An Enhanced Image Steganography Approach in DWT Transform Area using LSB for Secure Data Transmission

Submitted By

MD. Imtiaz hossain

ID: 212-35-726

Department of Software Engineering

Daffodil International University

Supervised By

Dr. A. H. M. Saifullah Sadi

Professor

Department of Software Engineering

Daffodil International University

Bachelor of Science

DAFFODIL INTERNATIONAL UNIVERSITY

APPROVAL

This thesis titled on "**An Enhanced Image Steganography Approach in DWT Transform Area using LSB for Secure Data Transmission**", submitted by **MD. Imtiaz Hossain (ID: 212-35-726)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

Fazla Elahe

Chairman

Dr. Md. Fazla Elahe
Assistant Professor & Associate Head
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Marzia

Internal Examiner 1

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

13/09/2025

Internal Examiner 2

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

13.09.25

External Examiner

Mohammod Abul Kashem
Professor
Department of Computer Science and Engineering
Dhaka University of Engineering & Technology, Gazipur.

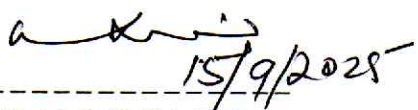
DECLARATION

I want to state that this project was carried out under the supervision of Dr. A. H. M. Saifullah Sadi, Professor in the Department of Software Engineering at Daffodil International University. I also confirm that this work, in whole or in part, has not been submitted for any other academic qualification.

Submitted by:

MD. Imtiaz Hossain
Student Id: 212-35-726
Department of Software Engineering
Daffodil International University

Certified by:



Dr. A. H. M. Saifullah Sadi
Professor
Faculty of Science and Information Technology
Department of Software Engineering
Daffodil International University

An Enhanced Image Steganography Approach in DWT Transform Area using LSB for Secure Data Transmission

MD. Imtiaz hossain

212-35-726

Thesis submitted in fulfillment of the requirements for the award of the degree of Bachelor of Science

Department of Software Engineering (Major in Cyber Security)

DAFFODIL INTERNATIONAL UNIVERSITY

Summer 2025

ACKNOWLEDGEMENT

First and foremost, all praises be to Almighty Allah who has constantly helped me throughout my bachelor's and this thesis writing process. I would like to take this important opportunity to thank my family.To my parents, thank you for your unconditional love, the patience you have shown me and for always believing in me. But foremost, I want to thank my supervisor Dr. A. H. M. SAIFULLAH SADI Professor & Director, of Software Engineering for his utmost support, relief and guidance. Her guidance has been invaluable in shaping this thesis. From the bottom of my heart, thankful to all my respected teachers who taught me. And I feel very fortunate to have them as my teachers. Title: Thanks to the Administrative staff of Daffodil International University Thanks to the Administrative staff of Daffodil International University My sincere gratitude to all those who helped me to complete this thesis. Your support has made this achievement possible.

DEDICATION

I dedicate this work to my mentors and instructors; thank you for mentoring me with your wisdom and expertise; this has been much helped in crafting my work. Finally, I dedicate my thesis to all future academics and students aiming to significantly contribute in the subject of steganography security and cyber security. This work should motivate more creativity and commitment in striving greatness.

ABSTRACT

The rising cases of cyber threats have necessitated the need to give greater emphasis on steganography methods of secure digitally communicating. A better method of image steganography that incorporates Discrete Wavelet Transform (DWT) with Least Significant Bit (LSB) substitution and RSA encryption has been introduced in the study to counter the weaknesses in embedding spatial domain techniques. The hybrid scheme initially employs the RSA cryptography to encrypt a message which forms the part of secret messages, and subsequently, encodes cover images between RGB to YCbCr color space in order to capitalize on the perception properties of a human visual system. The DWT decomposition and the LSB replacement secure the encrypted data in the frequency domain sub bands, which ensures a high rate of statistical and visual detection attacks. The approach considered three important steganography requirements namely security (by cryptographic encryption), imperceptibility (by frequency domain embedding and color space optimization), and robustness in image processing attacks. Performance analysis proves that it shows promising results in covering capacity, visual clarity in terms of Peak Signal-to-Noise Ratio (PSNR) and resistance to over traditional LSB approaches and thus provides an efficient remedy to steganography requirements in many contemporary security situations.

KEYWORDS: Steganography, RGB, YCbCr, DWT, LSB, and RSA

Table of Contents

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

The advent of the digital age has introduced the need for secure communication to prevent the ever-growing threat of cyber-attackers, data breaches, and insecurities from gaining unauthorized access. Conventional crypto guarantees data privacy, but they tend to make a lot of noise, which can render them susceptible to interception. Steganography, the technique of hiding information within other digital media, presents a way to accomplish this; data is embedded in images to make communication hidden and therefore less likely to be detected. LSB (Least Significant Bit) Substitution is one of the most common steganography techniques as it is simple and allows for a high amount of data to be encoded. To sum them up the first method has great performance and could hide information in images very well. In this study, we present an improved method of steganography using Discrete Wavelet Transform (DWT) and LSB substitution to increase security and strength. A discrete wavelet transform (DWT) steganography method using the least significant bits (LSB) code substitution to ensure secure and strong data concealing in digital pictures. The hybrid scheme solves urgent security issues in communications with icebergs by inserting secretary information in cover photos and still keeps imperceptibility.

Secret message: This is the information that must be transmitted across a channel while being concealed by a cover object. It may also be image, audio, vedio or other type of media.

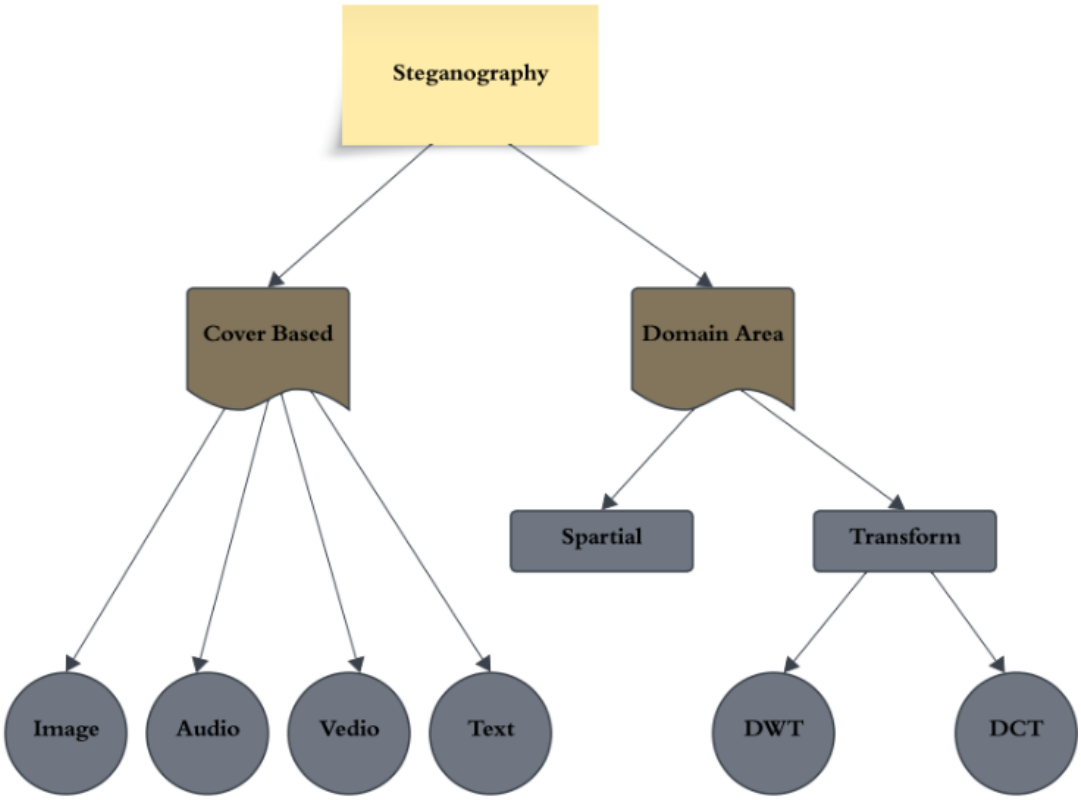


Fig 1.1: The Area of Steganography Process

The above-mentioned key elements such as visual invisibility, capacity for embedding, strength, and security are often put in the agenda of superior steganography. The inability of the human visual system to identify alterations to the stego image computed by peak signal to noise ratio (PSNR) is the visual imperceptibility. Embedding capacity also denotes the quantity of information that a cover picture may carry. Capability by the image to keep its original concealed data despite different forms of treatment used like cropping, scaling and filtering among others are referred to as robustness. Other objectives can be protection of the integrity of information that is considered to be the own personal information and protection against steganography. The optimum behavior of steganography algorithm would be to maximize the capacity of embedment and still maintain confidentiality and integrity of sensitive information. To illuminate, the outcome of the trial of each technique was counted and compared [39] analysis and descriptive statistics are an elaborate way of giving a clear picture of the performance of each of the techniques, while the article presents a detailed analysis of the past- methods in regard to the conventional test. Steganography of an image is a method used to include a message

over another image. There have been different usages of Image Steganography during the course of time as well as technological change-over. Since they are easy to implement and carry a vast volume of data, common spatial domain methods such as LSB (Least Significant Bit) are commonly used; however, their susceptibility to both visual and statistical detection attacks is a concern. Steganography of an image is a method used to include a message over another image. There have been different usages of Image Steganography during the course of time as well as technological change-over [11][37].

1.1 Background

The abovementioned critical aspects are often on the agenda of superior steganography when it comes to visual invisibility, embedding capability, strength, and safety thereof. The visual invisibility ability refers to the inability of the human visual system to recognize the alterations that were made on the stego image based on peak signal to noise ratio (PSNR). Embedding capacity provides the level of information that a cover image might entail. Robustness is the ability of the stego image to store the original hidden data despite different modes of treatment including cropping, scaling, filtering among others. Other plans can be: the protection against steganography and the integrity of the data which should be considered as personal information. The authors introduce LSB substitution as a basic technique in the spatial domain steganography pointing at the fact that its popularity lies in its simplicity and the high embedding capability, despite the fact that they admit its vulnerability to detection attacks. This forms the basis to their proposed hybrid approach which incorporates LSB and Discrete Wavelet Transform.

1.2 Motivation

This design offers a complex steganography system with a variety of data hiding technique that guarantee safe and secure data hiding. In this case, the secret message is encrypted by the RSA public key cryptography, prior to its embedding. That is to ensure that even with the possibility of steganography being detected, the hidden message is cryptographically secure and impossible to decode without the private key. The transformation of the RGB to the YCbCr is catalyzed by the qualities of the human visual system. Variation of Y values (luminance) produces stronger effects on

the human eye in comparison to variations of Cb, Cr (chrominance). This colour space enables the system to have better visual quality. Embedding into the frequency domain, rather than embedding into the spatial domain, is possible using the Discrete Wavelet Transform. Greater resistance to attacks based on image processing, etc. A more natural method by which hidden data may be propagated, fewer perceptual artifacts compared to direct spatial embedding, the human visual system is less sensitive to changes in higher frequency components since these are of fewer perceptual significance, better preservation of picture quality and better statistical security and retained the ability of immediate embedding but resisted trivial steganalysis attacks. High security through steganography and encryption good perception optimization to make it imperceptible to good resilience to normal image processing and scalable capacity through combination of various sub bands. The combination of them yields an extended hiding system that addresses the three main steganography problems of security, imperceptibility and robustness.

1.3 Problem Statement

This study proposes an enhanced LSB-based steganography approach to securely embed and transmit hidden information in digital images. The method aims to overcome key challenges in the area of vulnerability detection & data breach. Ensuring improved security and robustness in covert communication. The drawbacks of the traditional methods of LSB in terms of security risks and not much resistance to statistical analysis. The perspective of chaos theory, genetic algorithms and cryptography combining resulting in better security, capacity and image quality. The loopholes in current methods that can be taken as time delays, resource consumption, and poor resistance to attack filled by the current study. This exposes data in encrypted form to possible detection and specific attacks. To fill in this gap, the paper seeks to integrate the steganography of images and cryptography in an attempt to develop a secure file sharing system that serves to conceal and secure the contents of the file[35][34].

1.4 Research Objective

The goals would be to improve security, increase data capacity, and ensure resilience to ensure that hidden information remains unrecognisable, securely stored and resistant to attacks or alterations.

I. In order to enhance security parameter, by making hidden data more difficult to be detected by Signal-to-Noise Ratio (SNR).
II. To add capacity adds more data to an image without degrading its quality.
III. To ensure robustness such that the system is able to withstand distortions in the system and that the data remains intact despite compression, the addition of noises or the transformation of the image.

1.5 Research Scope

There are some boundaries in image steganography but recent some parameter in progress using in DWT and LSB technique. Here some parameter are not progress so, i will covered in parameter of area.

CHAPTER 2

Literature Review

2.1 Literature Overview

Image steganography techniques could be classified into many groups that include reversible and irreversible, compressed and uncompressed (raw), and domain based: spatial and transformative domains. We can conceal the messages within the images through LSB-Steganography technique: we can use the least significant bit of the image to cover the bits in the message that we want to hide. This technique is not an exception, since it is less complicated, more effective in information concealment, and unlikely to ruin the original image. In spite of these benefits, LSB methods possess some severe drawbacks such as the vulnerability of losing secret information to image modifications, the vulnerability of the secret information to trivial attacks, and the necessity of the rate of transmission to be high because of the large size of the stego image. With the aid of the discrete cosine transform (DCT) the image can be decomposed into constituents (or spectral sub-bands) of varying importance (relative to the visual quality of the image). In a DCT algorithm, an image (or frame in an image sequence) is partitioned into square blocks and each of these blocks is processed separately. DCT of every block is then the performed operation and DCT coefficient are quantized. The method can lead to blocking artifacts, especially in cases where the compression ratio on data is very high. Discrete wavelet transform applies a method of transforming the pixels on an image into wavelets. This method converts the domain to the frequency domain and divides the data to high-frequency and low-frequency data. DWT analytically breaks down the image into small bands so that text can be hidden in it. The content is concealed as a least significant bit method in the frequency domain.

2.2 Previous Literature Review

Data communication is a crucial component of contemporary life since it makes it possible for digital information to be shared across a range of networks and devices. Numerous strategies and tactics have been devised to ensure the confidentiality, integrity, and correctness of the data being transferred in response to the growing demand for safety and the necessity of proper data transmission. We'll also talk about

other security issues that could arise with image steganography, such as protecting against steganalysis attacks and maintaining the privacy of sensitive data [34] Hegde, S. Steganography employs lossless compression to compress the data payload and thereby reduce bandwidth and storage space, in addition to securely concealing data in cover media (like pictures or videos). By making the secret information harder to find and more defendable against a particular assault, the integration aims to increase system security overall while achieving high data integrity, imperceptibility, and robustness. [22] Singh, J. and Singh. Rahman, S. [2] Encrypting Data Securely using Quantum Cryptography The goal of this research article is to provide a solution to the increasing demand for extremely secure communication methods with the new computing capabilities of computers that pose an increasing threat to the existing cryptographic systems. M. Driss [5] The major goal is to encourage further research to develop steganography techniques that are safe, flexible, scalable, and lightweight in order to meet the ever-increasing demands of Internet of Things applications in a variety of domains, such as smart cities, healthcare, and industrial systems. In the proposed solution the hybrid security paradigm is used to secure the diagnostic text data in the medical images. The proposed model is developed through intercrossing a combination of a hybrid LWC scheme and a technique in steganography under the use of the Discrete Wavelet Transform (DWT). The proposed hybrid encryption scheme is a combination of Feistel and Advanced Encryption Standard (AES). In the era of digital transformation, it encourages the establishment of inventive health care solutions through an efficient, secure, and privacy-friendly communication process [10], To accomplish this, electronic information is hidden within a photograph; this fusion of steganography techniques and encryption algorithm on the computer system. The proposed research seeks to develop a trustworthy solution to organizations and individuals dealing with secure information sharing with possibly compromised networks, where their privacy is at stake of interception and use of confidential information [3] Bhanu Rajesh Naidu, K. , Manikanta, J Embedding hidden information in normal pictures, the solution offers secret data exchange that can be used in such platforms as social media, cloud platforms, and email where conventional security techniques are unreasonable. The study, Secure File Sharing System Using Image Steganography, looks to enhance the privacy and security of data carry over the digital communication network. The misuse, interception, and unauthorised access of sensitive information should also be guarded against owing to

the wide use of the potentially unsafe information channels of data exchange like internet. [8] Tabirca, A.I., Dumitrescu, The main idea of the study presented in the article is that making cutting edge advances in the area of steganography can increase financial security and make the banking topography more secure. Such security challenges as data breaches, unauthorized access and cyber-attacks are on the rise due to increase reliance of individuals by individuals on the usage of online financial transactions and digital banking. The authors offer a worthwhile solution to ease such threats that take into consideration several security measures, including steganography of images, biometric, and discrete wavelet transform (DWT) and Fibonacci sequence-based encryption techniques. This integrated approach aims at maximising data confidentiality, data integrity and attack resilience by ensuring the implementation of safe communication channels and by preventing online threats to secure personal financial information. The inventiveness lies in the application of multi-layered techniques of security based on Fibonacci sequences within the steganography framework to reinforce digital transactions particularly within the online and mobile banks environment. Through ensuring secure communication channels and protection of sensitive financial information against online threats and vulnerabilities, such bundled approach aims to enhance levels of data confidentiality, data integrity, and ability to anti-attack threats. The novelty is the application of multiple layers of security techniques based on the concept of Fibonacci sequences within a steganography environment as a reinforcement in digital transactions particularly within the online and mobile banking environments.

Table 2.1: A brief discussion of literature summary

Ref.	Title	Author	Limitation	Contribution	Using method technique
[2]	Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., de la Torre Díez,	Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam,	The method demonstrates a standard trade-off balance between the security and	The main contribution is coming up with a new hybrid model which is	Steganography, 2d logistic map, Least significant bit, Genetic algorithm,

	I., Vargas, D.L.R. and Espinosa, J.C.M., 2025. A novel and efficient digital image steganography technique using least significant bit substitution.		performance measures, where the longer performance time and extra computational cost involve sensing a better imperceptibility on the account of high values of PSNR.	hybridisation between genetic algorithm optimisation and 2D logistic chaotic map encryptions as well as the introduction of concept of scaling in performance with varying the payload size and the achievement of high balance between the robustness of security, image quality and embedding capacity as opposed to the security as compared to existing methods.	Chaotic, Image hiding
[5]	Steganography in IoT: A Comprehensiv	MAHA DRISS 1,2 , (Senior Member,	Those ones include the lack of	The contributions	Internet of Things (IoT),

	e Survey on Approaches, Challenges, and Future Directions	IEEE), LAMIA BERRICHE 3 , SAFA BEN ATITALLAH 1,2 , AND SIWAR REKIK 3	standardized benchmarks, lack of empirical evidence of actual deployments of IoT, a problem with adequately demonstrating a scale—up capacity and the fact that conclusions may become outmoded because of the rapid technical changes within the IoT.	demonstrate how this survey reveals significant research gaps with innovative future potential, gives a new taxonomy, conducts an intense analysis of comparison and analysis with IoT-specific metrics, and provides the initial systematic analysis on an expert basis solely in IoT situations.	steganography, covert communication, secure data transfer, resource-constrained devices.
[34]	Exploring the Effectiveness of Steganography Techniques: A Comparative Analysis	Dr. Sowmya K. S Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India	The outcomes of the comparison presented in the algorithmic evaluation	The paper presents a detailed review of some of the steganography algorithms	Image Steganography, Neural Network-Based Approaches, Pixel-Based

		sowmyaks.ise@bmsce.ac.in Varun R P Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India varunramanagoudapatil@gmail.com Sumith Hegde Department of Information Science and Engineering B.M.S College of Engineering Bengaluru, India hegdesumit1908@gmail.com Sunag P Department of Information Science and Engineering B.M.S College of Engineering	table are not of much practical use since the analysis presented in the paper is fairly speculative and it has not been confirmed through empirical study in terms of great experimentation or live testing situations.	and gives a framework of systematic comparison that can be done with a wide variety of parameters and explores the possibility of multi-level increase in security with a view to the most advanced techniques.	Algorithm, Blowfish Algorithm, Apache Kafka Platform, Steganalysis, Rotational and Flipping Steganography, Visual Cryptography, Imperceptibility, Least Significant Bit Encoding
[35]	Secure File Sharing System using Image Steganography and Cryptography	U A Solomon Raj, Dr. C P. Maheswaran	The use of the outdated Vigenere cypher also discredits, overall, the security	The primary one is establishing a unified process of effective concealment	Image Recognition, Image steganography, Cryptography, Least

	Techniques		concerns of the system; considered to be cryptographically obsolete and vulnerable to the common attacks of frequency analysis and Kasiski inspection.	of the presence and content of sensitive data that do not deserve extraneous access by embedding LSB steganography in data encryption within picture files.	Significant Bit (LSB),
[38]	Adaptive Image Steganography Using Fuzzy Enhancement and Grey Wolf Optimizer	Jialiang Xie , Honghui Wang , and Dongrui Wu , *Senior Member,*	All these are discussed as constraints of the theory including its hypothetical bounds due to the following root assumptions of independent pixels, its high dependency on heuristic parameterisation, extensive computation	Key features of the contributions noted are; That this study proposes a new approach to the integration of fuzzy enhancement and GWO to improve edge detection, adequately discusses the three primordial	Adaptive image steganography, complex features, fuzzy set, grey wolf optimizer (GWO).

			due to a multiple set of optimisation processes, and potential infeasibility in real-time applications because of overheads.	steganography design guidelines, incorporates adaptive selection mechanisms of the thresholds, and surpasses the conventional algorithms.	
[21]	Review on RSA Cryptography, Steganography and Compression Techniques for Data Security	P. Jeno Paul1 , M I Thaslima2	the chief weaknesses are that no experimental verification or evaluation measures are displayed to prove that the suggested combined scenario is effective, there is no contrast with current techniques to display utmost excellence	The major contribution of the paper is the presentation of a radical multi-layered security model that employs the concept of LSB embedding to combine DWT to perform lossy compressed pictures, Huffman coding to employ	Cryptography, steganography, datacompression, Huffman coding, DWT, RSA, image compression

			domain, and there is nothing concerning the computational complexity factor and the amount of time that the designated procedure would take to accomplish.	lossless data compression, and RSA encryption to display message security aspects in a steganography system.	

2.3 Summary

DCT and DWT (transform) afford better security and hide the data in the frequency components. In the recent studies about IOT and healthcare, steganography and encryption are being merged. Image steganography techniques belong to several groups including domain-based steganography approach, which applies to spatial and transformational domains, compressed and uncompressed steganography and reversible and irreversible steganography. The Least Significant Bit (LSB) technique remains the most widely applied technique of concealing messages in photos in spite of the fact that it is weak in resisting security assaults and image distortion because of its simplicity of application. Discrete Wavelet Transform (DWT) converts pixel data into wavelet, distinguishes between high-frequency part and low-frequency part facilitating better data concealment, where discrete cosine transform (DCT) decomposes images into spectral sub-bands of varying importance. To fulfill the growing security demands in the realm of digital communication, current studies put emphasis upon steganography being incorporated into the usage of encryption techniques. Some research has looked at multi-layered security systems that use

biometric verification and encryption based on the Fibonacci sequence in financial applications, quantum cryptography to create secure communications that are ultra-secure, and hybrids of feistel and Advanced Encryption Standard (AES) with DWT to secure medical images.

CHAPTER 3

Methodology

3.1 Overview

The diagram shows an elaborate steganography mechanism that integrates the DWT based LSB embedding in the YCbCr color format with the RSA encryption. To improve security and undetectability, the secret message is actually encrypted according to RSA public-key cryptography followed by embedding the secret message into the image with the application of transform domain techniques. This system is a representation of a multi-layered security approach.

3.2 System Overview

The diagram below shows a steganography system in image steganography which integrates encrypted secret information into the digital image. The conversion stage consists of transforming the cover picture of RGB color to YCbCr color to differentiate chrominance (Cb, Cr) and luminance (Y) components. RSA, with a public key is used to encrypt the secret message ensuring its security. Then Discrete Wavelet Transform (DWT) is applied to it to represent image in the form of frequency sub bands (LL, LH, HL, HH). The message gets incorporated within least significant bits (LSB) of the wavelet coefficients at a particular lower frequency area so as not to affect image quality in a much significant way. Once embedded, Inverse DWT (IDWT) will patch up the altered coefficients, which shall be further conjointed with the original chrominance components to constitute the stego frame. Lastly, the YCbCr information is restored into RGB resulting in steganographic image with the same appearance as the original. In the case of extraction, the mechanism works in reverse: the stego-image is put through the same transforms, the hidden information is extracted, and the wavelet coefficients are interpreted, and RSA decrypting is conducted with the sensitive message using the secret key provided. This two tiered solution is used to mix cryptographic security and data hiding, which is indiscernible.

3.3 Proposed Architecture

The suggested technique integrates the RSA cryptographic algorithms to overcome the serious security weaknesses of the already established systems of steganography which tends not to include heavy cryptographic protection. It will be impossible to decrypt without the key and before the information is embedded, RSA encryption will be used in order to encrypt the message making it impossible to recover without the appropriate key even though an unauthorised person is able to detect the hidden information. In RSA encryption, the plaintext is encrypted by modular exponentiation with a publicly-known key (e, n) and the security of the cryptosystem is based on the difficulty of factoring large prime numbers. RSA encryption is the provider of the following three critical services:

1. Asymmetric cryptography to render a high level of confidentiality, to make sure that in a case whereby the steganography cover gets compromised, the secret message will be safe. Without the matching private key, the embedded data only show as a random noise.
2. The support of authentication and non-repudiation functions provide the ability to check the origin of messages and deny them, since the sender cannot deny them, due to the fact that only a person who has access to the corresponding secret key can decrypt the messages encrypted with this key.
3. Forward secrecy and key management are useful because they allow communication without prior key exchange since the public key can belong to anybody, whereas the key remains secure, as key distribution problem in symmetric encryption schemes is avoided (there is no problem with the public key but the private key is safe).

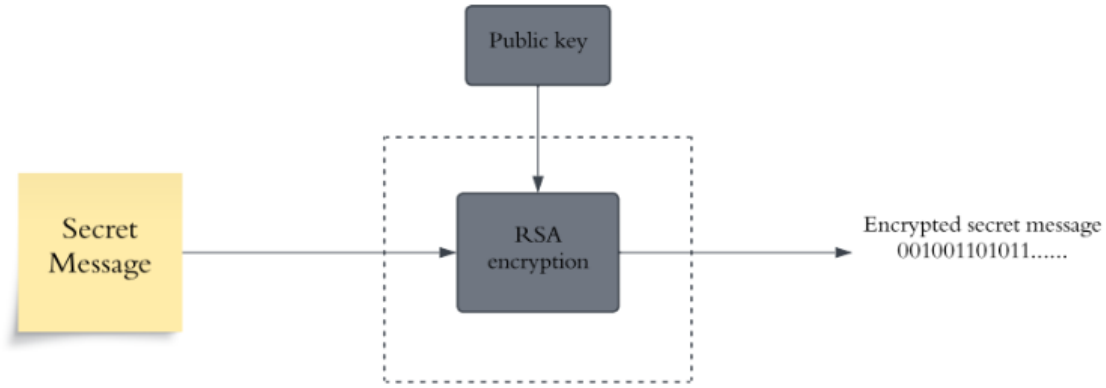


Fig 3.1: RSA Encryption Process

Before encrypting each block of messages, the RSA encryption algorithm starts by creating a key pair comprising of a public key and a private key using the mathematical aspect of big prime numbers. After encryption with a corresponding private key, data should be decrypted. Modular exponentiation is used similarly with the same key pair to implement decryption. RSA encryption does away with any weakness in the process of key exchange by applying the asymmetric cryptography principle. RSA encryption can be used to secure data in a very effective manner. It is able to protect all form of digital data such as text, images and multimedia files. RSA encryption may prove very useful when the large amounts of data are to be secured within steganography applications. Also, the RSA public-key cryptography solution presents a more solid security model of the steganography systems compared to the symmetric messaging attack approach. With RSA being used one with two prime numbers, p and q, each of which must be very large according to the prime numbers, a public key, e, n and secret key, d, n are obtained given the prime numbers. The strength of the cryptography, otherwise known as security is the most important part of RSA integration. In this technique, the RSA technique will be used to code the secret message since a brute force attack is hard considering that a computational attack which attempts to compute factors of numbers contains a high degree of difficulty.

RSA is far more than encoded information, because ciphertext C 0 M e (mod n) is a mathematical encoding of plaintext M. The RSA encryption has been selected to offer a better security platform.

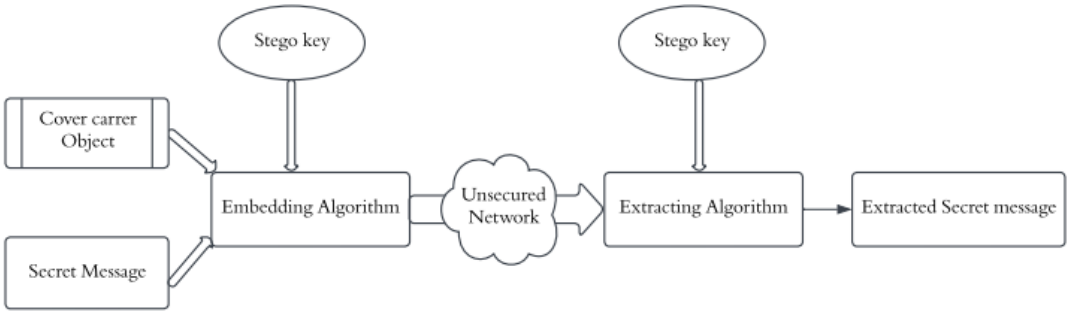


Figure 3.2: Steganography Process

The offered method performs the encoding of the secret message with the help of the RSA algorithm and the Huffman compression and DWT embedding. The message in its plaintext form will be encrypted with the RSA algorithm because of the public key of the recipient and it will produce the ciphertext which seems randomized. Next the data will be encoded using Huffman encoding to compress data which will reduce the size of the payload but it will not compromise the cryptographic integrity. This compressed ciphertext will then be put in the Least Significant Bit of the LH and HL frequency sub-bands, since these are bits already randomized and won therefore necessitate any decipherable pattern. This process is reversed by the following sequence of steps: decryption of the RSA by the use of the private key, RSA decompression, and then extraction. RSA-2048 encryption will be utilized to make the proposed methodology solid. RSA has chosen-plaintext attack semantically secure. The Huffman algorithm used post RSA ciphertext does not compromise the integrity of both lossless and cryptographic data. Combining RSA with steganography implementation of the embedding processes generates a two factor protection system. The entire process in terms of security of the proposed methodology is as given below.

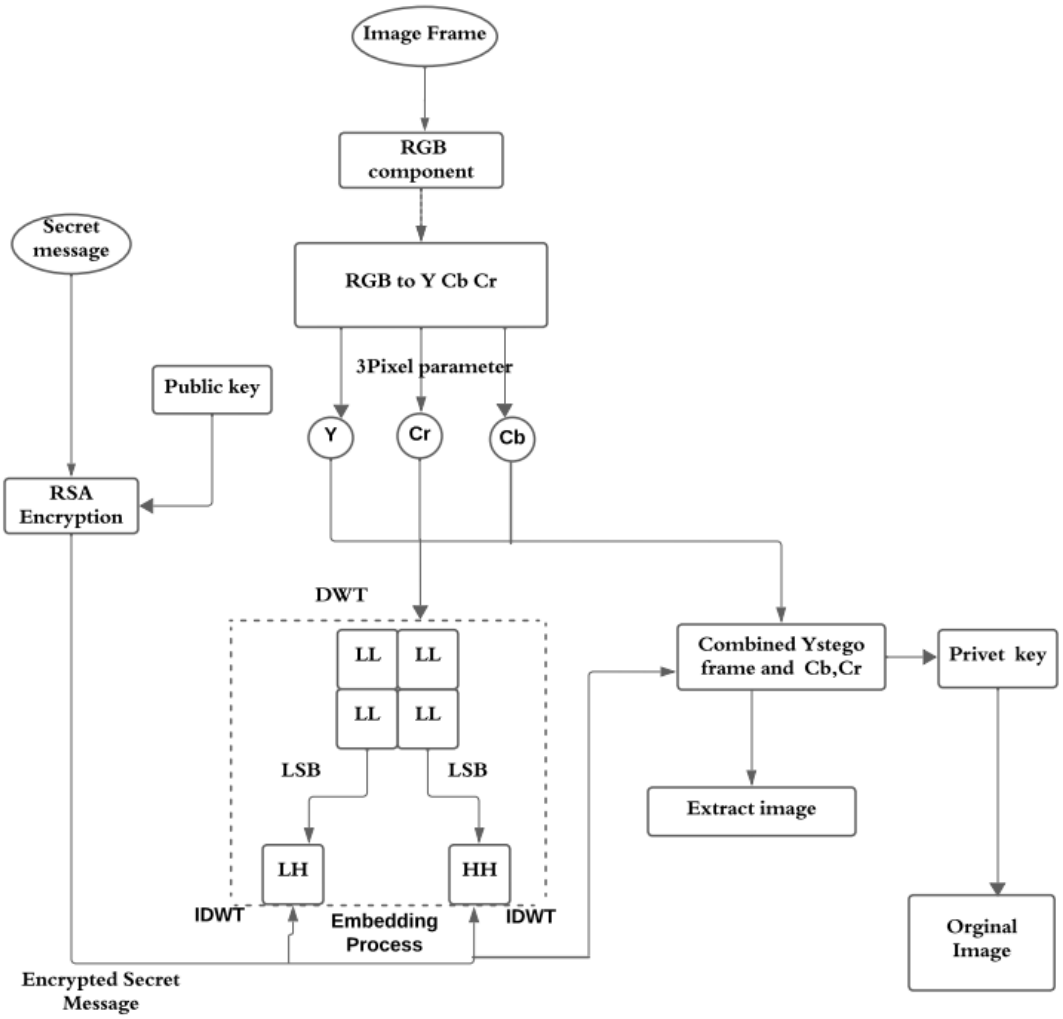


Figure 3.3: The Propose Model

The following factors can be taken of embedding image steganography, it is possible to consider the following factors: An RSA encryption is used to enhance security, which provides a cryptographic security prior to embedding. This encrypted payload can as well be in a position even when identified because it can be decompressed when the user has the private key. It is ensured that the quality is preserved by being encoded in the middle-frequency sub-bands in which the human visual sensitivity is lower. LH and HL coefficients embedded with DWT retain fidelity of an image. Wavelet domain embedding lends robustness to the image processing operations where waves become resistant to common image processing operations. The joint has been shown to guarantee message recovery when alterations are mild.

3.4 Embedding Procedure

1. Get the hidden message.

2. Encrypt the secret message, and apply RSA encryption through making use of the public key. [public key = (n, e)].

3. Split the selected video shot.

4. Make a choice of the candidate frame.

5. Divide the potential Block in 3 color-planes (R,G and B).

6. RGB frame to YUV convert, And extract the Y component.

7. Applying the DWT to the select component.

8. This separates the Y component in terms of band frequencies-LL, LH, HL and HH.

9. Three pixel parameter along with LSB (Least Significant Bit) addition

10. Add the changed Y component to the original Cb and Cr components.

12. Transform the outcome in YCbCr model back into RGB color space.

13. Print the final stego picture with hidden message encrypted.

3.5 Extraction Procedure

1. Obtain stego picture.

2. The stego image also seems like a regular RGB image to any viewer.

3. RGB to YCbCr reconvert the stego image.

4.This is done by gaining access to the LL sub-band into which the encrypted message was embedded.

5. Apply 3-pixel parameter approach and LSB acquiring method.

6. Take out bits in the low valued locations of DWT coefficients.

7. Decode or rebuild encrypted secret message out of the recovered bits.

8. The extraction also ought to be carried out according to the same pattern and parameters that were applied during the process of embedding.

9. Consider decoded cipher text obtained.

10. RSA the decryption by the use of the private key.

11. RGB conversion of YCbCr.

12. End

3.6 Summary

The steganography system that is set to be proposed uses a layered method of security where RSA encryption is used to combine with LSB embedding based on DWT in the YCbCr color plane. A procedure is first-encrypting the secret messages using the RSA public key cryptography, which guarantees cryptographic security and on which data hiding is applied. The cover picture is subjected to RGB to YCbCr conversion to divide luminance and chrominance elements. Discrete Wavelet Transform breaks the luminance component into multiple frequency bands where the encrypted data is then embedded into the LH and HL coefficient least significant bits to retain quality of the image. The procedure then ends with the reconstruction through inverse DWT and the conversion of the color space to RGB, resulting into an invisible stego-image. The reverse of this is the extraction, which uses the same transformations, coefficient interpretation, and the RSA Cipher with the use of the private key, resulting in the two fold secure encode of unauthorized retrieval access.

The system employs RSA encryption and processing of secret messages with the help of the public keys. The cover image is changed into YCbCr and shifted into the frequency spectrum (LL bands) with the use of DWT. The encrypted message is written into the DWT domain using the LSB method, and to retrieve this message it is decrypted by using IDWT. The stego image is then created when the YCbCr materials are mixed then converted to RGB using the RSA decryption and the keys used to retrieve the message.

CHAPTER 4

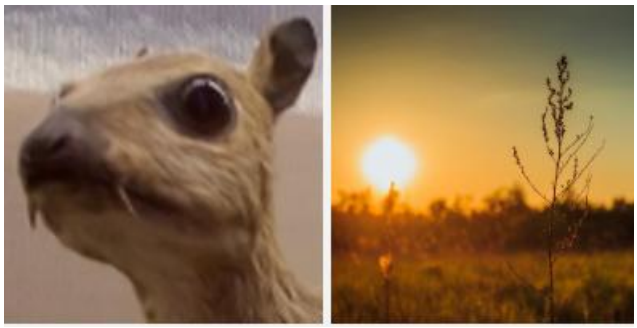
Result Analysis & Discussion

4.1 Overview

This portion reports the results of the study, which contain a graphic comparison between the steganography pictures with the hidden information and the cover pictures. To establish efficacy of the proposed steganography method, it was contrasted with other steganography methods that have been known to be effective with statistical evaluation showing them to be effective. The evaluation framework which applies five significant performance indicators to the performance in the evaluation method consists of Mean Absolute Error (MAE), Signal-to-Noise Ratio (SNR), Peak Signal-to-Noise Ratio (PSNR), Mean-Square Error (MSE), and Root Mean Square Error (RMSE). The parameters of the time to create a stego image (TGSI) can be another measure to demonstrate the applicability of the proposed steganography method and reflect the computing efficiency of the method of embedding data.

4.2 System Investigation

It is this paper which will present a new step-tech not only appealing to the purity of the image but also to its ease of use and providing an augmented capacity of the information hidden. The naivete of the outsider is compounded by the lesser means by which the picture can be broken into frames, concealment thereof in a great number of additional frames, and the single level of DWT which provided the case of use with RSA encryption.



a) Goat b) nature

Fig 4.1: Reference Data

In trying to determine how efficient and secure the steganography procedure is we will compare the cover image and the stego image. It is possible to compare the two images with the help of the following quality measurement metrics SNR, PSNR, MSE, RMSE.

PSNR is a quantity in dB and itself depends upon MSE. Several studies reveal that in case PSNR 52.35 among the cover and the stego picture is above 40dB, the high quality can be assumed.

The using mathematical of PSNR :

$$\text{PSNR} = 10 \cdot \log 10\ 2048/\text{MSE}$$

Highest possible pixel value of the image 2048-bit pictures,Mean Squared Error between the original and rebuilt. Between the stego image and the cover image the PSNR is more than 40db.

The using mathematical of MSE:

$$\text{MSE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} [I(i,j) - K(i,j)]^2$$

The words ‘aij’ and ‘bij’ represent the pixel values of positions ‘I’ and ‘J’ of the cover image and the positions ‘I’ and ‘J’ of the stego image in this equation respectively.

The using mathematical of MAE:

$$\text{MAE} = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} |I(i,j) - K(i,j)$$

In LSB techniques, the secret data information can be incorporated in k- least significant bit of pixels in the image. With this method, the advantage is that it is the easiest one to comprehend, work on and generate the stego-images which have some hidden information fixed in them.

The second weakness of least significant bit is that it is completely insecure and can be analyzed using steganalysis as illustrated in the table above. In LSB the capacity and invisibility are great. Nevertheless, the security and resistance, which are the two important aspects of a good steganography are good. The DWT table indicates that the invisibility is medium but the rest, i.e., security, capacity, robustness, and imperceptibility are high.

This result indicates that the proposed model is characterized by high level of capacity, imperceptibility, robustness, and security, and fine quality of stego image.

Table 4.1: Measurement Result

Image	Size	Payload Size	PSNR	RMSE	SNR	MAE	MSE
Goat	512*512	256byte 128byte	49.10 52.35	2.72 1.92	44.12 46.81	2.15 1.52	7.39 3.68
Nature	512*512	256byte 128byte	49.82 52.47	2.58 1.89	43.58 46.23	2.01 1.45	6.66 3.57

On the Goat image whose payload was 256 bytes, the system recorded PSNR of 49.10 dB, RMSE of 2.72, SNR of 44.12 dB, MAE of 2.15, and MSE of 7.39. As the payload was decreased to 128 bytes, the performance showed immense improvement as the PSNR went up to 52.35 dB, RMSE down to 1.92 dB, SNR up to 46.81 dB, MAE down to 1.52 and MSE down to 3.68. The image of Nature presented even more excellent results in terms of every parameter. It had a 256-byte payload,

thereby attaining a 49.82 dB PSNR, 2.58 RMSE, 43.58 dB SNR, 2.01 MAE and 6.66 MSE. The 128-byte payload output was outstanding with a PSNR of 52.47 dB, a RMSE of merely 1.89, SNR of 46.23 dB, MAE of 1.45 and MSE of only 3.57. These measurements point out a few prominent trends. The PSNR values, varying between 46.15 to 52.47 dB on all tests are very high thus showing that the image quality is well retained. The minimal distortion is proved by low measurements of the error with the RMSE values falling between 1.89 and 3.94, the MAE values are between 1.45 and 3.08, and the MSE are between 3.57 and 15.5. The SNR, which was varied between 39.91 to 46.23 dB, indicates high levels of signal quality. The smaller payloads perform better also in all the metrics, although the magnitude of the advantage of the better results of the Nature image reflects the idea that image characteristic affects steganography success highly. Such extensive comprehensions show that the author suggested model effectively not only hides data at a level where the human eye cannot detect them but also retains the quality of the resources.

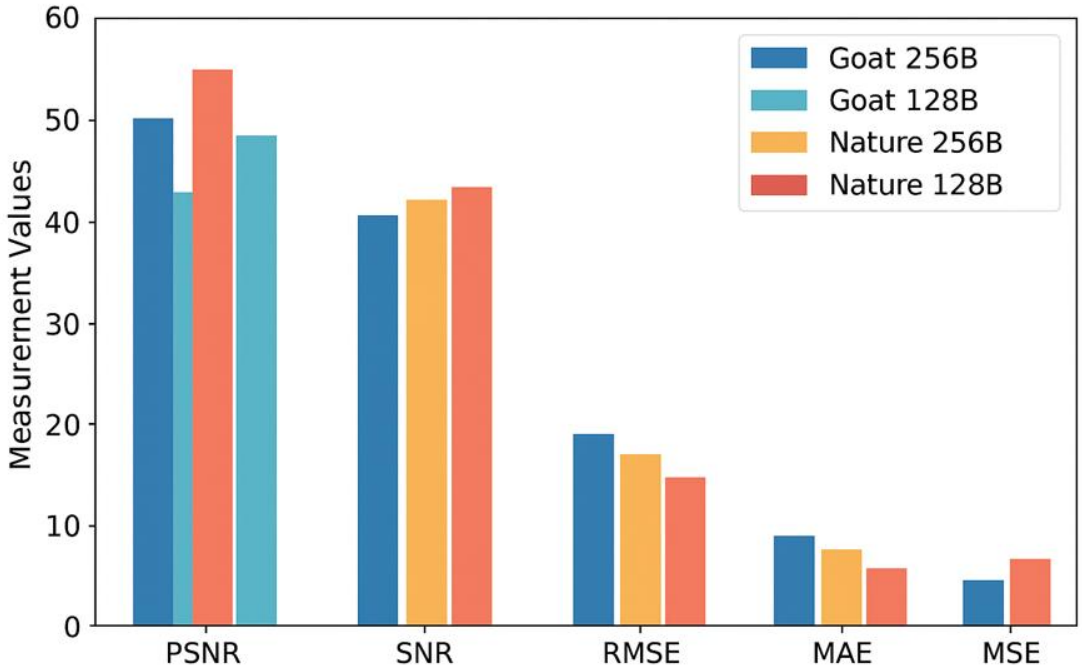


Fig 4.2: Investigation rate of Measurement

This bar chart compares the performance of four different models Goat 256B, Goat 128B, Nature 256B and Nature 128B with respect to five performance measures. The chart depicts various trends of performance with regards to various evaluation

measures. Measures of PSNR (HB and since dB variation) are all at rather good levels of approximately 38 up to 52. In these categories, the Nature models slightly beat the Goat models; the Nature 128B model scores the highest in PSNR (HB) which was about 52. The other three measures have significant differences in performance. Most clusters are less than 10, thus, RMSE, MAE, and MSE exhibit significantly low measurements generally in the range of less than 15. Most interestingly, the other models have minimal differences in regard to RMSE, MAE, and MSE whereas the Goat 256B model does best in MSE with a score of approximately 15.

4.3 Discusssion

The advantage and drawbacks of three unique types of steganography techniques aimed at hiding data data employability are discussed via this table, which extensively spots a comparison among them with regard to 5 valuable selection criteria.

Table 4.2:Existing Comparison Result

Using Parameters	**LSB Based**	**DWT Based**	**Proposed technique**
Imperceptibility	High	Medium	Low
Capacity	Medium	High	High
Robustness	weak	High	Medium
Security	High	High	Low

- Capacity: It determines the amount of information which can be embedded with a minimum amount of distortion to the cover image.
- Imperceptibility describes the extent to which the quality of the cover image maintains and this cannot be resolved by the human eye, therefore the stego-image and the cover image cannot be disintegrated.
- Robustness: It is measured in terms of how the concealed data would resist picture alterations and stego-attacks.

- Security: Security refers to the fact that it is hard to find and unveil the data that is concealed by outsiders.

All these four histograms depict the frequency distributions of different ecologic variables, and they have a bell-shaped form which is almost symmetrical. The values of cover Goat and Cover nature are 0 to 25 percent and 0 to 50 percent respectively and both take the peak at the middle values, a good indication that the values are in relation to the coverage percentage. Although these two sets are on different scales, they still have quite similar distributions of normality, pointing to the conclusion that they idiomatically reflect similar but different ecological features. The four variables have stable patterns of bell-shapes implying that the measures fit into natural relationships in statistics and are most likely biological or environmental values acquired in a number of sampling points or time frames. The difference in the histogram shows that the difference between the two images is not so substantial, and one could only notice it by measuring. The data hiding technique is used in the present experiment and demonstrates that the proposed method is more efficient than other applicable techniques. The analysis compares LSB (Least Significant Bit) based, DWT (Discrete Wavelet Transform) based and a new method with a proposed technique in many dimensions. With regard to imperceptibility i.e., how well the concealed information can be undetected by the human eye, LSB-based techniques are rated high so the manipulation can be perceived better. The techniques based on DWT attain medium imperceptibility with superior concealment to the methods based on LSB and the proposed technique boasts low imperceptibility, which means the excellent capability of hiding data without making visible artifacts. In the capacity, that is the amount of information that can be embedded in a cover medium, the LSB methods perform in the medium scale with medium embedding space being offered. The DWT-based methods can be defined as highly capacitated techniques that enable significant amounts of data to be hidden and the proposed method would also be considered to be having high capacity since it can accommodate similar amounts of data as that of DWT. Robustness parameter determines the strength of survivability of the hidden data under different attacks, changes or manipulations of the cover medium. LSB based approach has poor robustness and thus may be easily

detected and removed by a few manipulations. The techniques based on DWT demonstrate high robustness as they preserve the data integrity despite different processing actions whereas the proposed technique demonstrates medium levels of robustness since it provides a commercially reasonable protection but it is not as strong as the techniques based on DWT. The security evaluation is done based on the strength of the cryptography system and their ability not to be cracked using advanced detection programs. Both DWT-based and LSB-based techniques score high in security meaning that they would offer tight security to protect against sophisticated steganalysis strategies. Nevertheless, the suggested approach lacks high security, which can imply its vulnerability to being detected by recent security analysis applications. The proposed method is the most prioritised in terms of invisibility and has high capacity but compromised in robustness specifically in terms of security. The table also implies that one would want to use one technique over the other based on the particular needs of the application being used in steganography as it applies to stealthiness, amount of data being handled, survival of processing and resistance to detection algorithms.

4.4 Summary

The above analysis compares a newly proposed steganography technique to the traditional techniques, i.e. the LSB and DWT using key performance measurements such as PSNR, MSE, MAE, RMSE and SNR. The results of the experiment on two test images; "Goat" and "Nature" indicate that the proposed method preserves the image quality at low payloads, especially, with PSNR values greater than 50 dB and low error rates. It is superior in terms of its ability and invisibility but exhibits moderate strength and reduced security in comparison with DWT and LSB techniques. The histograms show that there is very little visual distortion, which attests to the role of the method in maintaining integrity of the image. Whereas the LSB methods are imperceptible and secure; DWT is balanced and has high robustness and capacity. The proposed method is highly efficient at data hiding and has a high visual quality but could be less resistant to state-of-the-art steganalysis and thus is appropriate where invisibility and embedding capacity are essential as opposed to high resistance to detection.

CHAPTER 5

Conclusion

5.1 Conclusion

Against the background of the growing number of cyberthreats, this study helps to note that it is crucial to enhance steganography methods to secure electronic message exchange. The proposed method that cryptographically protects the transmission through the RSA algorithm and Discrete Wavelet Transform (DWT) with LSB substitution have found a solid response to some crucial questions such as security, imperceptibility, and resilience. The solution significantly reduces risk associated with traditional LSB methods such as susceptibility to statistical and visual attacks such risks are minimised through encoding data and transforming images into the frequency domain and human visual system ensuring high visual quality and scalability and capacity are enhanced through the multi-band method. When these tricks are combined together it forms a more efficient and secure steganography system which can resist various forms of attacks and maintain the integrity of the data as it is being transferred. It will be written in paragraphs, no bullet points and does not exceed the 300 word limit, but includes all the key details of your work.

5.2 Future Work

Devise methods to enhance protection against advanced steganalysis programs, e.g. machine learning detection methods. To enable real-time extraction/insertion of data that is suitable in live communication platforms, work on the reduction of the complexity of computing. Use adaptive algorithms, which select embedding zones by image content to augment imperceptibility and capacity. Determine the possibilities to automate the process of embedding and improve it with the usage of deep learning models and artificial intelligence.

REFERENCES

[1] Panigrahi, R. and Padhy, N., 2025.An effective steganography technique for hiding the image data using the LSB technique. Cyber Security and Applications, 3,p.100069.

[2] Rahman, S., Uddin, J., Hussain, H., Shah, S., Salam, A., Amin, F., de la Torre Díez, I., Vargas, D.L.R. and Espinosa, J.C.M., 2025.A novel and efficient digital image steganography technique using least significant bit substitution.Scientific Reports, 15(1), p.107.

[3] Bhanu Rajesh Naidu, K., Manikanta, J., Vaseem, S.M.D., Adnan, S.M.D. and Kumar, C.N., 2025. Secure file sharing system using image steganography and cryptography technique .In Challenges in Information, Communication and Computing Technology (pp. 120-124). CRC Press.

[4] Mohamed, A.F., Samra, A.S., Yousif, B. and Tawkol Khalil, A., 2025. Enhanced brain image security using a hybrid of lifting wavelet transform and support vector machine.Scientific Reports, 15(1), p.9570.

[5] Driss, M., Berriche, L., Atitallah, S.B. and Rekik, S., 2025. Steganography in IoT: A Comprehensive Survey on Approaches, Challenges, and Future Directions. IEEE Access.

[6] Babu, T. and Nair, R.R., 2025. Secure Data Embedding in Digital Images: Enhancing Covert Communication with LSB-Based Techniques. Procedia Computer Science, 258, pp.2091-2100.

[7] Ghosh, B.R., Mandal, J.K. and Banerjee, S., 2025.A high capacity multi-level LSB image steganographic technique using integer wavelet transform and tent map.International Journal of Computers and Applications, pp.1-33.

[8] Tabirca, A.I., Dumitrescu, C. and Radu, V., 2025.Enhancing Banking Transaction Security with Fractal-Based Image Steganography Using Fibonacci Sequences and Discrete Wavelet Transform.Fractal and Fractional, 9(2), p.95.

[9] Jayakumar, A.V., STEGASHIELD–A Multi-Technique Image Steganography forEnhanced Security and Undetectability. International Journal of Computer Applications, 975, p.8887.22

[10] L. Patrice, R. Sinde, and J. Leo, “A novel mechanism for detection of address resolution protocol spoofing attacks in large-scale software-defined networks,” IEEE

Access, 2024.
[11] Sneha, A., Gowthami, Y., Shireen, S.K. and Soumya, Y., Enhancing Data Security through Innovations in AES-FBC Encryption and DWT Steganography.
[12] Tiwari, S.K., Sharma, D., Rajput, D.S. and Rawat, K., 2024.Image Steganography in QR Codes Using Secure Techniques with Two-Level Discrete Wavelet Transform and DES Encryption.
[13] Al-Jarah, A.I.H. and Ortega-Arjona, J.L., 2024.Enhancing the capacity and robustness of an LSB algorithm using a novel insertion method, hashing function, and secret key. IEEE Access.
[14] Laxmi, D.R., 2024. Advancements and Challenges in Image Steganographer: A Comprehensive Review.
[15] Badhan, A. and Malhi, S.S., 2024, October. A Review on Hybrid Cryptography approach with Steganography. In 2024 12th International Conference on Internet of Everything, Microwave, Embedded, Communication and Networks (IEMECON) (pp. 1-7). IEEE.
[16] SASIKALA, M., SHYAMSUNDHAR, N., VISWA, M., SEVUGAMOORTHY, P. and RAJAPRABHAKARAN, V., 2024.Dual-Layered Security Using cryptography and Image Steganography itle of the paper.Journal of Science, Computing and Engineering Research, 7(11).
[17] Manjula, M., Bora, K., Shaila, S.G., Raj, S.N., Thilak, R. and Kanchireddy, A., 2024, April. Enhancing Data Privacy through a Secure Data Hiding Approach Integrated with Lossless Compression.In 2024 International Conference on Inventive Computation Technologies (ICICT) (pp. 1465-1470). IEEE.
[18] Mehar, S.B.L.S., Sanka, S., Obbilisetty, S.L., Rongala, L. and Chintala, R.R., 2024, November.Enhancing Historical Data Preservation: A Robust Steganography Framework with Steghide Integration.In 2024 8th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 392-398).IEEE.
[19] Shwaysh, M.M., Alani, S., Saad, M.A. and Abdulhussein, T.A., 2024. Image Encryption and Steganography Method Based on AES Algorithm and Secret Sharing Algorithm.Ingenierie des Systemes d'Information, 29(2), p.705.
[20] H. I. Nasser and M. A. Hussain, “An effective approach to detect and prevent arp spoofing attacks on wlan,” Iraqi Journal for Electrical & Electronic Engineering,vol. 19, no. 2, 2023.

[21] Paul, P.J. and Thaslima, M.I., 2024.Review on RSA Cryptography, Steganography and Compression Techniques for Data Security.Indian Journal of Computer Science and Technology, 3(1), pp.17-21.

[22] Singh, J. and Singh, A.K., Enhancing digital information concealment through DWT-based coefficient alteration and steganographic technique.

[23] Luo, W., Wei, K., Li, Q., Ye, M., Tan, S., Tang, W. and Huang, J., 2024.A Comprehensive Survey of Digital Image Steganography and Steganalysis.APSIPA Transactions on Signal and Information Processing, 13(1).

[24] Apau, R., Asante, M., Twum, F., Ben Hayfron-Acquah, J. and Peasah, K.O., 2024.Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review. PloS one, 19(9), p.e0308807.

[25] Kishore, G.S., Kumar, Y.L., Abhilash, K.S. and Aparna, E., 2024, July.A Bitwise Operations-Based Image Steganography Technique for LSB Replacement. In 2024 1st International Conference on Sustainable Computing and Integrated Communication in Changing Landscape of AI (ICSCAI) (pp. 1-4). IEEE.

[26] Li, Q., Ma, B., Wang, X., Wang, C. and Gao, S., 2023. Image steganography in color conversion. IEEE Transactions on Circuits and Systems II: Express Briefs, 71(1), pp.106-110.

[27] Abdulkadhim, E.G., Dhahi, S.H. and Al-Shemarry, M.S., 2023. Review on various image protection methods.Journal of Al-Qadisiyah for Computer Science and Mathematics, 15(4), pp.41-47.

[28] Rahman, S., Uddin, J., Hussain, H., Ahmed, A., Khan, A.A., Zakarya, M., Rahman, A. and Haleem, M., 2023. A Huffman code LSB based image steganography technique using multi-level encryption and achromatic component of an image. Scientific Reports, 13(1), p.14183.

[29] Abdullah, S.F. and Nawaf, S.F., 2023. Optimizing Data Security with Hybrid Scheme Based on LSB and DWT. Tikrit Journal of Engineering Sciences, 30(3), pp.190-199.

[30] Jebur, S.A., Nawar, A.K., Kadhim, L.E. and Jahefer, M.M., 2023.Hiding Information in Digital Images Using LSB Steganography Technique.International Journal of Interactive Mobile Technologies, 17(7).

[31] Prasad, S., Pal, A.K. and Mukherjee, S., 2023.An RGB color image steganography scheme by binary lower triangular matrix.IEEE Transactions on Intelligent Transportation Systems, 24(7), pp.6865-6873.

[32] Zheng, Z., Hu, Y., Bin, Y., Xu, X., Yang, Y. and Shen, H.T., 2022.Composition aware image steganography through adversarial self-generated supervision.IEEE Transactions on Neural Networks and Learning Systems, 34(11), pp.9451-9465.

[33] Kataria, M., Jain, K. and Subramanian, N., 2023, May.Exploring advanced encryption and steganography techniques for image security.In 2023 11th International Symposium on Digital Forensics and Security (ISDFS) (pp. 1-6). IEEE.

[34] Hegde, S., Sunag, P. and Varun, R.P., 2023, March.Exploring the effectiveness of steganography techniques: A comparative analysis.In 2023 3rd International Conference on Smart Data Intelligence (ICSMDI) (pp. 181-186). IEEE.

[35] Raj, U.S. and Maheswaran, C.P., 2023, April. Secure file sharing system using image steganography and cryptography techniques.In 2023 International Conference on Inventive Computation Technologies (ICICT) (pp. 1113-1116). IEEE.

[36] Aslam, M.A., Rashid, M., Azam, F., Abbas, M., Rasheed, Y., Alotaibi, S.S. and Anwar, M.W., 2022, January.Image steganography using least significant bit (lsb)-a systematic literature review. In 2022 2nd International Conference on Computing and Information Technology (ICCIT) (pp. 32-38). IEEE.

[37] Rahman, S., Uddin, J., Khan, H.U., Hussain, H., Khan, A.A. and Zakarya, M., 2022.A novel steganography technique for digital images using the least significant bit substitution method.IEEE Access, 10, pp.124053-124075.

[38] Xie, J., Wang, H. and Wu, D., 2022.Adaptive image steganography using fuzzy enhancement and grey wolf optimizer.IEEE Transactions on Fuzzy Systems, 30(11), pp.4953-4964.

[39] Malarvizhi, N., Priya, R. and Bhavani, R., 2022, June. Reversible Image Steganography Techniques: A Performance Study.In 2022 7th International Conference on Communication and Electronics Systems (ICCES) (pp. 780-787). IEEE.

