number of the secret message that will be employed to retrieve the message from the Stego image.

© Daffodil International University

1st pixel position,

$$\left(J_x + 1, J_y\right) = \left\{\frac{\sqrt{2}.\frac{W}{2}}{2}\right\} + 1, \{\frac{\sqrt{2}.\frac{H}{2}}{2}\} \ldots\ldots (3.7)$$

2nd pixel position,

$$\left(J_x, J_y + 1\right) = \left\{\frac{\sqrt{2}.\frac{W}{2}}{2}\right\}, \left\{\frac{\sqrt{2}.\frac{H}{2}}{2}\right\} + 1 \ldots\ldots (3.8)$$

3rd pixel position,

$$\left(J_x - 1, J_y\right) = \left\{\frac{\sqrt{2}.\frac{W}{2}}{2}\right\} - 1, \left\{\frac{\sqrt{2}.\frac{H}{2}}{2}\right\} \ldots\ldots (3.9)$$

4th pixel position,

$$\left(J_x, J_y - 1\right) = \left\{\frac{\sqrt{2}.\frac{W}{2}}{2}\right\}, \left\{\frac{\sqrt{2}.\frac{H}{2}}{2}\right\} - 1 \ldots\ldots (3.10)$$

This method uses the Secret Message Size (Ms) to extract the value of SL from the stego image using Equation (11).

Secret Message Bit Length,

$$SL = MS * 8 \ldots\ldots (3.11)$$

3.5 XOR-Based Image Steganographic Techniques

At the beginning of the proposed message embedding and retrieval technique, the user provides the cover image and secret message. Assuming the secret message is 81 bits in size and is retrieved from a string, the process comprises altering the pixels of the cover picture to hide the information. First, the total number of pixels required to include the secret message is calculated. In this case, for instance, 81/3 = 27 pixels would be required overall, with six pixels required for each of the four orientations. In the embedding process, take a look at a cover image where the width (W) and height (H) are both set to six units. The center pixel, denoted as (Tx, Ty) and calculated as (H/2, W/2)| = (3, 3), is chosen as the starting point for embedding. Based on the RGB values of the pixel

 © Daffodil International University

(3, 3), three secret message bits are used to replace the least significant bits (LSBs) of the Red, Green, and Blue components. Then, using a 4-directional strategy that includes upward, upward-right, and other directions, the remaining secret message bits are progressively embedded into pixels.

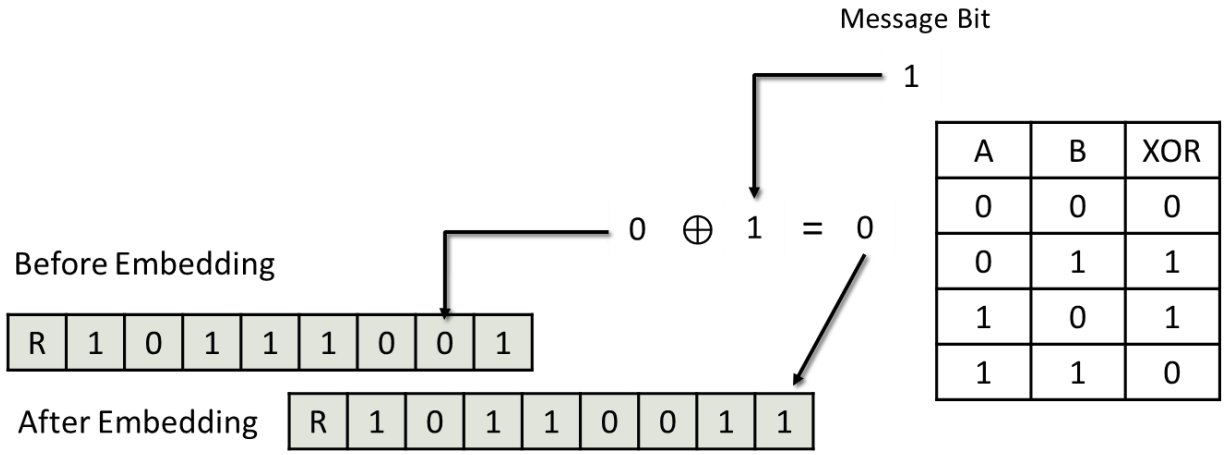


Figure 3.4: Embedding technique XOR.

During the retrieval process, the user provides the stego image. The coordinates (Jx+1, Jy), (Jx, Jy+1), (Jx-1, Jy), and (Jx, Jy-1) of the cover image, which has dimensions of H = 6 and W = 6, are calculated using the provided equations. Binary values are reversed and converted to decimal values from these locations. By assisting in the derivation of Ms, this process enables the secret message size (SL) to be calculated using a given equation (Eq. 11). The RGB values of the central pixel position (Tx, Ty) at (3, 3) are then determined. The least significant bits of the Red, Green, and Blue components are removed and stored in an array. Using a predetermined process, the method retrieves the remainder of the secret bits along designated directional paths, such as upward, upward-right, etc. The reconstructed secret message is represented as a string derived from the collected bit array. This makes hiding and extracting sensitive information within cover photos easier, using minute changes in pixels and specific directed embedding techniques to store and retrieve sensitive information securely. (Bhuiyan et al., 2019) XOR is a widely known embedding technique; thus, we found it relevant to use it throughout our study.(Al-Dmour & Al-Ani, 2016; Cheddad, Condell, Curran, & McKevitt, 2010) (Khari et al., 2020; Nath & Som, 2018)

© Daffodil International University

3.6 Embed and Retrieve Technique

This initial step represents the starting point of the data embedding technique within a flowchart. It acts as a launching pad for subsequent actions taken to conceal the hidden image message. Selecting an input cover image is one of steganography's significant steps. This is the image where secret data will be stored. Based on one parameter, there should be some form of filter applied when selecting images that tend to hide secrets but do not compromise their appearance or cause suspicion. Based on several parameters of color, spatial, and other related matters, the cover image will thus be classified into four different parts. From this, it may give a sense of classification and structure in view of the systematic way in which data embedding takes place. A previously segmented dimension of the image is studied more rigorously at this stage.

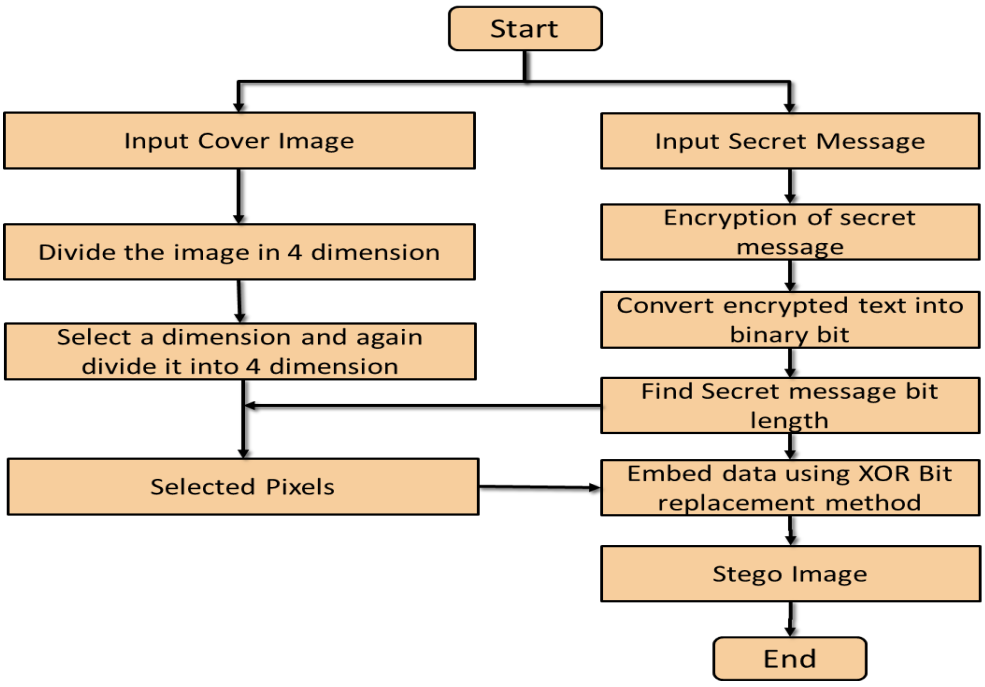


Figure 3.5: Embedding technique

It allows detailing the pixel choice to fit more complex embedding within a given dimension. As such, at this stage, the hidden message is based on what one needs to embed within the image. Generally, this message has sensitive or private information intended to be transmitted or stored in a safe manner. Therefore, it has to be encrypted by using some algorithm and corresponding keys so that the hidden data inside will remain safe and confidential during the embedding process.

© Daffodil International University

This is an encrypted file, which is translated into binary bits, meaning it comes in the form of a string of 1's and 0's. Since its binary nature defined its structure, it becomes easy to manipulate its content and embed it within an image. The number of bits comprising the secret message is counted, giving the required data that should be placed in the image, making it an adequate carrier without any loss or overflow of data. The data will be embedded by careful pixel selection to avoid obvious alterations in the overall appearance of the image. In the XOR bit replacement technique, the value of the selected pixels gets modified by XORing the binary bits of the encrypted message. Therefore, this method permits more robust data hiding with slight visual changes in the image. The resultant stego image follows the embedding process. This modified image now contains the hidden data and thus acts as a carrier for the hidden message. After this, in the flowchart, it shows that data embedding inside the image is completed.

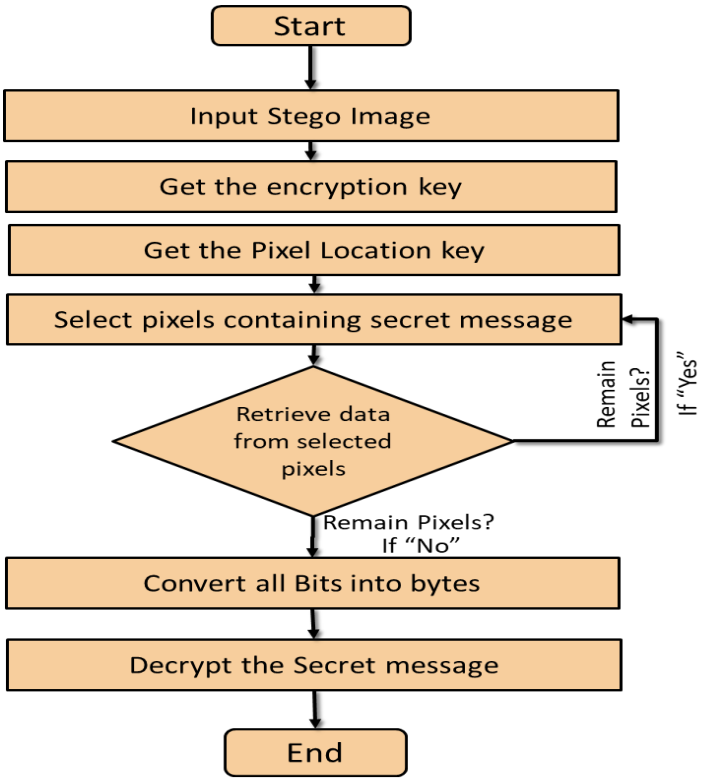


Figure 3.6: Retrieving technique

© Daffodil International University

3.7 Embedding and Retrieving Algorithm

In this way, it begins from the center of the image, using the coordinates that are halfway between the width and height to hide the center of the information. That indicates the length of the message, denoted by SL. In RGB, it is assumed that there is a bit per pixel. The calculation of total pixels (TP) depends on dividing SL by three. To convert it into a binary format, SL is reversed. Specific bits of the SL, like those of (Jx+1, Jy), (Jx, Jy+1), (Jx-1, Jy), and (Jx, Jy-1), are taken to be the identifying directional pixels. In this case, the value of a is set to 0 at initialization. The Distancemask D is calculated by dividing the square root of two by half of the image height. Further, the embedding will be done in loops emanating from the center diagonally, considering pixels (Dx/2) ± a and (Dy/2) ± a until Pd pixels are reached. Since the technique commences from the image center, it needs to conceal the message cleverly. The clever part is initially dividing parts of the message length into specific directional pixels, then gradually extending the embedding into diagonal positions and reducing perceptual distortion.

Table 3.1: Embedding and Retrieving Algorithm

Embedding Algorithm	**Retrieving Algorithm**
Result: Stego Image M← input I← input W = Image Width; H = Image Height; (Tx, Ty) = (H/2, W/2); embed ((Tx, Ty)); SL= Length of M; TP= SL/3;	Result: Secret Message S←input Ms ←(Jx+1,Jy), (Jx, Jy+1), (Jx-1,Jy), (Jx, Jy-1) Ms← decimal(reverse(Ms)) SL← (Ms * 8)) W = Image Width; H = Image Height; (Tx, Ty) = (H/2, W/2); retrieve ((Tx, Ty));

© Daffodil International University

Pd= TP/4;
SL← reverse(binary(SL))
(Jx+1, Jy), (Jx, Jy+1), (Jx-1,Jy), (Jx, Jy-1) ←SL
a = 0;
D=H/2. √2;
while a ≤ Pd do
F = (Dx/2) ± a, (Dy/2) ± a
embed(F);
a++;
function embed (position):
RGB← position
Update RGB ← message
	SL= Length of M;
	Tp= SL/3;
	Pd= TP/4;
	a = 0;
	D=H/2. √2;
	while a ≤ Pd do
	F = (Dx/2) ± a, (Dy/2) ± a
	retrieve(F);
	a++;
	function retrieve (position):
	RGB← position
	message[]← RGB

After embedding, the two inputs for the method are the stego image and the coordinates (Jx+1, Jy), (Jx, Jy+1), (Jx-1, Jy), (Jx, Jy-1), where the secret message bits are inserted. The decimal values are calculated for these locations, and the order is reversed to receive the message bit sequence. Ms is the sum of the decimal values for the selected pixel positions, which must be multiplied by 8 to estimate the secret message length (SL). The width and height of the image are calculated, while the center coordinates (Tx, Ty) are at half the width and half the height of the image.The length of the message is obtained by recalculating SL. Assuming RGB has three bits per pixel, divide SL by three to determine the Total Pixels (TP) required to obtain the message. Pixels for retrieval (Pd) are identified using a quarter of TP. Setting 'a' to 0 is the initial step in the retrieval process. The diagonal value (D) of a square indicates its diagonal length. Retrieval continues in a loop up to Pd, extending diagonally from the center by accounting for pixels (Dx/2) ± a and (Dy/2) ± a. To recover the hidden content in a methodical manner, the retrieval algorithm first decodes

© Daffodil International University

preset pixel coordinates. The original secret message is then gradually pieced together from the diagonally expanded retrieval area.

3.8 Evaluation

MATLAB is the main tool used in this study, along with quality matrices for evaluation, because it is widely used by other researchers. (Aqeel & Raheel, 2019; Huang et al., 2019; Alam et al., 2020)

3.8.1 Equations of Quality Metrics

Equations provide mathematical definitions of the four quality assessment matrices—MSE, SSIM, PSNR, and capacity ratio—that are frequently used to assess the efficacy and security of the steganography process.(Aqeel & Raheel, 2019; Huang et al., 2019)

3.8.1.1 Mean-square error (MSE)

Shows the greatest degree of error between the compressed and original images. Mean squared error, or MSE, is used to calculate the difference between the corresponding pixels of the original and stego images. The definition of MSE in mathematics is,

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

$\boldsymbol{a}$= The height of the frames (number of rows of pixels).

$\boldsymbol{b}$= The width of the frames (number of columns of pixels).

$\boldsymbol{(i, j)}$= Pixel intensity of the original frame at $i\text{^}th$ row, and $j\text{^}th$ column.

$\boldsymbol{(i, j)}$= Pixel intensity of the stego frame at $i\text{^}th$ row, and $j\text{^}th$ column

Higher reliability is indicated by a lower Mean Squared Error (MSE) score, which shows the least amount of error between the original image and the stego.

© Daffodil International University

3.8.1.2 Peak Signal to Noise Ratio (PSNR)

PSNR evaluates the quality of an image by contrasting an original with a compressed or distorted copy. It is used to assess the stego image's subtlety in relation to the original image in image steganography. The PSNR is estimated using the mean squared error (MSE) and the maximum pixel value, which for 8-bit images usually equals 255.

$$PSNR = 10 \log_{10} \frac{MAX_X^2}{MSE}$$

MAX= possible maximum pixel value in the image (For an 8-bit image, the max value is 255 (11111111)).

PSNR is measured in dB, and it is based on MSE. Several studies demonstrate that a picture can be deemed high quality if the PSNR between the cover and stego image is greater than 40 dB.

3.8.1.3 Capacity Ratio

The term "capacity ratio" refers to an important steganography parameter that measures how much secret data can be stored in a cover object, like an image, without significantly changing the cover medium. This ratio demonstrates how well data is hidden without sacrificing the carrier's aesthetic appeal. Steganographic techniques conceal information within a cover medium so that the changes are not visible to the naked eye. Since it establishes the ideal ratio for information concealment while maintaining the integrity of the cover medium, the capacity ratio is essential to accomplishing this goal.

$$\textbf{Capacity ratio} = \frac{\textbf{Secret Data Size}}{\textbf{Image Size}} \times 100$$

The capacity ratio must be high.

© Daffodil International University

CHAPTER 4: EXPERIMENTS AND RESULTS

4.1 Introduction

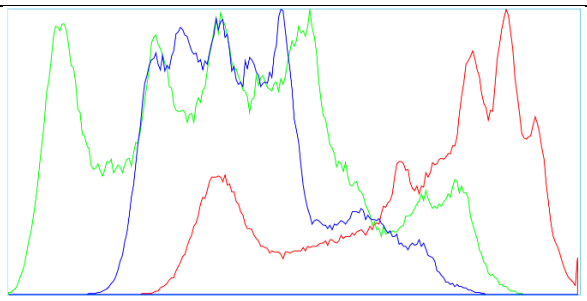
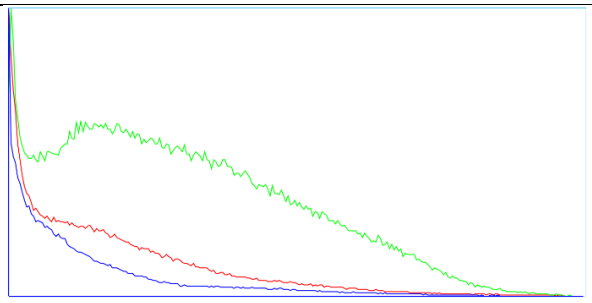
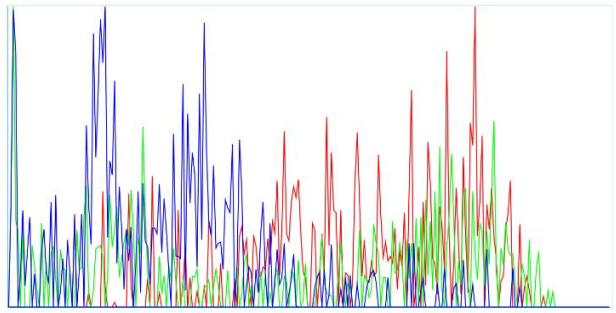
This section presents an in-depth analysis of the proposed steganographic method. Particular emphasis is placed on visual comparison between the original cover image and the altered stego image. Such a comparison enables a visual demonstration of how successful the method has been in embedding information into the cover image without revealing its presence. The proposed method has also been compared with other well-established methods of steganography to gather details on its results. This is further supported by statistical analysis. The primary metrics of measurement are mean-square error, peak signal-to-noise ratio, capacity ratio, and structured similarity index measurement. These have been widely used in the field of image processing and steganography and are meant to measure the quality differences between the stego image and its cover counterpart. Such would carry out in detail an assessment that includes perceptual similarity, the noise introduced during embedding, the integrity of the concealed data, and the overall quality of the resultant image. Thus, the proposed technology will be subject to a broad analysis, including various quality parameters, visual inspection, and comparison with contemporary techniques.

4.2 Test Data

Lena, Lake, and Pepper, the three images were used in the research to explain the proposed method.(Khmag et al., 2015; Shanthakumari & Malliga, 2019; Zhai et al., 2008) (Zhang et al., 2008)

© Daffodil International University

Table 4.1: Cover Image for Proposed Model Implementation.

Number	Image	Image name	Size	Histogram
1		Lena	512*512	
2		Lake	512*512	
3		pepper	512*512	

© Daffodil International University

The 512 × 512 photos are the most frequently used size in the related study, they are taken into consideration for analysis in this case.(Alam et al., 2020; B. Singh et al., 2021; X. Wu et al., 2020)The selection was motivated by frequently using these figures in steganography works.

4.3 Result

Table 4.2: Quality Measurement Metrices for the Proposed Model.

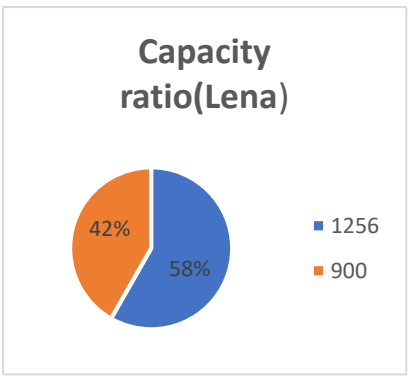
Image	**Size**	**Payload**	**PSNR**	**MSE**
Lena	512*512	512 bytes	73.8880309756	0.0000000409
		256 bytes	76.7692926621	0.0000000210
		128 bytes	79.7634777772	0.9999997727
Lake	512*512	512 bytes	74.0081783393	0.0000000397
		256 bytes	76.9087381858	0.0000000204
		128 bytes	79.9357417969	0.0000000101
pepper	512*512	512 bytes	73.9382148155	0.0000000404
		256 bytes	76.9422099878	0.0000000202
		128 bytes	79.8038775552	0.0000000105

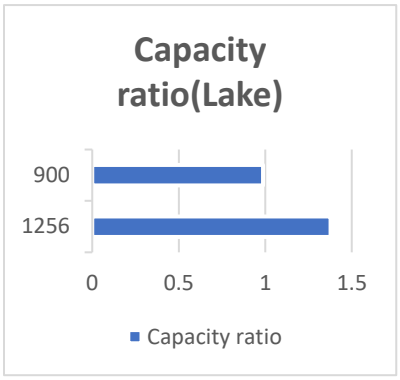
Table 4.3: Quality Measurement Metrics (capacity ratio)

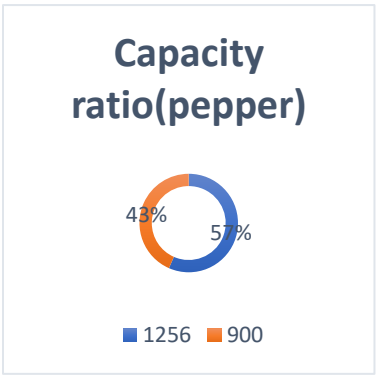
Image	**Size**	**Payload**	**Capacity ratio**
Lena	512*512	1256 bytes	1.27766927
		900 bytes	0.915527344
Lake	512*512	1256 bytes	1.37766927
		900 bytes	0.986527344
pepper	512*512	1256 bytes	1.29766927
		900 bytes	0.995527344

© Daffodil International University

Graphical representation of capacity ratio of images:







For Lena, Lake, and pepper, 512 × 512 images were utilized in Table 2, with payload sizes of 512 bytes, 256 bytes, and 128 bytes, respectively, taken into consideration. Lena had MSE values of 0.0000000409, 0.0000000210, and 0.9999997727 using the proposed approach, while Lake had MSE values of 0.0000000397, 0.0000000204, and 0.0000000101. The MSE values for pepper were 0.0000000404, 0.0000000202, and 0.0000000105 in that order. While the corresponding PSNR readings for Lake were 74.0081783393, 76.9087381858, and 79.9357417969, Lena's values were 0.0000000409, 76.7692926621, and 79.7634777772. Pepper was observed with a PSNR value of 73.9382148155, 76.9422099878, and 79.8038775552. In Table 3 Images of size 512×512 (Lena, Lake, and Pepper) were tested with payloads of 1256 bytes and 900 bytes, showing slight variations in capacity ratios — Lena (1.28, 0.92), Lake (1.38, 0.99), and Pepper (1.30, 1.00).

4.5 Comparison with Existing Model

The experimental results, analysis, and comparison of other modern steganographic techniques with the two most often used images by other researchers—pepper and Lena—are presented in this part. (Z. Khan et al., 2016; Sarkar & Karforma, 2018)

Table 4.4: Comparison among techniques.

Image	Image Size	Payload	Techniques	SSIM	MSE	PSNR

© Daffodil International University

Lena	512 X 512	128 bytes	Proposed Model	0.9999997727	0.9999997727	79.7634777772
			Thresholding Model (Z. Khan et al., 2016)	0.99996	0.0040	72.0590
			4 direction Model (Sarkar & Karforma, 2018)	0.99998	0.0007	79.9107

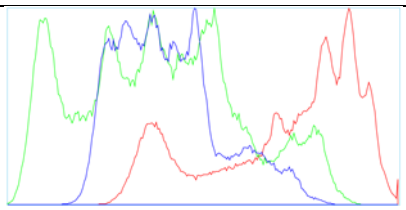
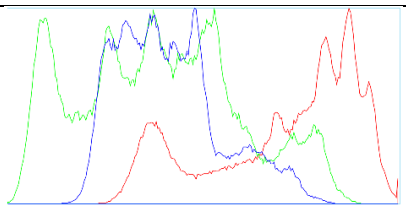
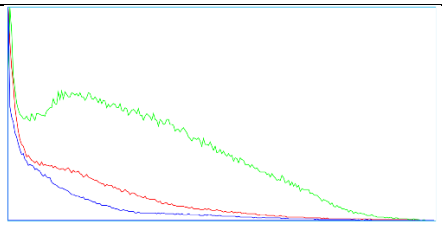
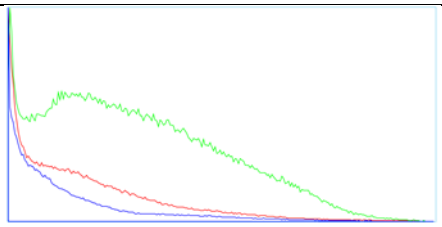
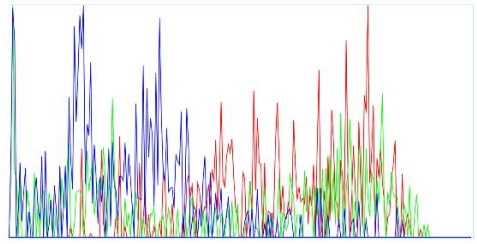
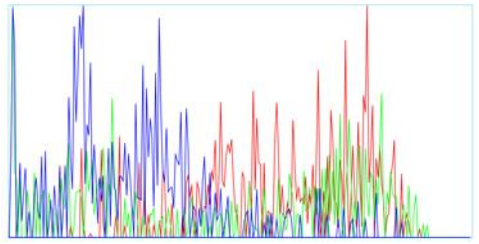
According to Table 2's results, there are only slight differences between the original and stego images. Both stego images have exceptionally high SSIM values (>0.99999) and extremely low MSE for the recommended X model with a 128-byte payload. Significantly high PSNR values (>79 dB) indicate minimal perceived changes and excellent image quality retention. By way of contrast, the thresholding model demonstrates a noteworthy reduction in SSIM and an increase in MSE, signifying more conspicuous distinctions between the stego and original images. Besides, the PSNR values remarkably decline, signifying image integrity loss against the proposed X model. Also, the 4-direction model shows variance in PSNR, MSE, and SSIM. While the MSE increased, the SSIM values remained relatively high, indicating more pronounced changes due to the steganography process. However, since the PSNR values were variable, the results were also found to be non-uniform concerning image quality retention. Generally, based on the results of both stego images, the proposed model outperforms the thresholding and 4-direction models in SSIM, MSE, and PSNR. This confirms its capability for better data hiding with an undetectable trade-off in visual quality since it will have the best picture fidelity and imperceptibility among all contemporary steganographic systems investigated in this work.

4.6 Comparative Visual Analysis

Table 4.5: Comparative analysis between cover image and stego image based on Histogram.

image	Payload	Cover image	Stego image

© Daffodil International University

Lena	512 bytes		
Lake	512 bytes		
pepper	512 bytes		

The histogram analysis shows that the cover and stego images do not differ significantly. The output of the histogram shows that the two images are not very different, a difference that is not visible to the naked eye. Using the data hiding technique, this experiment shows the performance of the proposed algorithm compared to similar algorithms.

© Daffodil International University

CHAPTER 5: CONCLUSION

This research presents an enhanced technique for 4-directional pixel selection in image steganography. Due to the presence of fine quality images, the proposed method significantly increases the capacity for data hiding in images by overcoming the deficiencies of traditional LSB substitution methods. After applying an RSA encryption algorithm on the hidden data, further protection is afforded to the modeling during its development. Features and results indicate that this model presents more outstanding performance in terms of image quality and data hiding capabilities against other steganographic techniques. There lie several pathways from which this thesis will lead to promising ways and contributions toward safe and effective data embedding within images, along with many important applications in several areas of research that are concerned with the safety of transmitted data or hidden communications. From the above explanation and analysis, it is proved that the proposed technique for hiding data using steganography is better in terms of security and less imperceptible than many other existing techniques used for data concealment. However, the 512 × 512 cover image of this model retains a maximum of 1256 bytes of hidden data. We want to address these constraints in our upcoming work, enabling it to handle over 1256 bytes into a 512 × 512 cover image.

© Daffodil International University

REFERECES

Abid, R., Iwendi, C., Javed, A. R., Rizwan, M., Jalil, Z., Anajemba, J. H., & Biamba, C. (2023). An optimised homomorphic CRT-RSA algorithm for secure and efficient communication. *Personal and Ubiquitous Computing*, *27*(3). https://doi.org/10.1007/s00779-021-01607-3

Abikoye, O. C., & Ogundokun, R. O. (2021). Efficiency of LSB steganography on medical information. *International Journal of Electrical and Computer Engineering*, *11*(5). https://doi.org/10.11591/ijece.v11i5.pp4157-4164

Abood, E. W., Abdullah, A. M., Al Sibahee, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Kalafy, S. A. A., & Ghrabta, M. J. J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. *Bulletin of Electrical Engineering and Informatics*, *11*(1). https://doi.org/10.11591/eei.v11i1.3279

Alam, S. T., Jahan, N., & Hassan, M. M. (2020). A new 8-directional pixel selection technique of LSB based image steganography. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, *325 LNICST*. https://doi.org/10.1007/978-3-030-52856-0_8

Al Maki, W. F., Muktyas, I. B., Arifin, S., Suwarno, & Aziz, M. K. B. M. (2023). Implementation of a Logistic Map to Calculate the Bits Required for Digital Image Steganography Using the Least Significant Bit (LSB) Method. *Journal of Computer Science*, *19*(6). https://doi.org/10.3844/jcssp.2023.686.693

Aslam, M. A., Rashid, M., Azam, F., Abbas, M., Rasheed, Y., Alotaibi, S. S., & Anwar, M. W. (2022). Image Steganography using Least Significant Bit (LSB)-A Systematic Literature Review. *Proceedings of 2022 2nd International Conference on Computing and Information Technology, ICCIT 2022*. https://doi.org/10.1109/ICCIT52419.2022.9711628

Dalal, M., & Juneja, M. (2021). A survey on information hiding using video steganography. *Artificial Intelligence Review*, *54*(8). https://doi.org/10.1007/s10462-021-09968-0

© Daffodil International University

Degadwala, S., Panda, S., Vajravelu, A., & C, R. (2024). Data Hiding using Video Steganography. *International Journal of Electronic Security and Digital Forensics*, *1*(1). https://doi.org/10.1504/ijesdf.2024.10052934

Duan, X., Gou, M., Liu, N., Wang, W., & Qin, C. (2020). High-capacity image steganography based on improved xception. *Sensors (Switzerland)*, *20*(24). https://doi.org/10.3390/s20247253

Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A New High Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network. *IEEE Access*, *8*. https://doi.org/10.1109/ACCESS.2020.2971528

Ehsan Ali, U. A. Md., Ali, E., Sohrawordi, Md., & Sultan, Md. N. (2021). A LSB Based Image Steganography Using Random Pixel and Bit Selection for High Payload. *International Journal of Mathematical Sciences and Computing*, *7*(3), 24–31. https://doi.org/10.5815/ijmsc.2021.03.03

Fu, Z. J., Wang, F., Sun, X. M., & Wang, Y. (2020). Research on Steganography of Digital Images based on Deep Learning. *Jisuanji Xuebao/Chinese Journal of Computers*, *43*(9). https://doi.org/10.11897/SP.J.1016.2020.01656

Ghoul, S., Sulaiman, R., & Shukur, Z. (2023). A Review on Security Techniques in Image Steganography. *International Journal of Advanced Computer Science and Applications*, *14*(6). https://doi.org/10.14569/IJACSA.2023.0140640

Jebur, S. A., Nawar, A. K., Kadhim, L. E., & Jahefer, M. M. (2023). Hiding Information in Digital Images Using LSB Steganography Technique. *International Journal of Interactive Mobile Technologies*, *17*(7). https://doi.org/10.3991/ijim.v17i07.38737

Khan, M., & Rasheed, A. (2023). A high-capacity and robust steganography algorithm for quantum images. *Chinese Journal of Physics*, *85*. https://doi.org/10.1016/j.cjph.2023.06.016

Kuppuswamy, P., Al-Maliki, S. Q. Y. A. K., John, R., Haseebuddin, M., & Meeran, A. A. S. (2023). A hybrid encryption system for communication and financial transactions

 © Daffodil International University

using RSA and a novel symmetric key algorithm. *Bulletin of Electrical Engineering and Informatics*, *12*(2). https://doi.org/10.11591/eei.v12i2.4967

Kuyoro, A., Nzenwata, U. J., Awodele, O., & Idowu, S. (2022). GAN-Based Encoding Model for Reversible Image Steganography. *Revue d'Intelligence Artificielle*, *36*(4). https://doi.org/10.18280/ria.360407

Liao, X., Yin, J., Chen, M., & Qin, Z. (2022). Adaptive Payload Distribution in Multiple Images Steganography Based on Image Texture Features. *IEEE Transactions on Dependable and Secure Computing*, *19*(2). https://doi.org/10.1109/TDSC.2020.3004708

Mahmoud, M. M., & Elshoush, H. T. (2022). Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography-An Innovative Approach. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3155146

Maji, G., Mandal, S., & Sen, S. (2021). Cover independent image steganography in spatial domain using higher order pixel bits. *Multimedia Tools and Applications*, *80*(10). https://doi.org/10.1007/s11042-020-10298-6

Mohamed, M., Mofaddel, M., & Abd El-Naser, T. (2023). Comparison Study Between Simple LSB and Optimal LSB Image Steganography. *Sohag Journal of Sciences*, *8*(1). https://doi.org/10.21608/sjsci.2022.165686.1036

Molato, A. D., Calanda, F. B., Sison, A. M., & Medina, R. P. (2022). LSB-based Random Embedding Image Steganography Technique Using Modified Collatz Conjecture. 2022 7th International Conference on Signal and Image Processing, ICSIP 2022. https://doi.org/10.1109/ICSIP55141.2022.9886754

Rahman, S., Masood, F., Khan, W. U., Ullah, N., Khan, F. Q., Tsaramirsis, G., Jan, S., & Ashraf, M. (2020). A novel approach of image steganography for secure communication based on LSB substitution technique. *Computers, Materials and Continua*, *64*(1). https://doi.org/10.32604/CMC.2020.09186

 © Daffodil International University

Rahman, S., Uddin, J., Khan, H. U., Hussain, H., Khan, A. A., & Zakarya, M. (2022). A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method. *IEEE Access*, *10*. https://doi.org/10.1109/ACCESS.2022.3224745

Rustad, S., Setiadi, D. R. I. M., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University - Computer and Information Sciences*, *34*(6). https://doi.org/10.1016/j.jksuci.2020.12.017

Saad, A. H. S., Mohamed, M. S., & Hafez, E. H. (2021). Coverless Image Steganography Based on Optical Mark Recognition and Machine Learning. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3050737

Sahu, A. K., & Sahu, M. (2020). Digital image steganography and steganalysis: A journey of the past three decades. In *Open Computer Science* (Vol. 10, Issue 1). https://doi.org/10.1515/comp-2020-0136

Setiadi, D. R. I. M. (2021). PSNR vs SSIM: imperceptibility quality assessment for image steganography. *Multimedia Tools and Applications*, *80*(6). https://doi.org/10.1007/s11042-020-10035-z

Setiadi, D. R. I. M. (2022). Improved payload capacity in LSB image steganography uses dilated hybrid edge detection. *Journal of King Saud University - Computer and Information Sciences*, *34*(2). https://doi.org/10.1016/j.jksuci.2019.12.007

Shah, P. D., & Bichkar, R. S. (2021). Secret data modification based image steganography technique using genetic algorithm having a flexible chromosome structure. *Engineering Science and Technology, an International Journal*, *24*(3). https://doi.org/10.1016/j.jestch.2020.11.008

Shanthakumari, R., & Malliga, S. (2019). Dual-layer security of image steganography based on IDEA and LSBG algorithm in the cloud environment. *Sadhana - Academy Proceedings in Engineering Sciences*, *44*(5). https://doi.org/10.1007/s12046-019-1106-0

 © Daffodil International University

Shehab, D. A., & Alhaddad, M. J. (2022). Comprehensive Survey of Multimedia Steganalysis: Techniques, Evaluations, and Trends in Future Research. *Symmetry*, *14*(1). https://doi.org/10.3390/sym14010117

Subramanian, N., Elharrouss, O., Al-Maadeed, S., & Bouridane, A. (2021). Image Steganography: A Review of the Recent Advances. *IEEE Access*, *9*. https://doi.org/10.1109/ACCESS.2021.3053998

Suresh, K. S., & Kamalakannan, T. (2022). Image steganography based on LSB using various scanning methods in spatial domain. *International Journal of Health Sciences*. https://doi.org/10.53730/ijhs.v6ns3.7552

Tayyeh, H. K., & Al-Jumaili, A. S. A. (2022). A combination of least significant bit and deflate compression for image steganography. *International Journal of Electrical and Computer Engineering*, *12*(1). https://doi.org/10.11591/ijece.v12i1.pp358-364

Wang, Z., Zhou, M., Liu, B., & Li, T. (2022). Deep Image Steganography Using Transformer and Recursive Permutation. *Entropy*, *24*(7). https://doi.org/10.3390/e24070878

Wu, X., Xu, M., Qiao, T., Pan, B., & Liao, X. (2022). Review of reversible data hiding based on the spatial domain of images. In *Journal of Image and Graphics* (Vol. 27, Issue 1). https://doi.org/10.11834/jig.210292

Yang, A., Bai, Y., Xue, T., Li, Y., & Li, J. (2023). A novel image steganography algorithm based on hybrid machine leaning and its application in cyberspace security. *Future Generation Computer Systems*, *145*. https://doi.org/10.1016/j.future.2023.03.035

Yang, J., Shang, F., Liao, Y., & Chen, Y. (2023). Toward High Capacity and Robust JPEG Steganography Based on Adversarial Training. *Security and Communication Networks*, *2023*. https://doi.org/10.1155/2023/3813977

 © Daffodil International University