ENHANCED LEAST SIGNIFICANT BIT-BASED ALGORITHMS FOR SPATIAL DOMAIN IMAGE STEGANOGRAPHY

ABDALLA RAMAH AL ENZI

UNIVERSITI SAINS MALAYSIA

2025

ENHANCED LEAST SIGNIFICANT BIT-BASED ALGORITHMS FOR SPATIAL DOMAIN IMAGE STEGANOGRAPHY

by

ABDALLA RAMAH AL ENZI

Thesis submitted in fulfilment of the requirements
for the degree of
Doctor of Philosophy

June 2025

ACKNOWLEDGEMENT

First and foremost, I would like to offer my sincerest gratitude to Allah for blessing me with endurance and fortitude to complete this dissertation.

This thesis would not have been possible without the support of many people. I am much grateful to my principal supervisor, Prof. Dr. Putra Sumari, and co-supervisor, Associate Professor Dr. Samer Atawneh, for their invaluable assistance, encouragement, guidance, and expertise. I appreciate all their time and ideas to make my Ph.D. experience productive and stimulating. Without them, the road towards completing this thesis would have been difficult.

I would also like to extend my sincerest appreciation to my dear parents for their constant love and support throughout my studies. Their unwavering faith in my abilities has been a source of inspiration and motivation. Furthermore, I would like to express my gratitude to my dear friends, Faisal Eyadah and Mohammad Abdullah, for their unwavering support and encouragement. Their presence and companionship have been a source of comfort and motivation during challenging times.

Last but most importantly, I would like to express my love and appreciation to my beloved wife, Sophia Al Masoudi, for her endless love, support, and encouragement throughout my studies. Her unwavering belief in my abilities and her willingness to sacrifice her time and energy to support me have been a constant source of inspiration and motivation.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF SYMBOLS

MAX_I	Maximum possible pixel value in the image
SSIM(x,y)	Structural Similarity Index Measure between images x and y
μ_x	Mean of image xxx (average pixel value of image x)
μ_y	Mean of image yyy (average pixel value of image y)
σ_{xy}	Covariance between images x and y
σ_{x^2}	Variance of image x (measure of the spread of pixel values in image x)
σ_{y^2}	Variance of image y (measure of the spread of pixel values in image y)
C_1	Small constant added to avoid division by zero in the SSIM formula
C_2	Small constant added to avoid division by zero in the SSIM formula
K_1	Constant used to calculate C_1 in SSIM
K_2	Constant used to calculate C_2 in SSIM
L	Dynamic range of the pixel values (maximum pixel value minus minimum pixel value)
BPP	Bits Per Pixel (a measure of embedding efficiency)

LIST OF ABBREVIATIONS

AES	Advanced Encryption Standard
ASCII	American Standard Code For Information Interchange
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
dB	Decibels, a unit of measurement for PSNR
EMD	Exploiting Modification Direction
ENMPB	Expected Number of Modifications per Byte
ENMPP	Expected Number of Modifications per Pixel
EOF	End-Of-File marker
GIF	Graphics Interchange Format
HAS	Human Auditory System
HVD	Human Visual System
IDFT	Inverse Discrete Fourier Transform
IQM	Image Quality Metrics
JPEG	Joint Photographic Experts Group
KB	Kilobyte
LSB	Least Significant Bit
MSE	Mean Squared Error
PNG	Portable Network Graphics
PILSB	Pixel Indices Least Significant Bit
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Differencing
RGB	Red, Green, and Blue Channels
RGBA	Red-Green-Blue-Alpha
RRLSB	Reversible Rewritable Least Significant Bit
SDLSB	Semi-Adaptive Least Significant Bit
SMLSB	Single Mismatch LSB Embedding
SNR	Signal-to-Noise Ratio
SSIM	Structural Similarity
SSIS	Spread Spectrum Image Steganography
ZIP	Compressed File

LIST OF APPENDICES

ALGORITMA BERASASKAN BIT TERKURANG BERERTI TERTINGKAT UNTUK STEGANOGRAFI IMEJ DOMAIN RUANGAN

ABSTRAK

Dalam keselamatan imej digital, steganografi menyembunyikan data dalam imej menggunakan kaedah Least Significant Bit (LSB), yang sering menjejaskan kualiti imej. Kajian ini memperkenalkan tiga algoritma baharu: Pixel Indices Least Significant Bit (PILSB), Semi-Adaptive Least Significant Bit (SDLSB), dan Reversible Rewritable Least Significant Bit (RRLSB), yang bertujuan untuk meningkatkan kualiti imej stego dengan meminimumkan bilangan bit yang diubah semasa proses penyisipan. Matlamat kajian ini adalah untuk menangani kekangan steganografi LSB tradisional, terutamanya isu keselamatan yang terjejas, kejelasan yang berkurangan, dan kapasiti beban yang terhad. Metodologi kajian melibatkan analisis perbandingan ketiga-tiga algoritma ini, dengan mengukur Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), dan Structural Similarity Index (SSIM) merentasi saiz imej dan mesej rahsia yang berbeza. PILSB menggunakan LSB Merah dan Hijau untuk penyisipan data serta LSB Biru untuk penunjuk, yang meningkatkan kecekapan penyisipan. SDLSB secara dinamik menguraikan byte berdasarkan intensiti warna untuk meningkatkan kapasiti beban, sementara RRLSB menggunakan reverse LSB dalam proses dua peringkat untuk penyisipan data secara tidak langsung. Hasil eksperimen menunjukkan peningkatan yang ketara dalam kecekapan, kejelasan, dan kapasiti beban: PILSB mencatatkan peningkatan PSNR sebanyak 3.5%, pengurangan MSE sebanyak 25%, dan peningkatan SSIM sebanyak 0.05; SDLSB meningkatkan PSNR sebanyak 4%, mengurangkan MSE sebanyak 20%, dan memperbaiki SSIM sebanyak 0.07; RRLSB mencatatkan peningkatan PSNR sebanyak 5%, pengurangan MSE sebanyak 30%, dan peningkatan SSIM sebanyak

0.08. Algoritma ini juga menunjukkan ketahanan yang kukuh terhadap alat steganalisis, mencapai kadar pengesanan masing-masing sebanyak 2.5%, 1.6%, dan 0.9% menggunakan StegExpose, mengatasi teknik yang ada. Kesimpulannya, kajian ini memajukan keselamatan imej digital dengan meningkatkan kualiti imej stego, kapasiti beban, dan ketahanan terhadap steganalisis. Kajian lanjut akan meneroka pengembangan kaedah ini kepada imej dengan kedalaman bit yang lebih tinggi, video, dan fail ZIP, serta mengintegrasikan teknik kriptografi untuk keselamatan yang dipertingkatkan, dengan potensi aplikasi dalam penyembunyian data perubatan dan transaksi dalam talian yang selamat.

.

ENHANCED LEAST SIGNIFICANT BIT-BASED ALGORITHMS FOR SPATIAL DOMAIN IMAGE STEGANOGRAPHY

ABSTRACT

In digital image security, steganography conceals data within images using Least Significant Bit (LSB) methods, which often compromise image quality. This research introduces three novel algorithms: Pixel Indices Least Significant Bit (PILSB), Semi-Adaptive Least Significant Bit (SDLSB), and Reversible Rewritable Least Significant Bit (RRLSB), which aim to improve stego-image quality by minimizing the number of modified bits during the embedding process. The goal is to address the limitations of traditional LSB steganography, particularly issues of compromised security, reduced imperceptibility, and limited payload capacity. The methodology involves a comparative analysis of the three algorithms, measuring Peak Signal-to-Noise Ratio (PSNR), Mean Squared Error (MSE), and Structural Similarity Index (SSIM) across different image and secret message sizes. PILSB uses Red and Green LSBs for data embedding and Blue LSBs for indexing, improving embedding efficiency. SDLSB dynamically decomposes bytes based on color intensity to increase payload, while RRLSB employs reverse LSB in a two-stage process for indirect data embedding. Experimental results show significant improvements in efficiency, imperceptibility, and payload capacity: PILSB achieves a 3.5% PSNR improvement, 25% MSE reduction, and 0.05 SSIM enhancement; SDLSB enhances PSNR by 4%, reduces MSE by 20%, and improves SSIM by 0.07; RRLSB achieves a 5% PSNR improvement, 30% MSE reduction, and 0.08 SSIM enhancement. These algorithms also demonstrate strong resistance to steganalysis tools, achieving detection rates of 2.5%, 1.6%, and 0.9% respectively using StegExpose, outperforming existing techniques. In conclusion, this research advances digital image security by improving

stego-image quality, payload capacity, and resistance to steganalysis. Future research will explore extending these methods to multi-bit-depth images, videos, and ZIP files, as well as integrating cryptographic techniques for enhanced security, with potential applications in medical data hiding and secure online transactions.

CHAPTER 1
INTRODUCTION

1.1 Overview

Due to the internet and advancement in modern technology, the world has become a small village. Nowadays, the rapid growth of the internet has led to an extensive transfer/exchange of files such as images, video, and data files. Exchanging, downloading, and uploading files over the internet have become familiar to a large percentage of the population because of the simplicity and speed of hiding the files. However, the availability and easiness of communication among people through the internet cost an individual's privacy. With advancements in digital communication technology, ensuring individuals' privacy becomes increasingly challenging. Efforts to serve this goal have created ways of hiding private information (Kordov & Zhelezov, 2021).

Today, the most popular information security methods are Steganography and Cryptography; they are often interconnected. They share goals and objectives to protect confidential information and ensure that it reaches the other party safely. Steganography and cryptography differ in that in the latter. It is possible to notice that a secret message has been encrypted. However, this hidden message is not decodable unless one knows the appropriate keys. In steganography, the hidden message itself may not be difficult to decode, but hardly would one notice the presence of this secret message. The justification of steganography's supremacy over cryptography is that hiding information in a photograph of a family picnic is less suspicious than communicating an encrypted file (AL-Shaaby & AlKharobi, 2017).

Digital steganography refers to hiding secret data within different types of digital multimedia files, such as images, audio, video, and text. This concealment is performed in a manner that makes it extremely difficult to detect the presence of the embedded secret message. (Achmad, 2017). These altered images, known as stego-images, appear no different from the original images to most people. Ideally, only parties using the images as means of communication can detect the hidden messages (Chitradevi, et al., 2017).

Most types of multimedia files used in hiding data are digital images since they have a vast amount of redundant data. In addition, because digital images have the property of innocence, scholars have preferred them as the carrier media for hiding secret information (Shaik, et al., 2017; Sahu & Sahu, 2020). Also, the digital image is one of the most familiar multimedia files that are readily available online. The original image, usually called the carrier or cover image, embed the secret data to produce the stego-image. The cover images and stego-images must match closely, making it challenging to raise suspicion or attract any unwanted attention of any difference between the two images (Nashat & Mamdouh, 2019). It is an ongoing research area with many applications in distinct fields such as industrial applications, smart cities, military secrets, medical, banking information, online transactions, and other financial and commercial purposes (Douglas, et al., 2017; Sahu & Sahu, 2020). These applications become an urgent necessity when the loss of information is strictly prohibited (Bhagat & Bhardwaj, 2019).

Researchers and governmental agencies are currently engaged in efforts to improve the security and privacy of data transmission and communication. One strategy they're concentrating on is image steganography, which entails concealing confidential information within images. These institutions also aim to develop algorithms to identify

hidden messages used by individuals or groups involved in illegal activities such as terrorism, cybercrime, or other aggressive behaviors (Dalal & Juneja, 2021).

To decide which steganographic system is better than another, a process of evaluation of steganographic systems is necessary. There are three evaluation criteria for determining and measuring the superiority of steganographic systems over another in terms of their priority: the distortion measure (Imperceptibility), the amount of confidential information (steganographic capacity or payload), and security (Pradhan, et al., 2016). However, the standard consistency criteria often considered for evaluating an image steganography method are insufficient (Roy & Changder, 2016).

In general, steganographic systems encounter difficulties when someone uncovers the concealed data within the stego-image. Likewise, if the method employed to hide confidential information raises doubts, it might be deemed ineffective. Hence, the main goal of a steganography system is to veil sensitive information in a manner that reduces the likelihood of the secret message being discovered (Woolley, et al., 2017). Therefore, imperceptibility plays a vital role in the effectiveness of a steganographic system. It is crucial for such systems to ensure that statistical detection methods are unable to detect any hidden secret data. This characteristic allows the confidential information to remain unnoticed and undisclosed, safeguarding its secrecy (Zakaria, et al., 2018). Therefore, if noticeable alterations are found in the stego-image, the potential for compromising the hidden messages becomes higher. In such cases, if the observer can provide evidence confirming the existence of a secret message, it indicates that the steganographic system has been compromised and is no longer considered effective or secure (Chen, et al., 2018).

Most steganographic systems exploit the limitation of the human being's sense in their embedding process without being doubtable or suspicious by the Human Visual System (HVS). Since hiding secret information in a cover image may introduce some noise or modulate this cover image. The embedding process must not degrade the perceived quality of stego-image to get a secure steganographic system (Atawneh, et al., 2017).

The embedding payload refers to the maximum number of bits embedded in a particular image (Zakaria, et al., 2018). Subsequently, to improve a steganography method, it must be considered to increase the amount of confidential data that can conceal without impacting the properties of the stego-image (Atta & Ghanbari, 2018). Security can remain the embedded data intact after joint data processing operations, even if the stego-image undergoes observer attacks (Zakaria, et al., 2018). A steganography algorithm can be considered robust if both the detection and the demolition of the confidential information are too harsh to the attackers (Köhler, et al., 2017).

Improving the steganographic algorithm enhances its properties in terms of steganographic capacity, imperceptibility, and security (Duan, et al., 2020). However, strengthening a particular property may negatively affect others. For instance, the steganographic capacity and undetectability are challenging to maximize simultaneously. The amount of embedded information will directly affect the number of modifications in the cover image during the embedding process (Muhammad, et al., 2015). That means utilizing higher capacity by hiding more data in the cover image produces more modifications, thus degrading the quality of the cover image. In other words, the payload is highly affected by imperceptibility, where the more significant load produces lower

imperceptibility quality and vice versa (Duan, et al., 2020). However, no steganographic system can hide specific cover images without slight effects. Therefore, reducing the probability of detection indicates a better steganography method (Rehman, et al., 2019).

The steganography techniques are categorized in terms of the embedding domain into three categories: Spatial, Transform, and Adaptive domain steganography (Dalal & Juneja, 2021). The spatial domain is the most accessible and most straightforward technique to embed the secret message into the digital image by manipulating the different pixels of the cover image based on intensity values directly (Kadhim, et al., 2018). Examples of spatial domain steganography are LSB scheme (Chan & Cheng, 2004), pixel value differencing (PVD) (Wu & Tsai, 2003), Mapping based Steganography (Wang & Chen, 2006), Palette based Steganography (Fridrich, et al., 2001), Collage Steganography (Shahreza & Shahreza, 2006), Spread Spectrum Image Steganography (SSIS) (Tsai, et al., 2001), and Code-based Steganography scheme (Yu, et al., 2005). Transform domain steganography methods are also known as frequency domain steganography methods. The private message bits get hidden under the frequency coefficients instead of directly embedding the secret message within the cover image. These techniques transform the cover image from spatial domain to frequency domain, and then the secret message bits are embedded into these transformed coefficients (Kadhim, et al., 2018). Unlike spatial domain techniques (based on pixel values that describe the intensity values), the transform domain techniques (based on frequency components) hide the secret information in the significant parts of the cover image (Dalal & Juneja, 2021). There are many transform domain methods such as Discrete Wavelet Transform (DWT) (Nag, et al., 2011), Discrete Cosine Transformation (DCT) (Mali, et al., 2012), Discrete Fourier Transform (DFT)

(Keshari & Modani, 2011), Complex Wavelet Transform (CWT) (Singh & Siddiqui, 2013), Integer Wavelet Transform (IWT) (Raftari & Moghadam, 2012), Dual-tree Complex Wavelet Transform (DTCWT) (Selesnick, et al., 2005), etc. The adaptive steganography improves the performance of steganography by using artificial intelligence in selecting the to-be-modified locations in the cover image pixels adaptively according to the significant characteristics and statistics of the cover image. After the factors and statistics of the cover image are analyzed, a particular mathematical model is utilized. However, any steganography technique is implemented either in the spatial or frequency domains. Hence, the adaptive strategy has presented an additional layer to spatial and frequency domain techniques (Dalal & Juneja, 2021). This research focuses on developing steganographic algorithms in the spatial embedding domain.

Steganalysis is the science of detecting and decoding hidden information within stego-objects and breaking the security of these objects (Dalal & Juneja, 2021). Nonetheless, the primary objective of steganography is to prevent detection of the transmission of a concealed message. With the growing use of steganography techniques, the significance of steganalysis techniques is also becoming more prominent (Douglas, et al., 2017). Generally, most steganographic systems leave some signs behind produced stego-objects; thus, these signs make these objects detectable even though these signs are invisible or indiscernible by humans. If some parts of a cover object are modified, this will affect this object's perceptual and statistical characteristics in some way. Therefore, it can be considered an indicator of hidden information within this object (Attaby, et al., 2017).

1.2 Motivation

Methods for hiding information have been in existence for centuries. Today, the methods under inspection by scholars involve embedding information within digital media, specifically digital images. However, since nothing is perfect, these digital methods have limitations. These limitations can be the entry point for attacks to detect the existence of a secret message. Here comes the role of scholars to analyze loads of these steganography methods. Assessing these attacks allows countermeasures to be developed to protect steganography systems. In addition, understanding the limitations of these methods will allow the construction of more robust strategies that can better survive manipulations and attacks (Tamanna & Sethi, 2017).

The most widely used image steganography method is the LSB embedding, which provides the basic idea of image steganography in a simple way and reasonable embedding capacity. It states that the secret message bit is embedded into the LSB of the cover image pixels (Nag, et al., 2016; Tamanna & Sethi, 2017). Current steganalysis methods reliably detect this technique; the intruder can access the embedded secret data by picking LSBs. Thus, the developed improvements of LSB embedding became the field of interest by scholars (Tamanna & Sethi, 2017).

Furthermore, there was a growth of interest in using the extensions of LSB based image steganography, such as the improved LSB replacement (Chan & Cheng, 2004), LSB matching (LSBM) (Li, et al., 2009), LSBM revised (LSBMR) (Jarno, 2006), and LSBMR edge-adaptive (EA-LSBMR) (Luo, et al., 2010) to overcome the limitations of the simple LSB based image steganography (Nag, et al., 2016; Veena & Arivazhagan, 2018). Recent advancements in this domain include the AVAP method (Pan, et al., 2021),

RPBS method (Ali, et al., 2021), PLS method (Tiwari & Gangurde, 2021), SED method (SolaK & Altinşik, 2019), and LSB with SK method (Amarendra, et al., 2019), reflecting a diversified landscape of innovative approaches aimed at enhancing the security and robustness of steganographic systems.

The primary challenge in steganography lies in preserving the natural appearance and quality of the stego-image. Achieving this involves carefully controlling modifications to pixel values and addressing any introduced distortion during the embedding of hidden information. Distortion can arise from various factors, such as altering pixel intensity or color values, which may result in perceptible changes to the image's visual characteristics. This challenge is crucial as it directly impacts the detectability of concealed information within the image. Analysts reviewing the stego-image may utilize a range of statistical analysis techniques or visual inspection methods to uncover anomalies suggestive of concealed data. Consequently, the overarching objective is to render the hidden data imperceptible, seamlessly integrating it with the image to impede detection efforts and ensure the stego-image remains indistinguishable from an original version. Achieving this degree of imperceptibility demands sophisticated embedding techniques that minimize both the statistical and visual traces of the hidden data while maintaining the image quality.

Consequently, there has been a proposal for modified versions of LSB image steganography methods, which employ adaptive and non-adaptive LSB steganography algorithms that disregard the properties of the cover image. The aim is to bolster security and robustness while still allowing for a significant embedding payload. This approach presents a challenge by aiming to decrease the likelihood of detection through the

reduction of bit-level modifications on pixel values and manipulation of the intensity histogram of the cover image, thus complicating detection efforts.

The selection of a non-adaptive scheme for the proposed algorithms—Pixel Indices Least Significant Bit (PILSB) and Reversible Rewritable Least Significant Bit (RRLSB)—is aligned with the objective of ensuring robust security while maintaining visual consistency. This research highlights the advantages of the non-adaptive approach, particularly in minimizing the number of modified bits to preserve imperceptibility and reduce the risk of detection. In contrast, the adoption of an adaptive scheme in the Semi-Adaptive Least Significant Bit (SDLSB) algorithm reflects a targeted effort to improve adaptability to varying cover image characteristics. By dynamically adjusting the embedding process based on local pixel intensity, SDLSB enhances payload capacity while maintaining a high level of security. Therefore, this research presents a comprehensive embedding framework that strategically combines non-adaptive and adaptive paradigms to achieve a balanced trade-off between efficiency, imperceptibility, and robustness in LSB-based steganography.

The primary aim of this study is to design a customizable steganographic system capable of selecting the most suitable algorithm from three proposed options based on specific requirements such as the cover image size, characteristics, and the secret message size. Additionally, the system evaluates the results of each algorithm by analyzing stego-image quality metrics, as well as conducting statistical and visual analyses. This approach involves careful consideration of various factors to enhance the efficiency of the embedding process, thereby ensuring a superior level of security and imperceptibility. The study addresses three distinct research inquiries focusing on crucial aspects of designing

and implementing the steganographic algorithm, providing valuable insights into its efficacy and functionality.

1.3 Problem Statement

Both adaptive and non-adaptive image steganography algorithms currently face various identified chalenges that necessitate further research investigation. These problems have raised concerns and require careful examination to improve the effectiveness of these algorithms. Additionally, there is a pressing need to develop a customizable steganography application which utilizes the most suitable and effective algorithm to ensure security, stego-image quality, and payload capacity maintenance. Through rigorous requirements analysis and result evaluation, the best algorithm can be determined for application in real-world scenarios. In summary, the key problems that require attention can be outlined as follows:

- **Compromised Security in Non-Adaptive Methods:** A significant challenge lies in the vulnerability of traditional non-adaptive LSB steganography to steganalysis attacks due to predictable embedding patterns and static bit manipulation. These weaknesses make it easier for unauthorized users to detect or extract hidden data. Therefore, it is essential to reinforce these algorithms with more dynamic and unpredictable embedding mechanisms to improve resilience against statistical and structural attacks.

- **Poor Visual Quality of Stego-Images:** Non-adaptive LSB techniques often result in noticeable distortions in the stego-image, especially when embedding large payloads or when changes are concentrated in sensitive visual areas. Enhancing

the visual fidelity of stego-images is critical to maintaining imperceptibility. This necessitates the development of advanced algorithms that can reduce visual artifacts and preserve image quality by minimizing the number of modified bits and targeting less visually sensitive regions.

- **Maintaining Payload Capacity:** Another key challenge is increasing the payload capacity within steganographic frameworks. Traditional methods often encounter limitations in accommodating large-scale data payloads, necessitating the exploration of innovative techniques to enhance embedding efficiency and scalability. This entails the development of adaptive algorithm that can dynamically adjust embedding parameters to accommodate larger data payloads while minimizing distortion and maximizing data concealment capacity. Moreover, the scalability of steganographic algorithms must be enhanced to facilitate the seamless integration of expansive data payloads within the cover image. Achieving this requires a comprehensive understanding of the underlying embedding processes and the development of novel algorithms capable of optimizing the utilization of available embedding space.

- **Trade-Off Between Payload Capacity and Security:** A major limitation of current non-adaptive methods is the inverse relationship between data hiding capacity and security. Increasing the payload often reduces the unpredictability of the embedding pattern, making it more vulnerable to detection. A robust steganographic system must optimize this trade-off by maximizing data embedding while ensuring minimal detectability and high image quality. This calls

for the design of multi-layered or hybrid algorithms that improve both capacity and security simultaneously.

Despite the promising possibilities of both adaptive and non-adaptive LSB steganography techniques, significant challenges persist. These include vulnerabilities in security measures, degradation of stego-image quality, and the inherent trade-off between data concealment and security robustness. A thorough examination of these challenges using a collaborative approach is essential to develop practical solutions that enhance the integrity and usability of LSB steganography algorithms.

In summary, this research addresses the core challenges of compromised security, poor stego-image quality, and the trade-off between payload and imperceptibility, aiming to develop robust, secure, and efficient spatial domain steganographic techniques.

1.4 Research Objectives

The primary objective of this research is to address the inherent limitations of current LSB steganography techniques operating within the spatial domain. These methods commonly grapple with the challenge of striking a delicate balance between stego-image quality, security, and payload capacity. The core objective of this investigation is to refine the efficiency of data embedding within images by minimizing modified bits during the embedding process. This refinement aims to enhance security, stego-image quality, and maintain payload capacity. Achieving these objectives involves developing a customizable application incorporating multiple LSB steganography algorithms. These methodologies will be carefully designed to address various parameters,

such as the size of the secret message, characteristics of the cover image, and other relevant considerations.

To achieve this overall objective, this research will focus on investigating the following specific objectives:

1. **Designing an Index-Based LSB Algorithm to Address Security and Visual Quality:**
    - Design an algorithm that optimizes non-adaptive LSB-based image steganography by incorporating an index in each embedding cycle.
    - Aim to minimize embedding distortion while increasing imperceptibility and enhancing security, especially for short secret messages.
    - Focus on reducing the number of LSB modifications and the bit-level cost of pixel value changes to lower the probability of detection.
    - Address the limitation in current state-of-art methods that degrade stego-image quality.
2. **Designing a Dynamic Intensity-Aware LSB Algorithm to Address Payload Capacity and Visual Quality:**
    - Design a dynamic algorithm for image steganography to increase payload capacity, particularly for large secret message sizes.
    - Ensure stego-image quality is maintained while adapting to the characteristics of the cover image, such as color intensity.
    - Dynamically embed the secret message based on pixel intensity to enhance imperceptibility, security, and payload capacity.

- Overcome the limitations posed by current state-of-the-art methods and supplement the previous algorithm by addressing payload constraints while minimizing the expected modified bits inherited from the previous proposed algorithm.

3. **Designing a Hybrid Two-Layer LSB Algorithm to Address Trade-Off Between Capacity, Security, and Visual Quality:**
    - Design an improved LSB-based image steganography with a spatial domain non-adaptive algorithm.
    - Concentrate on optimizing the trade-off between embedding efficiency, imperceptibility, security, and payload capacity, which represents the most significant challenge in current methods to address.
    - Design an algorithm to minimize the expected number of modified bits per pixel, thereby reducing the visible impact of embedded data on the stego-image.
    - Generate two virtual stego-images to optimize the balance between imperceptibility, security, and payload capacity.
    - Introduce a hybrid approach that combines elements from previous algorithms and addresses limitations in both these algorithms and current-state-of-the-art methods. This overcomes challenges like limited payload and stego-image distortion within a two-layer framework, enhancing imperceptibility, stego-image quality, security, and maintaining payload.
    - Directly address the core limitation of trade-off by balancing capacity, security, and visual quality within a multi-layered approach.

This detailed research plan aims to significantly advance LSB-based image steganography by targeting specific limitations and enhancing imperceptibility, security, and payload capacity through algorithmic enhancements.

1.5 Research Contributions

This research presents a customized application consisting of three algorithms that aim to enhance the imperceptibility, security, and payload capacity of both adaptive and non-adaptive LSB steganography in the spatial domain. These algorithms have been carefully designed to address specific scenarios and adapt to different input parameters, such as the size of the secret message, cover image, and various image characteristics. Each algorithm represents a unique optimization approach that contributes to enhancing the overall quality of the stego-image. These algorithms are important for moving forward our knowledge in this field. It's worth noting that they build upon existing LSB image steganography methods, adding useful improvements. Overall, this research has made significant contributions by introducing new and innovative algorithms and techniques:

1. PILSB is a secure steganographic algorithm based on pixel indices LSB. It enhances embedding efficiency by reducing distortion, improving imperceptibility, and increasing security. It minimizes LSB modifications, making detection less probable specially for short secret messages.

2. SDLSB is an innovative semi-adaptive dynamic steganographic algorithm that enhances LSB replacement in terms of payload and imperceptibility. By decomposing the image into intensity-based non-overlapping blocks and employing a distinct embedding process for each block, SDLSB enables up to three embedded bits per byte while

minimizing the probability of detection. This approach improves the payload capacity while maintaining imperceptibility of the stego-image.

3. The proposed Reversible Rewritable Least Significant Bit (RRLSB) steganographic method enhances embedding efficiency, imperceptibility, security, and payload capacity. Via merging virtual stego-images and using indices and indirect embedding method, it reduces bit modifications, improves imperceptibility, and lowers the probability of detection. Additionally, it expands payload capacity with rewritable LSBs.

1.6 Research Scope

This research is primarily focused on improving Least Significant Bit (LSB) image steganography techniques within the spatial domain. The scope of the study is limited to the design, development, and evaluation of non-adaptive and adaptive LSB-based algorithms aimed at enhancing imperceptibility, payload capacity, and security.

The study encompasses the following specific boundaries and limitations:

- Designing and implementing three steganographic algorithms—PILSB, SDLSB, and RRLSB—each addressing specific limitations of traditional LSB methods, including low embedding efficiency, compromised security, and poor visual fidelity.
- Utilizing 2D digital RGB images of various standard sizes (128×128, 256×256, 512×512, and 1024×1024) as cover media to evaluate the robustness, scalability, and adaptability of the proposed algorithms.
- Embedding secret messages of varying lengths, ranging from 1 KB to 8 KB, in order to test the scalability and payload handling capabilities of the algorithms under different conditions.

- Assessing stego-image quality using objective Image Quality Metrics (IQMs) such as Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), and Structural Similarity Index (SSIM) to measure imperceptibility.
- Evaluating the security of the proposed methods through fundamental steganalysis techniques, including visual inspection, histogram analysis, and RS (Regular/Singular) analysis, to assess resistance to detection.
- The scope is limited to the spatial domain; transform domain techniques (e.g., DCT, DWT), real-time applications, or cryptographic enhancements are not within the scope of this study.
- The evaluation is conducted in a controlled simulation environment using benchmark datasets. Hardware implementation and real-world deployment scenarios are not addressed.

Through this focused scope, the study aims to make a meaningful contribution to the field of spatial domain steganography by offering efficient, secure, and imperceptible data-hiding methods.

1.7 Research Steps

There is a distinction among steganography methods based on how they handle the trade-off between payload capacity and stego-image quality. Some methods prioritize a higher payload, which can lead to more distortion in the resulting stego-images. However, these methods are often considered less valuable (Broda, et al., 2017). On the other hand, successful steganography systems are those that can maximize the payload while preserving the quality of the stego-images (Wazirali, et al., 2019). It is also recognized

that striking a balance between enhancing stego-image quality and maintaining an acceptable payload level is an efficient approach. This contributes significantly to increasing steganographic capacity while keeping the probability of detection unchanged (Wazirali, et al., 2019).

In this study, the main objective is to enhance the embedding efficiency of spatial domain steganography in terms of imperceptibility, security, and payload capacity. The methodology employed for this research focuses on investigating the embedding efficiency and the statistical undetectability of the proposed algorithms. These elements are vital for reaching the intended research goals. Figure 1.1 visually represents the different phases of this study.

The overall design and flow process of the research is depicted in Figure 1.1. It outlines how the research problem is identified and the path taken to achieve the research objectives. The first step in problem-solving is recognizing and defining the problem. Here, the issue is identified as the flaws and limitations of current digital image spatial steganography methods.

Following problem identification, the next step is to develop algorithms aimed at resolving the existing drawbacks in current techniques and producing competitive outcomes. provide the basis for the next steps in the research process. Afterward, the implementation of these algorithms, which leads to the evaluation stage, marking the final phase of the research.

The evaluation stage is divided into two parts: performance evaluation and assessment of security. It involves analyzing and evaluating the results obtained from

implementing the proposed algorithms. The success of the proposed algorithms is determined based on their performance in achieving the desired research objectives.

Overall, Figure 1.1 provides an overview of the research design and flow process, showcasing the systematic approach taken to address the identified problem and evaluate the effectiveness of the proposed algorithms.

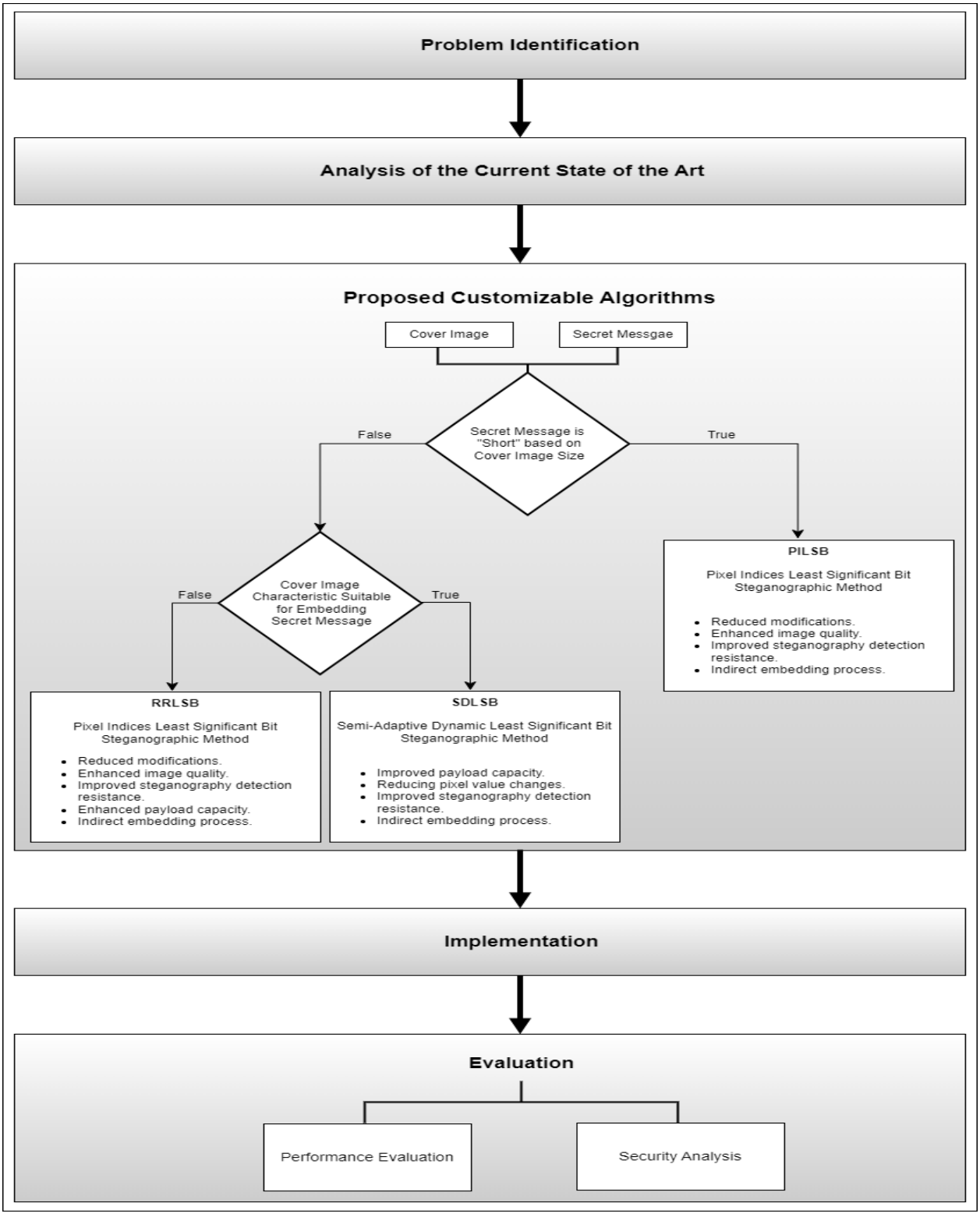

Figure 1.1 The research methodology framework

1.7.1 Problem Identification

The research problem in both adaptive and non-adaptive LSB steganography revolves around improving the security and robustness of the steganographic systems. This includes minimizing the probability of detection by reducing the number of bit-level modifications on pixel values and altering the intensity histogram of the cover image, thereby making the detection of hidden data more challenging for potential adversaries.

Another significant aspect is the trade-off between embedding a high payload and the resulting image distortion. It is imperative to develop a solution that enables the hiding of a significant amount of data within a digital image while minimizing both perceptual and statistical degradation in the quality of the resulting stego-image. Additionally, the ease of detecting secret data through LSB analysis highlights the need for improved LSB embedding algorithms.

The main research challenge lies in developing steganographic algorithms that can improve the stego-image by reducing the number of modified bits. This involves finding methods that can effectively maintain imperceptibility and statistical properties of the cover image while maintaining the payload capacity.

Overall, the research aims to address the identified problem by developing novel LSB steganography algorithms, both adaptive and non-adaptive, designed to enhance embedding efficiency, preserve image quality, and bolster the security and robustness of the steganographic system.

1.7.2 Analysis of Current Techniques

In the field of image LSB steganography, numerous methods have been proposed to enhance the hiding of data within images. It is crucial to examine these existing techniques and identify their drawbacks and limitations in order to develop improved algorithms for embedding payload and enhancing image quality.

Spatial domain techniques involve direct manipulation of pixels or bits within an image to enhance its quality. This approach offers the advantage of lower execution time while achieving a high embedding rate (Jeevitha & Prabha, 2018). However, these techniques are relatively simple in terms of embedding and extraction complexity and suffer from a significant drawback, which is the introduction of additive noise into the image. This noise has a direct impact on the Peak Signal to Noise Ratio (PSNR) and the statistical properties of the image (Awe, et al., 2020).

One of the widely utilized methods in spatial domain steganography is the LSB technique, which allows for a large amount of data to be stored in the image without significant degradation of the original image. However, this technique has limitations such as manipulating the image using LSB may result in data loss. Additionally, the hidden data can be easily destroyed by simple attacks or intrusions (Rashid & Arora, 2021).

Overall, while spatial domain techniques provide a way to achieve high data capacity and message integrity, they also face challenges such as additive noise and susceptibility to attacks. Addressing these issues is crucial to improving the robustness and security of the steganographic system.

To overcome these limitations, this research will focus on studying the existing methods, understanding their drawbacks, and developing novel algorithms that can improve the stego-image quality. The aim is to advance the field and enhance the security and robustness of steganographic systems.

1.7.3 Proposed Algorithms

This section introduces novel algorithms in LSB image steganography in the spatial domain, addressing the limitations of current techniques. The objective is to improve embedding efficiency by reducing the number of LSB modifications and minimizing the bit-level cost of pixel value changes, thus lowering the probability of detection. The proposed algorithms, namely PILSB, SDLSB, and RRLSB, are customizable options designed to address specific input parameters.

These algorithms are shown in Figure 1.2 and are subjected to analysis and evaluation in this research. By employing LSB embedding methods, they constitute a fundamental framework for the subsequent examination and evaluation of their effectiveness in achieving the research goals.

Each proposed algorithm comprises two main phases: embedding and extraction. The first algorithm, PILSB, initiates the embedding phase by converting the cover image into a binary representation and transforming the secret message into corresponding secret message bits. The embedding process involves selecting specific pixels and embedding two secret message bits by comparing them with the LSB values of the red and green bytes. A match/mismatch table is utilized to determine the modified bits for each selected

pixel. Furthermore, the LSB of the blue byte is employed to embed the index. At the conclusion of this phase, the stego-image and private key are generated.

Subsequently, the extraction phase begins by verifying the correctness of the secret key. Upon successful authentication, the location of the embedded secret message is determined. The stego-image is then converted into a binary image for further analysis. The analysis is conducted on each selected pixel, where the index value stored in the LSB of the blue byte is examined to determine the actual secret message values embedded in the LSBs of the red and green bytes. This process allows for the complete extraction of the message.

The PILSB algorithm discussed in this study presents a secure approach for embedding and extracting secret messages using steganography. It offers an efficient solution, particularly when dealing with small secret message sizes. The PILSB algorithm, can effectively hide secret data within images while preserving the overall stego-image quality and appearance of the original image. This algorithm offers a valuable method for secure communication, enabling the confidential transmission of data while ensuring that the stego-image remains inconspicuous.