ENHANCED STEGANOGRAPHY FRAMEWORK BASED ON LOSSLESS COMPRESSION AND HISTOGRAM

DIMA SULIMAN MOHAMMAD KASASBEH

UNIVERSITI SAINS MALAYSIA

2024

ENHANCED STEGANOGRAPHY FRAMEWORK BASED ON LOSSLESS COMPRESSION AND HISTOGRAM

by

DIMA SULIMAN MOHAMMAD KASASBEH

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

July 2024

ACKNOWLEDGEMENT

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

﴿يَرْفَعِ اللَّهُ الَّذِينَ آمَنُوا مِنكُمْ وَالَّذِينَ أُوتُوا الْعِلْمَ دَرَجَاتٍ ۚ وَاللَّهُ بِمَا تَعْمَلُونَ خَبِيرٌ{11} ﴾ سورة المجادلة

First and foremost, praise and thanks are due to Allah (SWT), who humbly deserves my unending thanks and praise for his countless blessings, and peace and blessings be upon his Messenger, Mohammed (Peace Be Upon Him).

I would like to take this opportunity to express my sincere gratitude and appreciation to my supervisor, Dr. Mohammed Anbar, for all his encouragement, continuous support, efforts, and insightful advice he gave me throughout my research period.

Additionally, I want to express my gratitude and thanks to my first supporter and helper throughout this journey, my husband, for his never-ending encouragement. I have never forgotten the heartfelt thanks to my children, Yara, Siwar, and Sanad—those little hands that rose to the sky and gave me prayers. Their love and encouragement have been invaluable and a constant source of motivation for me, pushing me to strive for excellence in my research. I am truly blessed to have such a loving and supportive family by my side.

Finally, I would be remiss in not mentioning my dear parents. Words cannot express my gratitude for their infinite encouragement and continuous support in every step of my life. Their unwavering belief in me has been the driving force behind my achievements. Their love and guidance have been invaluable, and I am forever indebted to them for their unwavering dedication. Without them, I could not have been here.

TABLE OF CONTENTS

LIST OF TABLES

Page

LIST OF FIGURES

Page

LIST OF ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
BPC	Bits Per Character
CPR	Cumulative Peak Regions
CR	Compression Ratio
DCT	Discrete Cosine Transform
DEPE	Directional Enclosed Prediction and Expansion
DPEH	Directional Prediction Error Histogram
EC	Embedding Capacity
HVS	Human Visual System
IF	Image Fidelity
LC	Local Complexity
LSB	Least Significant Bit
MSB	Most Significant Bit
MSE	Main Squared Error
PEH	Prediction Error Histogram
PSNR	Peak Signal-To-Noise Ratio
QHCT	Quaternary Huffman Compression Technique
QHT	Quaternary Huffman Tree
RDH	Reversible Data Hiding
RGB	Red, Green and Blue
RGB_CST	RGB Channel Selection Technique
RMSE	Root Mean Square Error
SNR	Signal-To-Noise Ratio
SP	Saving Percentage
SSIM	Structural Similarity Index Measure
2D-PEH	2-Dimensional Prediction Error Histogram

LIST OF APPENDICES

KERANGKA KERJA STEGANOGRAFI YANG DIPERTINGKATKAN BERDASARKAN PEMAMPATAN TAK HILANG DAN HISTOGRAM

ABSTRAK

Steganografi adalah teknik keselamatan siber yang berkesan yang memudahkan komunikasi terselindung dengan menyembunyikan kewujudan maklumat dalam gambar palsu. Perdagangan antara kapasiti penggabungan, tak nyata, dan kebalikan telah membawa cabaran baru dalam steganografi. Menyeimbangkan faktor-faktor ini adalah penting dan penting untuk pembangunan steganografi yang berkesan. Tesis ini bertujuan untuk mencadangkan teknik steganografi yang ditingkatkan untuk meningkatkan kapasiti penggabungan, mengekalkan ketaknyataan, dan mencapai kebalikan. Tiga model telah dicadangkan: pengekalan, generasi peta penggabungan, dan steganografi yang boleh dibalikkan. Dalam model pengekalan, teknik pengekalan teks tanpa kehilangan hibrid telah dicadangkan untuk menghapuskan kelebihan maklumat rahsia, dengan demikian meningkatkan kapasiti penggabungan. Dalam Model Generasi Peta Penggabungan, dua teknik telah dicadangkan untuk menentukan saluran RGB terbaik dan menghasilkan peta lokasi penggabungan sebelum proses penggabungan sebenar. Dalam model steganografi yang boleh dibalikkan, proses penggabungan 3D dicadangkan. Ia menyembunyikan aliran bit yang dipampatkan dalam 2D-PEH dengan nilai kompleksiti tempatan yang lebih rendah. Tambahan pula, ia menyembunyikan kunci pengekalan bersama-sama dengan parameter pengekstrakan lain menggunakan peta lokasi penggabungan yang dihasilkan. Prestasi teknik yang dicadangkan dinilai secara eksperimen untuk menentukan kapasiti penggabungan, tak nyata, dan kebalikan. Keputusan eksperimen menunjukkan teknik steganografi yang ditingkatkan yang dicadangkan melebihi teknik terkini seperti Penyekatan Penggabungan Tepi BTC (ABTC-EQ) dan teknik

Fungsi Modulus dan Perbezaan Nilai Pixel (PVDMF), dengan demikian menyelesaikan cabaran dan batasan yang ada. Model Pengekalan yang dicadangkan telah menunjukkan hasil yang menjanjikan dari segi nisbah pengekalan dengan purata 0.161 dan peratusan penjimatan dengan purata 84.90%. Selain itu, Model Steganografi yang Boleh Dibalikkan yang dicadangkan telah mencapai peningkatan yang signifikan berbanding teknik steganografi yang boleh dibalikkan yang sedia ada seperti Pasangan PEE dan Pergeseran Histogram Terpelintir (SHS). Ketahanan teknik yang dicadangkan diuji terhadap sistem visual manusia (HVS) dan serangan histogram. Nilai PSNR yang dicapai lebih tinggi daripada 66.84 dB, menunjukkan ketaknyataan yang lebih tinggi. Selain itu, ia mengekalkan kapasiti penggabungan yang tinggi sehingga 3.53 Mbytes berbanding teknik steganografi yang sedia ada.

ENHANCED STEGANOGRAPHY FRAMEWORK BASED ON LOSSLESS COMPRESSION AND HISTOGRAM

ABSTRACT

Steganography is an effective cybersecurity technique that facilitates covert communication by hiding information's existence within a spoof image. The trade-off between embedding capacity, imperceptibility, and reversibility has presented a new challenge in steganography. Balancing these factors is crucial and essential for the development of effective steganography. This thesis proposes an enhanced steganography framework to increase embedding capacity, maintain imperceptibility, and achieve reversibility. Three models were proposed: compression, embedding map generation, and reversible steganography. The compression model was modified to include a hybrid lossless text compression algorithm to reduce redundant secret information and boost embedding capacity. The Embedding Map Generation Model proposed two techniques to determine the best RGB channels and generate the embedding location map before the embedding process. In the reversible steganography model, a 3D embedding process is proposed. It hides compressed bitstreams in the 2D-PEH with a lower local complexity value. Additionally, it hides decompression keys along with other extraction parameters using the generated embedding location map. The performance of the proposed technique was experimentally assessed to determine embedding capacity, imperceptibility, and reversibility. The experimental results show that the proposed enhanced steganography framework outperformed state-of-the-art techniques such as Adaptive BTC Edge Quantization (ABTC-EQ) and Pixel Value Differencing and Modulus Function (PVDMF) techniques, consequently resolving the existing challenges and limitations. The proposed compression Model has demonstrated promising outcomes

regarding compression ratio, with an average of 0.161 and a saving percentage of 84.90%. Furthermore, the proposed Reversible Steganography Model has significantly improved existing reversible steganography techniques like pairwise PEE and Skewed Histogram Shifting (SHS). The resistance of the proposed technique was tested against human visual systems (HVS) and histogram attacks. The achieved PSNR value is higher than 66.84 dB, demonstrating higher imperceptibility. Additionally, it retains a high embedding capacity of up to 3.53 Mbytes compared to existing steganography techniques.

CHAPTER 1

INTRODUCTION

1.1 Overview

The digital revolution is greatly increasing the exchange of digital information worldwide in our daily lives. The sharing of digital information is crucial across various fields like science, education, commerce, and entertainment. However, eavesdroppers and attackers pose threats by trying to gain unauthorized access to this data, especially over public networks. Such attacks, known as cyberattacks, aim to access, modify, or destroy sensitive information that raises concerns about privacy and security. Therefore, dealing with cyberattacks is a key challenge in securely transmitting digital information and requires careful attention (Pramanik et al.,2022; Kumar et al., 2022).

Researchers in the field of cybersecurity have devised various techniques to protect transmitted digital information and address emerging problems of digital information security. These techniques include using secure protocols, cryptography algorithms, steganography, strong passwords, regularly updated software, and antivirus programs. Implementing these security measures in digital environments is paramount to ensuring the confidentiality, integrity, and availability of digital information, effectively safeguarding against cyberattacks, and upholding privacy and security. Additionally, educating individuals on safe online practices can also help reduce the risk of cyber threats (Giri et al., 2021; Pramanik et al., 2022).

Secure protocols like HTTPS and SSH play a crucial role in safeguarding digital information from cyber threats by encrypting data exchanged over networks and ensuring only authorized parties can decrypt sensitive information. Cryptography algorithms like AES and RSA provide robust protection for data at rest and in transit,

transforming it into unreadable formats that enhance security against unauthorized access (Prasad & Rohokale, 2020; Pramanik et al., 2022).

Additionally, strong passwords are vital for access control, preventing unauthorized entry into systems or accounts. Complex passwords, updated regularly and incorporating letters, numbers, and symbols, enhance security by reducing vulnerability to brute-force attacks. Furthermore, regular software updates and antivirus programs are crucial proactive measures for mitigating security risks. These updates address vulnerabilities, minimizing the potential for exploitation by attackers, while antivirus software provides real-time protection against malware, viruses, and other cyber threats (Giri et al., 2021; Prasad & Rohokale, 2020).

Steganography has gained significant popularity due to its ability to hide sensitive data within innocuous files, which extends to facilitating secret information exchange through various platforms like mobile devices, IP cameras, and social media applications such as WhatsApp, Instagram, and Snapchat (Giri et al., 2021; Pramanik et al., 2022). In steganography, hiding is critical for maintaining data confidentiality and security by concealing secret information within seemingly ordinary carrier files like images, audio, or videos. This hidden data remains undetectable to unauthorized entities, ensuring privacy and confidentiality during data storage and transmission and adding an extra layer of security that makes it difficult for attackers or unauthorized parties to intercept or access sensitive information (Prasad & Rohokale, 2020; Pramanik et al., 2022; Geetha et al., 2023).

However, steganography techniques frequently suffer from embedding capacity limitations, which can restrict the amount of data that can be hidden within a carrier image. This limitation arises from the need to maintain the visual or statistical properties of the carrier image to avoid detection. Additionally, imperceptibility poses

a concern, as any noticeable alterations to the carrier image may raise suspicion and defeat the purpose of covert communication (Megías et al., 2022; Geetha et al., 2023).

Compression is necessary primarily for optimizing storage space and reducing bandwidth usage. By compressing data, redundant or unnecessary information is removed or represented more efficiently, resulting in smaller file sizes. This is particularly crucial in today's digital landscape, where vast amounts of data are generated and transmitted daily. Compression techniques like lossless and lossy compression help in storing and transferring data more effectively, saving storage costs and improving data transmission (Sayood, 2018; Bull & Zhang, 2021).

Reversibility is another challenge that steganography techniques encounter, as the process of extracting hidden information from a carrier image without any loss or alteration can be difficult. Furthermore, steganography techniques can also be used for illegitimate purposes, such as hiding malware or sensitive information within innocent-looking files. This can be a significant security concern, as it allows attackers to bypass traditional security measures and potentially carry out covert operations undetected (Kumar et al., 2022; Megías et al., 2022).

1.2 Background

This section provides an overview of steganography and its challenges, as shown in Section 1.2.1 and Section 1.2.2, respectively.

1.2.1 Steganography

The history of steganography can be traced back to ancient civilizations, even though the name is modern. Methods such as engraving secret information on the sender's head, tattooing it on their bodies, writing in invisible ink, and engraving on wood then covering it with wax were all used in the past (Giri et al., 2021; Li et al.,

2021; Kumar et al., 2022). Steganography has evolved to incorporate modern technologies and applications that help keep private information safe. However, hackers and attackers still succeed in violating the security of exchanged information by exploiting vulnerabilities in communication systems and employing steganalysis attacks (Giri et al., 2021; Megías et al., 2022).

Steganography safeguards the security and privacy of transmitted information. Steganography techniques conceal the existence of the transmitted information within seemingly innocuous digital files. These files can encompass various multimedia types, including audio, video, and images. The concealment process makes it challenging for unauthorized individuals to detect the presence of hidden information, as it appears as normal content to the naked eye or standard analysis tools. Employing steganography enables communication parties to securely transmit classified information or protect sensitive data from potential breaches, thus enhancing overall information protection measures (Pramanik et al., 2022; Megías et al., 2022; Geetha et al., 2023).

Steganography is the art of concealing the existence of secret information within a deceptive carrier medium. The steganography technique involves three main stages: embedding, distribution, and extraction. In the embedding stage (which may include an optional secret key), the embedding algorithm utilizes the predefined secret key (if applicable) to hide the secret information in a manner that renders it impossible to retrieve. The embedding algorithm produces a stego-medium, which is then transmitted via communication channels.

Furthermore, the cover medium, also known as the carrier medium, serves as a distraction to camouflage the secret information content among its bits. The embedding algorithm substitutes unused or unimportant bits with secret information

bits. This effectively conceals the presence of the secret information within the carrier medium to prevent its detection (Fridrich, 2009; Megías et al., 2022).

In the extraction stage at the receiver's side, the extraction algorithm is employed to retrieve the hidden secret information from the stego-medium using the same secret key (Fridrich, 2009; Kadhim et al., 2019).

Figure 1.1 illustrates a steganography model depicted as a block diagram. In this model, the original carrier medium format, such as a digital image, serves as the platform for concealing secret information, provided a predetermined secret key is in place.

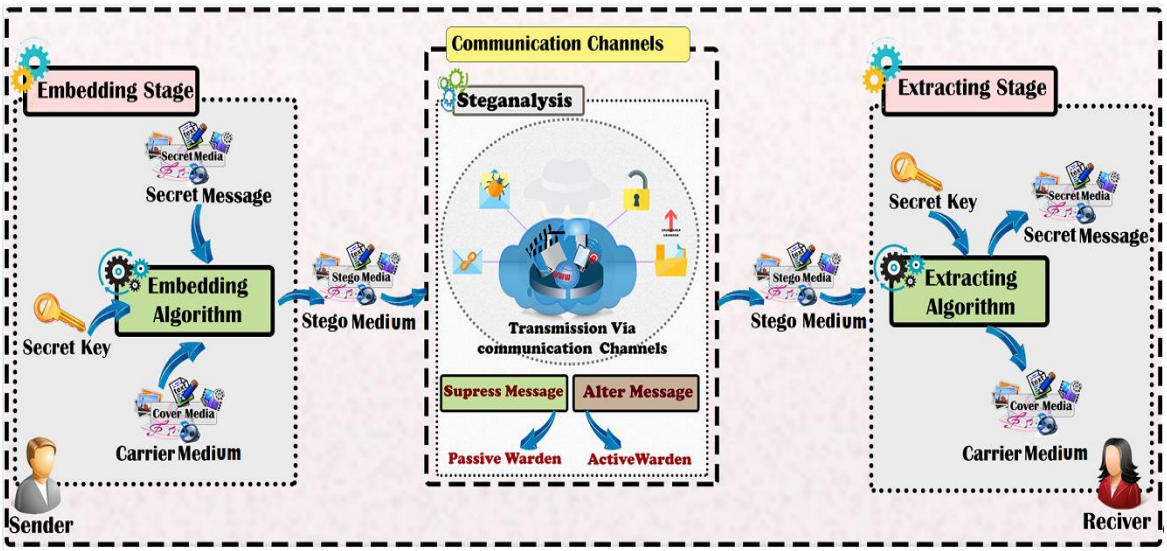

Figure 1.1 Steganography Model Block Diagram

As shown in Figure 1.1, the embedding process involves hiding the secret information within the carrier medium, resulting in a digital stego-medium file. This file is then transmitted through communication channels. The model comprises three primary stages: the embedding stage at the sender's end, the distribution stage through communication channels, and the extraction stage at the receiver's end.

Furthermore, the steganalysis technique analyzes embedding distortions and statistical artifacts in the stego-medium to determine the embedding algorithm's fracture, aiding the warden in extracting secret information. If embeds are suspected,

the technique performs either passive or active warden functions, depending on the warden model. Passive wardens suppress or ignore stego-medium, while active wardens alter messages to foil the escape plan (Prasad and Rohokale, 2020; Giri et al., 2021).

1.2.2 Steganography Challenges

Steganography faces significant challenges due to its core requirements: embedding capacity, imperceptibility, and reversibility. Embedding capacity refers to how much secret information can be hidden within the carrier image, while imperceptibility ensures minimal distortion when hiding information. Imperceptibility aims to make the hidden data undetectable by human senses or statistical analysis, maintaining the cover image's quality (Giri et al., 2021; Megías et al., 2022). Reversibility is crucial for accurately extracting hidden information from the stego medium without loss or corruption (Kadhim et al., 2019; Giri et al., 2021).

The trade-off between embedding capacity and imperceptibility presents a significant challenge in steganography techniques. Firstly, it's challenging to embed a substantial amount of secret data without significantly altering the carrier image. Secondly, there's a need to ensure that the embedded data remains undetectable to human senses or automated detection tools. Lastly, the ability to recover the original secret information from the stego-image without any loss or corruption is crucial. Thus, finding the right balance among these factors is essential for developing an effective steganography technique (Fridrich, 2009; Kadhim et al., 2019; Megías et al., 2022).

Additionally, techniques for accurately extracting hidden information while preserving its integrity are vital. However, developing these techniques is challenging as they require a delicate balance between embedding capacity and imperceptibility.

Attempting to solve one problem separately often exacerbates another (Hashim et al., 2018; Kadhim et al., 2019). The embedding process introduces noticeable distortion in the carrier image, which attackers can exploit by identifying irregularities in the image histogram and quality distortions, potentially revealing the presence of hidden information (Kadhim et al., 2019; Giri et al., 2021; Kumar et al., 2022).

Balancing the trade-off between embedding capacity and imperceptibility is crucial to ensuring the practicality and reliability of steganography techniques. This balance is essential for guaranteeing imperceptibility while maximizing embedding capacity and maintaining a high level of security in information exchange. These requirements are interconnected, as increasing embedding capacity often comes at the expense of imperceptibility, making it challenging to achieve both simultaneously (Kadhim et al., 2019; Megías et al., 2022).

1.3 Research Motivation

The motivations behind steganography techniques for various communication applications are multifaceted, addressing the evolving demands of secure communication (Kadhim et al., 2019; Giri et al., 2021). These motivations stem from a complex interplay of security demands, coupled with the expanding volume of information being transmitted, privacy concerns, and technological possibilities, influenced by the evolving landscape of communication needs.

The first motivation is to conceal the presence of secret information within an innocent carrier image, preventing unauthorized individuals from detecting its existence. Steganography also offers a secure method of transmitting sensitive information over public channels, which is crucial for maintaining trust and confidentiality, especially in high-stakes sectors like government, healthcare, finance,

and defense. However, attackers may use sophisticated methods to detect hidden information, posing challenges to the security of steganographic communication.

The second motivation is the desire for covert communication to bypass censorship or surveillance measures, allowing secret information exchange without arousing suspicion, attracting attention, or triggering censorship filters. Steganography techniques provide tailored solutions to the complex challenges and requirements of diverse communication scenarios, utilizing hidden communication methods (Giri et al., 2021; Pramanik et al., 2022).

1.4 Problem Statement

The existing steganography techniques confront several interconnected challenges that need to be overcome. In this research, the problem statement is summarized as follows:

1. The existing steganography techniques to overcome the high embedding capacity, including those utilizing data compression, overlook the carrier image characteristics and attributes, such as pixel local complexity and color channel attributes, to enhance embedding capacity.
2. The existing steganography techniques to overcome imperceptibility suffer from decreased embedding capacity, lack standardized guidelines for color channel selection, and do not consider channel capacity, susceptibility to noise, or overall image quality, leading to decreased imperceptibility.
3. The existing steganography techniques to overcome the reversibility challenge suffer from decreased imperceptibility and embedding capacity due to the need to embed additional information to identify the embedding location map, which decreases the size of the embedded secret information.

1.5 Research Objectives

The main goal of this research is to propose an enhanced steganography framework that increases embedding capacity and achieves imperceptibility and reversibility. The proposed technique accomplishes the following objectives:

1. To propose a compression model based on pattern matching dictionary and quaternary Huffman coding and leverage carrier image characteristics and attributes, such as local pixel complexity and color channel properties, to enhance embedding capacity.
2. To design a model based on the effective RGB color channel selection and embedding location map generation to maintain imperceptibility while preserving embedding capacity.
3. To propose a reversible steganography model based on the cumulative peak bins in the histogram of directional prediction error to achieve reversibility without embedding extra information for the location map.

1.6 Research Scope and Limitations

This research focuses on an enhanced steganography framework to increase embedding capacity, maintain imperceptibility, and achieve reversibility. Specifically, it involves concealing digital text within a digital image as the carrier media object. Within the scope of steganography techniques, time complexity plays a crucial role, representing the computational resources needed for various operations during the embedding and extraction of hidden information within digital media. Time complexity encompasses the efficiency analysis of algorithms used for compression, decompression, and data manipulation throughout the steganographic process. This evaluation includes measuring the time taken by embedding algorithms to hide

information within cover media and the time needed for extraction algorithms to retrieve the concealed data. Assessing time complexity aids researchers in understanding the computational burden associated with different steganographic approaches, facilitating the selection of techniques that strike a balance between performance and resource utilization. The following scope and limitations of this research have emerged:

1. The scope of the proposed compression model is limited to ASCII text files and evaluated using 14 standard files from the Calgary Corpus dataset. Evaluation is based on several space efficiency factors, including the compression ratio, number of bits per character, and saving percentage. However, time complexity, speed evaluation, and comparison with other studies are not considered.
2. The evaluation of the proposed reversible steganography model is conducted using standardized 512 × 512 RGB color images sourced from the USC-SIPI image database. The evaluation employs common evaluation matrics and widely used measuring tools for image quality assessment.
3. The evaluation metrics used include compression ratio, saving percentage, peak signal-to-noise ratio (PSNR), embedding capacity, bits per pixel, and mean square error (MSE). Additionally, the robustness of the proposed steganography technique against histogram attacks and HVS attacks is tested. However, time complexity, speed evaluation, and image manipulation (e.g., zooming, rotation, scaling.) are not considered and compared with other state-of-the-art studies.
4. The hiding of the compressed information within the carrier image is executed while considering the conditions of the proposed reversible steganography model, which relies on the decompression keys.

1.7 Research Contributions

The contributions of this research are distributed among the three main models: Data Compression model, the Embedding Map Generation model, and the Reversible Steganography model, as follows:

1. Compression Model offers the following key features: a hybrid Lossless Digital Text Compression Technique that reduces the size of secret information, crucial for boosting embedding capacity by eliminating redundancy in the secret data. Furthermore, it generates decompression keys at the sender's end, which are then utilized at the receiver's end to decompress extracted bitstreams without requiring the reconstruction of the Huffman quaternary tree.
2. Embedding Map Generation Model offers the following key features: a novel embedding location map generation technique that identifies embedding locations within the RGB carrier image without requiring additional information sharing. Additionally, it establishes assumptions and basic rules to determine the most efficient RGB color channels for concealing the compressed bitstreams, decompression keys, and other extraction parameters generated by the first model.
3. Reversible Steganography Model offers the following key features: a new adaptive reversible steganography technique for concealing compressed bitstreams in the 2D-DPEH. This technique utilizes DPEH with a lower local complexity value to prevent underflow and overflow problems. The model fulfills multiple security requirements, including information secrecy by hiding its presence in a spoof carrier image, resilience to signal processing attacks by minimizing modifications to the carrier image histogram, a large payload size enabled by using cumulative peak regions instead of a single peak point, and high quality of resulting stego images.

1.8 Research Steps

The proposed steganography technique introduces an enhanced method based on compression and the prediction error histogram of effective color channels. This research follows the basic stages of the scientific research methodology to enhance understanding of the main problem, conduct effective research, and ultimately achieve a comprehensive and efficient solution. The research progresses through five stages, as depicted in Figure 1.2 , providing an overview of the methodology involved in this study..

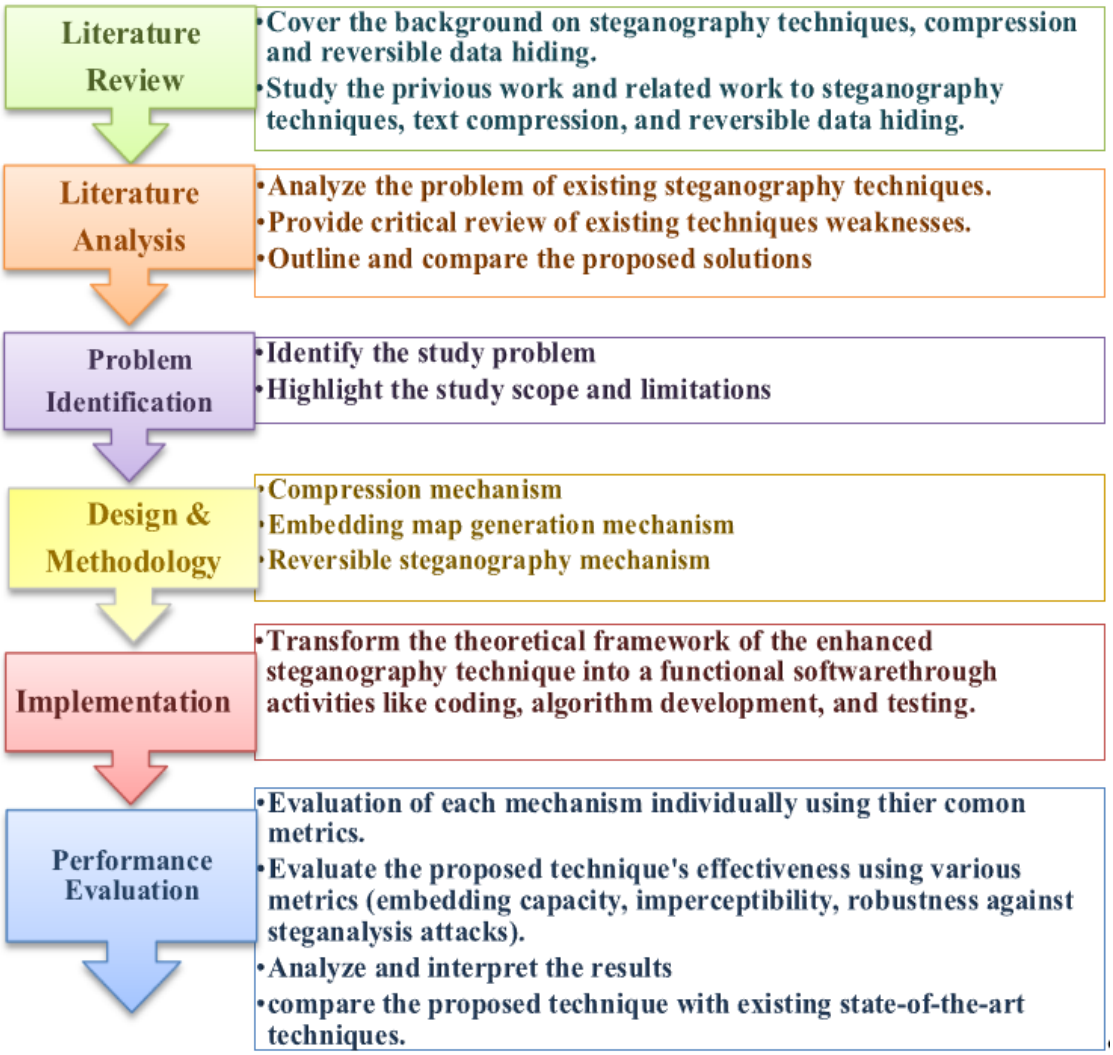

Figure 1.2 Overview of Research Methodology Stages for Enhanced Steganography Technique.

As depicted in Figure 1.2, the first stage involves conducting a literature review, which includes gathering background information on steganography techniques, text compression, and reversible data hiding. This stage also involves analyzing existing literature to identify their limitations and challenges.

The second stage, termed literature analysis, delves into examining the drawbacks of existing steganography techniques to pinpoint their main issues and challenges. This analysis includes comparative assessments for a thorough evaluation.

The third stage focuses on identifying the research problem statement, defining the research's scope and limitations, and formulating a hypothesis based on the identified problem and research objectives. This stage is crucial for establishing a solid methodological foundation to address the problem effectively.

The fourth stage outlines the design and methodology of the proposed enhanced steganography technique, which is based on compression and prediction error histograms. This stage encompasses three integrated models: the compression model, the embedding map generation model, and the reversible steganography model.

Finally, the implementation stage involves translating the theoretical framework of the enhanced steganography framework into functional software. This process includes writing and testing code, developing algorithms, and creating testing scenarios. Initially, each model is implemented independently, followed by their integration to form the complete technique.

The evaluation phase includes individual assessments of each model, along with comparisons against existing state-of-the-art techniques. The compression model's evaluation focuses on three key performance metrics for data compression

efficiency: the compression ratio, saving percentage, and bits per character (BPC). To conduct this evaluation, 14 standard files from the Calgary Corpus and ten additional large text files from various sources were used to gauge the proposed compression model's performance.

For the reversible steganography model, performance evaluation centres on two metrics: embedding capacity, indicating the number of hidden bits in the carrier image, and stego image quality assessed through Peak Signal-to-Noise Ratio (PSNR). Eight standard 512 × 512 RGB color images, such as Lena, Baboon, and Airplane, were employed as carrier images for this assessment.

Additionally, this phase includes detailed discussions of each model, an analysis of simulation results, and a comparison with current state-of-the-art techniques regarding performance and quality criteria. Subsequently, the proposed enhanced steganography framework is elaborated upon, presenting, and analyzing simulation results.

Finally, the technique undergoes evaluation and testing against histogram attacks and Human Visual System (HVS) attacks to assess its robustness and security aspects.

1.9 Thesis Outlines

The thesis is structured into six chapters as follows: Chapter 2 delves into the latest advancements and relevant works in steganography techniques, steganalysis, and data compression, outlining their respective strengths and limitations.

Chapter 3 elucidates the methodology and design of the proposed enhanced steganography technique, offering a comprehensive explanation of the three models' design.

Chapter 4 elaborates on the implementation specifics of the proposed models (compression, embedding map generation, and reversible steganography) to realize the enhanced steganography technique.

In Chapter 5, the experimental findings for each model are presented and discussed, focusing on their performance evaluation and comparisons with existing schemes. Additionally, the experimental results for the proposed technique are detailed, including assessments using various digital images and text files, alongside comparisons with existing schemes. Furthermore, the performance evaluation of the developed technique against different attacks is highlighted, emphasizing the achieved results.

Lastly, Chapter 6 encapsulates the conclusion and offers recommendations for future research endeavours.

CHAPTER 2

LITERATURE REVIEW

This chapter comprehensively reviews steganography and data compression literature, specifically focusing on image and text data compression techniques. It aims to thoroughly understand the research conducted in this field, highlighting the proposed approaches and techniques. Additionally, the chapter aims to identify any gaps or areas for further research to contribute to advancing image steganography techniques.

This chapter is structured as follows: Section 2.1 offers a detailed discussion of steganography and its various techniques related to image steganography, while Section 2.2. provides a brief overview of steganalysis. Section 2.3 provides a brief overview of steganalysis. The research gap and discussion are presented in Section 2.1.3. Section 2.4 gives a comprehensive overview of the preliminary background of the proposed technique. Section 2.5 shows the related techniques for the proposed data compression model, embedding map generation model, reversibility steganography model, and techniques that combine steganography and compression. Finally, Section 2.6 provides a summary of the chapter.

2.1 Steganography

Steganography, derived from the Greek words stegános, meaning covered, and graphia, meaning writing, literally translates to "covered writing." It encompasses the art and science of communicating in a manner that hides the existence of the communication itself. The term steganography reflects the process of concealing hidden writing, as linguistically seen in Greek. This interdisciplinary field integrates theoretical and practical data compression, signal processing, coding, and human visual perception

(Giri et al., 2021; Megías et al., 2022). The steganography technique consists of three main components:

- ***Carrier image***, a cover or host image, is utilised to conceal secret information within its bits. This approach enhances efficiency and deters tampering by modifying the carrier image bits, ensuring imperceptible manipulations.
- ***Secret information*** is digital text transmitted through communication channels, necessitating transformation to be seamlessly hidden while preserving the appearance and format of the carrier image.
- ***Stego image*** refers to the carrier image after the secret information has been concealed within its content.

Digital text comprises characters and symbols, each represented by binary bit code words, and utilizes various fonts and sizes for effective presentation in digital multimedia software. Different typefaces within digital multimedia are tailored for displaying alphabetic characters, numbers, and special symbols (Fridrich, 2009; Li et al., 2021).

The binary code representation adheres to standard character-encoding schemes, with ASCII and Unicode being predominant. ASCII encompasses 128 characters and symbols encoded using a 7-bit binary representation, facilitating the processing, storage, transmission, and display of digital text. Extended ASCII extends this with 128 additional characters, employing an 8-bit binary representation known as ALT codes, totalling 256 symbols and characters (Fridrich, 2009; Li et al., 2021).

A digital image is a numerical representation of a two-dimensional binary matrix comprising individual image elements, with each pixel describing characteristics like resolution, brightness, and color. Pixels, the smallest addressable elements, are

associated with both location and color components, the latter determined by red, green, and blue values in the RGB color model (Jackson, 2015; Nixon, 2020).

This model enables the mathematical description of consistent colors, expressing any perceived color as a combination of these values. The digital image matrix records color information, with pixels arranged in rows and columns corresponding to their positions in the image. The pixel array, with its fixed width and height, can accommodate various color ranges based on the image type (Jackson, 2015; Nixon, 2020). Figure 2.1 Illustrator R (Red), G (Green), and B (Blue) color component ordering on each axis for the 24-bits RGB color model.

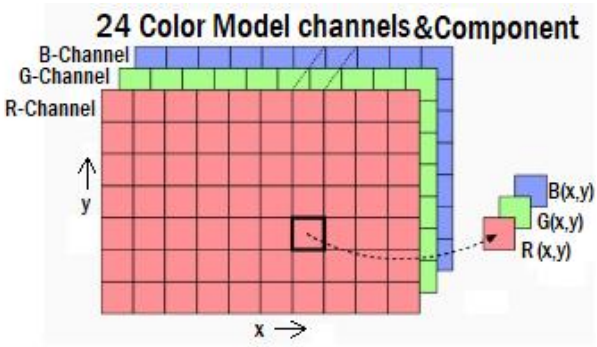

Figure 2.1 R (Red), G (Green), And B (Blue) Color Component Ordering on Each Axis For 24-Bits RGB Color Model.

The digital image histogram offers a visual representation of pixel color distribution, plotting the number of pixels for each color value on a graph, aiding quick assessment of an image's overall color distribution. The vertical axis shows the pixel count for each color value, while the horizontal axis ranges from 0 to 255, depicting color values. Dark and black areas are on the left side, with medium gray in the middle. The RGB color model, using red, green, and blue channels, creates colors by combining colored light sources, with each pixel expressed in terms of these primary colors(Nixon, 2020; Zhang et al., 2021).

RGB, a device-dependent model, is widely used for picture representation and display on electronic devices. In the 24-bit RGB model, each pixel requires 24 bits to

fully specify its color, resulting in 16,777,216 different colors. This model utilizes an additive process, starting with black and adding primary components to achieve desired colors, with black represented as (0,0,0) and white as (255,255,255) when primary color channel values are set accordingly (Nixon, 2020; Zhang et al., 2021).

Steganography techniques serve to safeguard secret information during communication by concealing it within carrier images, aiming to prevent detection, destruction, unauthorized access, and malicious attacks. These techniques must fulfill several requirements, including imperceptibility, embedding capacity, reversibility, and robustness, as well as security (Kadhim et al., 2019; Giri et al., 2021).

Imperceptibility ensures that the hidden information remains visually and statistically undetectable within the carrier image, preserving its quality. Embedding capacity, or payload size, denotes the ability to hide a substantial amount of information without degrading image quality, with larger capacities being preferable (Kadhim et al., 2019; Giri et al., 2021).

Reversibility and robustness guarantee that hidden information can be accurately extracted despite image modifications or attacks. Finally, security and confidentiality ensure that only authorized users can access the hidden information, remaining undetected by unauthorized individuals or detection algorithms (Fridrich, 2009; Kadhim et al., 2019; Giri et al., 2021).

2.1.1 Steganography Classification Overview

Steganography techniques can be classified in the literature based on the type of key, like cryptography, the type of carrier media, or the embedding process. These classifications help researchers and practitioners understand and analyze different steganography techniques. The first classification is premised on the fact that steganography techniques inherit cryptography's security characteristics and

components, such as the public key and private key (Kadhim et al., 2019; Giri, 2021; Nicholas, 2015).

Therefore, steganography techniques are classified into three types based on the key: Pure steganography techniques necessitate both sender and receiver possessing embedding and extraction algorithms without relying on secret key exchange protocols, hence termed keyless methods. Secret key steganography mirrors asymmetric key cryptography, employing a shared secret key for both embedding and extraction, known to both parties through a shared protocol. Public key steganography aligns with symmetric key cryptography, employing two keys—public and private—where the public key is widely distributed, while the private key remains known only to the recipient (Kadhim et al., 2019; Geetha et al., 2023).

The second classification is based on the carrier media type: Text-based, Image-based, Audio-based, Video-based, Protocol-based, and DNA-based. Furthermore, the classification of steganography encompasses two subdisciplines based on the embedding process: technical and linguistic steganography (Kadhim et al., 2019; Megías et al., 2022).

Linguistic steganography utilizes more creative and non-obvious methods of information hiding based on language and text manipulation. Technical steganography is more based upon scientific methods of hiding information in a multimedia carrier such as text, audio, image, or video without raising any suspicions of alteration to its contents (Fridrich, 2009; Kadhim et al., 2019; Megías et al., 2022).

Figure 2.2 shows the steganography technique classification.

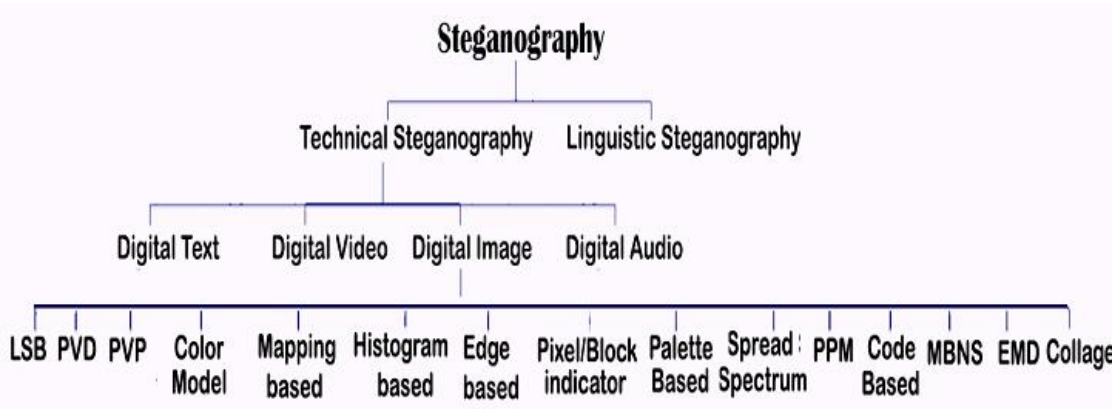

Figure 2.2 Steganography Techniques Classification.

Technical steganography encompasses techniques categorized by the type of cover used, such as digital image, video, audio, text, graphics, or other media, as well as by the methods employed to hide secret digital information within the carrier. These techniques aim to address trade-offs between robustness, imperceptibility, and embedding capacity (Kadhim et al., 2019; Geetha et al., 2023).

Employing secure communication methods, technical steganography conceals the existence of secret digital information. The process typically begins by identifying redundant bits in the cover media that can be altered without compromising integrity or being detected by the Human Visual System and steganalysis (Fridrich, 2009; Hussain et al., 2018; Kadhim et al., 2019).

Digital images are a preferred medium for secret information transfer due to their ubiquity and ease of sharing, offering a high level of security against detection. Digital image steganography techniques encompass spatial, frequency, and adaptive methods (Kadhim et al., 2019; Giri, 2021).

Spatial techniques involve embedding directly into pixel values, with classifications including Least Significant Bit (LSB), Pixel Value Difference (PVD), and Pixel Value Prediction (PVP), among others, offering simplicity and high capacity with controlled image quality (Fridrich, 2009; Kadhim et al., 2019).

Frequency-domain techniques, such as discrete cosine transform (DCT) and discrete wavelet transform (DWT), hide information in transform-domain coefficients, providing robustness and high capacity but with increased complexity. Adaptive steganography techniques improve embedding schema to avoid detection, utilizing the statistical properties of the carrier image to determine optimal embedding, with the aim of enhancing security while minimizing distortion and noise (Fridrich, 2009; Kadhim

et al., 2019; Giri, 2021). A brief comparison of the spatial domain techniques, transform domain techniques, and adaptive embedding techniques is shown in Table 2.1.

Table 2.1 Comparison between the Steganography Techniques Classification

Factors	**Spatial Domain**	**Transform Domain**	**Adaptive**
Technique complicity	Simple	Complex	Based on algorithm
Embedding capacity	High	Low	Algorithm dependent
Robust against image manipulation	Less prone	Highly prone	Algorithm dependent
Visual features Integrity Sharpness, blurring, edges	Maintainable Integrity	Lower Maintainable Integrity	Maintainable Integrity
Stego Visual Quality Imperceptibility	High	Less controllable	High controllable
pixel Embedding	Carrier media pixel value directly	Transform coefficient, indirectly	Algorithm dependent
Undetectability	Moderate	High	High
Carier media dependent	Dependent	Independent	Independent
Security against Geometric attacks	Vulnerable (not robust)	Resistant	less prone
Statistical detection attacks analysis (Histogram and RS)	Easy to expose/detect	Hard to expose/unsuccessful	Hard to expose/unsuccessful
Non-Structural detection attacks analysis (Feature set, SPAM)	Easily detectable	Easily detectable	Difficult/ algorithm dependent
Commonly Techniques	LSB, PVD, MBNS	DCT based, DWT based, CWT based	HVS, AI, Machine learning, Region based

Table 2.1: Continued…

Advantage	Simple implementation, high capacity with low distortion, Improve Imperceptibility	Robustness against attacks and steganalysis techniques, low distortion with high visual quality.	improve visual quality with higher capacity, HVS Very difficult to detect the embedding by naked eyes
Disadvantage	Lack of defense against geometric,	lower capacity, weak in term of security and	Lower capacity, poor security, Lack of defense against

	compression and statistical analysis attacks, weak in term of security and integrity.	integrity. Reversibility problem Some method in this field is poor robustness against attacks.	geometric, compression and statistical analysis attacks, complexity with high-cost implementation

2.1.2 Steganography Evaluation

Evaluation metrics are essential in steganography techniques as they enable the measurement of effectiveness, comparative analysis, quality assurance, optimization, decision support, and standardization. By utilizing appropriate metrics, researchers and practitioners can assess, enhance, and implement steganography techniques that effectively meet the diverse requirements of information security applications (Giri, 2021; Megías et al., 2022).

The evaluation of steganography techniques encompasses various aspects such as visual quality, embedding capacity, robustness, undetectability, and security. These metrics provide mathematical assessments of the similarity or difference between cover and stego images, focusing on distortion rather than perceived quality. Image histogram offers insights into pixel occurrence and distribution, aiding in imperceptibility evaluations by comparing the histograms of original cover images with stego images (Fridrich, 2009; Kadhim et al., 2019). Table 2.2, presents the common quality evaluation metrics and measurements, along with their descriptions and respective formulas. X and Y represent image rows and columns, while C and S denote cover images and stego images.

Table 2.2 Common Quality Evaluation Metrics for Steganography Techniques.

Matrix	Description	Formulas
Mean Square Error (MSE)	MSE measures the stego image accuracy according to the errors produced from embedding process	$\mathbf{MSE} = \frac{1}{X \times Y} \sum_{j=1}^{X} \sum_{K=1}^{Y} (S_{j\,k} - C_{j\,k})$

Signal To Noise Ratio (SNR)	SNR indicates the cover image distortion amount produced by embedding.	**SNR** = $10 \times log_{10}(\frac{\sum_{j=1}^{X\times Y} C^2}{\sum_{k=1}^{X\times Y} C_k - S_k})$
Peak Signal-To-Noise Ratio (PSNR)	PSNR measures the stego-image distortion in the unit of decibel (dB). PSNR reflects higher quality of the stego-image	**PSNR**= $10 \times log_{10} \frac{MAX^2}{MSE}$ Max is the maximum pixel value in both S and C equal 255.
Weighted Peak Signal to Noise Ratio (WPSNR)	WPSNR measures the stego image visual quality weight, perceptual and accuracy.	**WPSNR** = $10 \times log_{10} \frac{Max\ C^2}{NFV(S-C)^2}$ NFV: noise visibility function. **NFV** = NORM $(\frac{1}{1+\sigma_x^2(i,j)})$ σ: standard deviation, NORM: normalize the obtained value to either 0 or 1.
Normalize Cross Correlation (NCC)	NCC measures the degree of proximity or similarity between S and C is either different or similar. Maximum value constitutes the closer similarity between C and S ranges from −1 to 1.	**NNC** = $\frac{\sum_{i=1}^{X\times Y} (Ci \times Si)}{\sum_{i=1}^{X\times Y} Ci^2}$
Structural Similarity Index (SSIM)	SSIM measures the similarity comparison between cover images and stego image with values ranges between -1 and 1. largest values constitutes the closer similarity between C and S.	**SSIM** = $\frac{(2\times\mu_C\times\mu_S+K1)(2\times\sigma_{CS}+K2)}{(\sigma_C^2+\sigma_S^2+K2)\ ^2\times(\ \mu_C{}^2+\mu_S{}^2+K1)}$ Where: $\boldsymbol{\mu}_C$ and $\boldsymbol{\mu}_S$: the mean of pixels, $\boldsymbol{\sigma}_C$ and $\boldsymbol{\sigma}_S$: **C** and **S** variances, $\boldsymbol{\sigma}_{CS}$: the co-variance , and **K1** and **K2** : constants.
Bits error rates (BER)	BER measures the ratio of S total bits, and the distorted S' bits then count the number of errors.	BER= $\frac{S-S'}{S}$ Where S': attacked Stego-image.
Image Fidelity (IF)	IF measures the exact distinction between C and S, and the close distribution between them to ensure S without any visible distortion or loss.	**IF** = 1- $\frac{\sum_{i=1}^{X\times Y} (Ci \times Si)^2}{\sum_{i=1}^{X\times Y} Ci^2}$

The second steganography evaluation category is the embedding capacity (EC), which represents the percentage of embedded secret bits per pixel (bpp) for all the cover image pixels. There is a trade-off between embedding capacity and visual quality; the goal is to maximize embedding capacity while maintaining high visual quality. The embedding capacity, also called payload, is measured as follows: