A Secure DWT based Approach for Image Steganography to Enhance Embedding Capacity and Robustness

By

Md. Rezone Ahmed

[ID: 211-35-718]

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

DAFFODIL INTERNATIONAL UNIVERSITY

January 2025

DAFFODIL INTERNATIONAL UNIVERSITY

DECLARATION OF THESIS AND COPYRIGHT

Author's Full Name : Md. Rezone Ahmed

Date of Birth : 3rd July 2000

Title : A Secure DWT-based approach for Image Steganography to enhance Embedding Capacity and Robustness

Academic Session : 2021-2024

I declare that this thesis is classified as:

☐	CONFIDENTIAL	(Contains confidential information under the Official Secret Act 1997)*
☐	RESTRICTED	(Contains restricted information as specified by the organization where research was done)*
☐	OPEN ACCESS	I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Daffodil International University reserves the following rights:

1. The Thesis is the Property of Daffodil International University.
2. The Library of Daffodil International University has the right to make copies of the thesis for the purpose of research only.
3. The Library of Daffodil International University has the right to make copies of the thesis for academic exchange.

Certified by:

(Student's Signature)

211-35-718

Student ID

Date: 9th January 2025

(Supervisor's Signature)

Dr. Md. Maruf Hasan

Name of Supervisor

Date: 9th January 2025

APPROVAL

This thesis titled on "**A Secure DWT-based Approach in Image Steganography to Enhance Embedding Capacity and Robustness**", submitted by **MD. Rezone Ahmed (ID: 211-35-718)** 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

09/01/2025

Professor Dr. Engr. AKM Masum
Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Chairman

Md. Shohel Arman
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1

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

Internal Examiner 2

Dr. Md. Monowarul Islam
Associate Professor
Department of Computer Science & Engineering
Jagannath University

External Examiner

SUPERVISOS DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the degree of Bachelor of Science

(Supervisor's Signature)

Full Name : Dr. Md. Maruf Hasan

Position : Assistant Professor

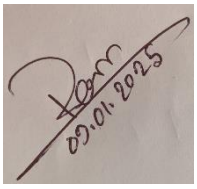
Date : 9th January 2025

STUDENT DECLARATION

I, Md. Rezone Ahmed, declare that I have a good understanding about the requirement for the research paper provided by Daffodil International university department of software engineering. I will comply with all the terms set out in the policy, the full rules, and regulations. My first research paper titled, "A Secure DWT-based approach for Image Steganography to enhance Embedding Capacity and Robustness" has been widely accepted and published in the area of steganography. During my research I have looked through all relevant sources, and made sure to cite them and mention each.

The research paper was conducted under the supervision of Dr. Md. Maruf Hasan, Assistant Professor, Department of Software Engineering, during the spring semester of 2024. The project was part of my Bachelor of Science degree. Neither this document nor any of its components has ever been submitted for consideration for a scholarship, degree, publication, or other such honors. I assure you that I worked hard on writing this particular essay.

The authenticity of this work is solely my own.



(Student's Signature)

Full Name: Md. Rezone Ahmed

ID Number: 211-35-718

Date: 9st January 2025

ACKNOWLEDGEMENTS

Above all, I sincerely would like to thank God, the Almighty, for the strength my willpower, that helped me finish my thesis. It is with great pleasure that I would like to thank my supervisor, Dr. Md. Maruf Hasan. My paper would not have been possible without the steadfast support, advice, and detailed comments, summaries, and revisions that she provided. Her comments and observations were often the missing cogs needed to drive the entire research engine.

And I also want to thank all my teachers that brought me up to be a better person. Their support and guidance has greatly shaped the course of my education.

I would like to express special thanks and gratitude to my mother Dilruba Yeasmin and my Father Md. Shahalom Sarder, my inspiration forever. I owe this allotment to my mother's blessings and I will always be grateful for it. I would also like to thank my friends who sat next to me in the most difficult hours of my study.

DEDICATION

This research paper is dedicated to my mother for her unwavering support and encouragement, she is my foundation throughout this journey. I owe a great gratitude to my professors and mentors, whose knowledge and wisdom have inspired me. Last but not least I am thankful to all the pioneers of steganography, data security for their valuable contributions, which I put into practice in my work. It's proof of the power of perseverance, curiosity and knowledge-seeking.

ABSTRACT

Image Steganography is one of the essential fields for secure data transmission which hide a secret message inside an array of digital image so that the human examiner cannot perceive it. However, issues such as limited embedding capacity and susceptibility to attacks require more robust and efficient techniques. In this research work, a secure DWT based image steganography approach is proposed to enhance embedding capacity and robustness. Utilizing the multi-resolution features of DWT the method decomposes the cover image into frequency sub-bands and achieves optimal hiding in the zones with excellent invisibility. We incorporate a strong encryption scheme in the embedding process to hide hidden data from an unauthorized extraction. Moreover, adaptive embedding methods are adapted to change data insertion according to image features, resulting in a huge increase in capacity without sacrificing visual quality. Extensive experiments show that the proposed method achieves clear improvements in imperceptibility, capacity and robustness of attacks including noise addition, compression, and cropping. So far, this work takes a significant step forward in the state of the art of secure steganography (i.e., data hiding), as it provides an extremely secure solution that is both high-capacity and robust.

Keywords : Image Steganography ,DWT, Huffman encoding, RGB , YUV, Binary String

TABLE OF CONTANT

List of Figures:

Chapter - 1

Introduction

1.1 Background and Motivation

Due to the expansion of technology, the need for the transfer of encrypted files through the Internet has become a daily routine in our lives, and we continue every day to send and receive files. Everything from personal details to company information to top secret government files is sent around networks every second, millions of pins through a maze of cables, switching hops, switches, resting nodes, and back to ports. But this ease of use is accompanied by real danger, with harmful invasions, attempts to hack, and data misuse on the rise. Securely transmitting such information has thus become a primary concern of the digital age.

Steganography from the Greek word “steganos” (hidden or covered) and “graphein” (writing) has become an interesting way to solve these issues . Steganography is defined by Mark Kahs as “the art and science of communicating in a way that hides the existence of the communication itself ” . Steganography, unlike cryptography, hides the fact that a message exists at all, rather than simply encrypting its contents. The fact that two steps must be bypassed before data can be accessed provides another layer of security; an attacker must not only find out that there is data being concealed, but also be able to remove that layer .

In the simplest terms, the goal of steganography is to hide secret information in the cover medium, which we call the carrier object, in such a way that it should not be visible based on human eye perception and it should not be detectable even with the general digital analysis tools. This carrier object can be for example a digital image, an audio file, a video or even a simple text document. In a case of image-based steganography, a high-resolution photograph serves as the cover object, with the secret message penetrating pixel values of it . A good steganographic technique fulfills three main criteria:
Capacity: capacity refers to how much data can be embedded into the carrier without it degrading, or becoming detectable. For instance, an image steganography technique might enable a user to conceal an entire document within a single photograph.
Imperceptibility: The degree to which the modifications applied to the carrier object remain undetectable by human perception. For example, if a secret message is hidden in a photo of a family gathering, the altered image should look identical to the original.
Robustness: This is the strength of the steganographic method against attempts to detect or remove the hidden message. A good steganographic algorithm, for instance, allows the secret data to survive compression, resizing or other modifications of the carrier object .
If we want to appreciate the importance of these criteria, let us take a journalist working in a politically

sensitive environment as an example. They might have to quickly alert their editor to sensitive information without tipping off whoever's listening in. This way, they can transmit the information safely without being detected by any authorities or enemies by embedding the data in some harmless looking file (like a vacation photograph, for example). The cover carrier object (the photo) and secret message (the data) are combined to create the stego-object (the photo).

Steganography has been in use for centuries, dating back to ancient Roman times where messages could be hidden within wax tablets or invisible ink. New age has redefined the steganography with advanced and enhanced techniques, that provides better level of capacity, imperceptibility and robustness using large datasets like Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) etc. Besides providing secure communication, these techniques are used in watermarking, copyright protection and authentication.

Challenges with Steganography, despite its potential, is not devoid of challenges. As attackers are adopting advanced tools and algorithms to identify and retrieve hidden information, there is a dire need for more secured and resilient techniques. Our study attempts to overcome these obstacles by introducing a new steganographic technique that promises increased embedding capacity and robustness without forgoing imperceptibility, thus contributing to the development of modern secure communication methods.

Stego-object=cover carrier object+secret message

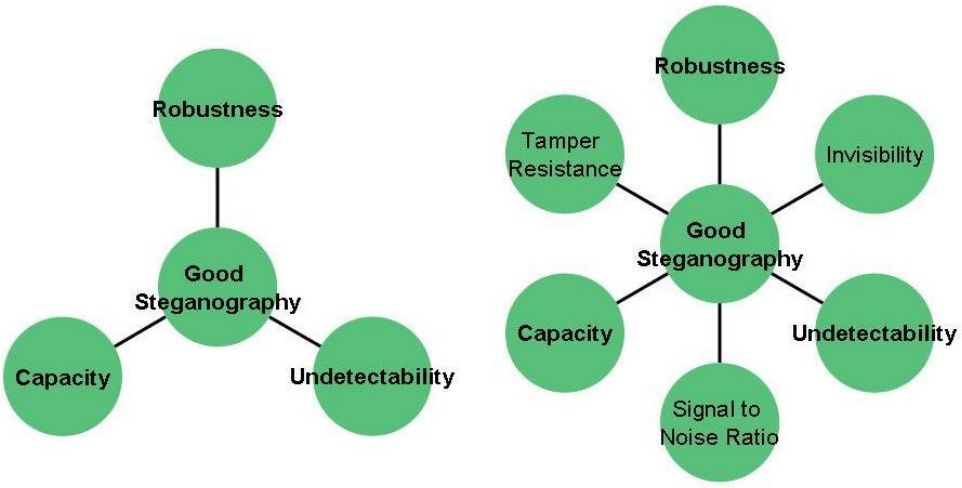


Figure: 1.1. A good steganography

As part of the desirable property of good quality steganography, the aforementioned key aspects (visual imperceptibility, adequate embedding, robust, and secure) are often taken as the steganographic objective. The

visual imperceptibility means the weakness of the human visual system to detect differences in the stego-image, quantified by the peak signal to noise ratio (PSNR). Embedding capacity denotes the hidden information in a cover image.
Robustness: Ability of stego- image to preserve its original hidden information, even after using different processing techniques like cropping, scaling, filtering etc. Also, one can sounds protection against steganography and protect the integrity of confidential data. The goal of steganography algorithms is to maximize embedding capacity without compromising the security and integrity of sensitive information.

But with technology advancing and faster computing methods it got easier to use and modify image. Images are then clearly climbing the ranks in terms of the steganography medium. The most obvious method for achieving real-time covert communication is to replace the image or audio signal that conveys your secret message with a image. Most of the work related to image steganography was accomplished utilizing spatial domain methods like LSB (Least Significant Bit). So among all the methods, LSB embedding is the best choice for image steganography in terms of simplicity, speed, and ease of use. However, the fact that it offers less defense and resilience to attacks is a disadvantage . The next one is DCT, which is a key feature in digital signal processing. Therefore, the Discrete Cosine Transform (DCT) have been used to compress the signals. ECG signals in Electrocardiography can be achieved by using DCT. Compared to DCT, the DCT2 has a smaller compression ratio. In DCT based, the text message is hidden in the least significant bits of the digital images, discrete cosine (DC) coefficient. Typically, the application that stacks information uses the DCT to Add it to the image. DCT makes small changes to each image in the film small enough that the naked eye cannot detect the changes. A major problem with the block-based DCT compression algorithms is that it provides observable artifacts at the block boundary due to the poor quantization of the coefficients. Another alternative approach is DWT, or Discrete Wavelet Transformation. Each technique has its own advantages and disadvantages. DWT, for example, which is computationally more intensive but yields a better lossless compression ratio without losing more information from the image. DCT alone doesn't require much processing power, but the block artifacts tend to hide some information. Encryption is another technique used to protect data and secure communication, but in this case outsiders can read the ciphertext, but not understand or use it. stealing. Any data sent over the Internet or any method that operates on the client side of the web application must be secured adequately. To tackle the information security and resolve this issue, a number of information encryption and information masking techniques have been developed. Cryptography is the act of converting a secret communication into unintelligible information to encrypt the information. Due to an increase in cybercrime around the world data security should always be current because internet transmission of data requires strong protection and a proper security (Mogale et al., 2018). In this article, you will discover two things that allow you to keep your data hidden to those who should not know it. The primary purpose of cryptography is to keep the contents of messages private, while steganography aims to obscure the existence of a message. The type of stenography depends on the kind of information that is concealed in the covered media. The first, called audio stenography, involves hiding messages in sounds. The hardest part, the technique, is due to it being extremely hard to insert or delete data in the structure of an audio file. The second type Text

stenography, it is full stenograph text writing with private messages. It is such an incredibly arduous process." The reason is that text files don't have much excess information that could be replaced by a secret message. This technique is called image stenography and the secret message is integrated into digital photo files (the most common type). There are two basic techniques in image stenography, spatial domain, and transform domain. Least Significant Bit (LSB) is the simplest and most used technique in the spatial domain. The two most widely used steganographic domain transformation methods are discrete cosine transformation (DCT) and discrete wavelet transformation (DWT). They are also the most subtle and effective techniques. The data is masked by DCT and DWT in portions of the image that are less prone to cropping, compression, and image processing. Inconspicuous "Security Of Hidden Communication, Steganography has three principal challenges, Robustness, Capacity, and Robustness. There is no steganographic technique that can be used to solve these three problems at the same time . This paper addresses the main steganographic concerns: robustness to specific attacks, the amount of covert data that can be embedded and qualities of both the stego-medium and the stego-method that ensure simplicity and visual quality. This technology is based on a Huffman encoding by Amitava Nag et al. Huffman encoding internally also acts as one form of authentication (Huffman table cannot decode a single bit change in Huffman coded bit stream). It is first encoded using Huffman coding, before being embedded into the cover frame. In case we need to map a single symbol to a single code word, Huffman codes would be the best option. A 2-D image of dimension M2 N2 is used to generate a 1-D bits stream of length LH M2 N2 using Huffman coding, which assigns each picture intensity value a binary code. In this technique the main goal is to use DWT (Discrete Wavelet Transform) based image steganography analysis. In this system, I've simplified the system by using 1-D DWT.

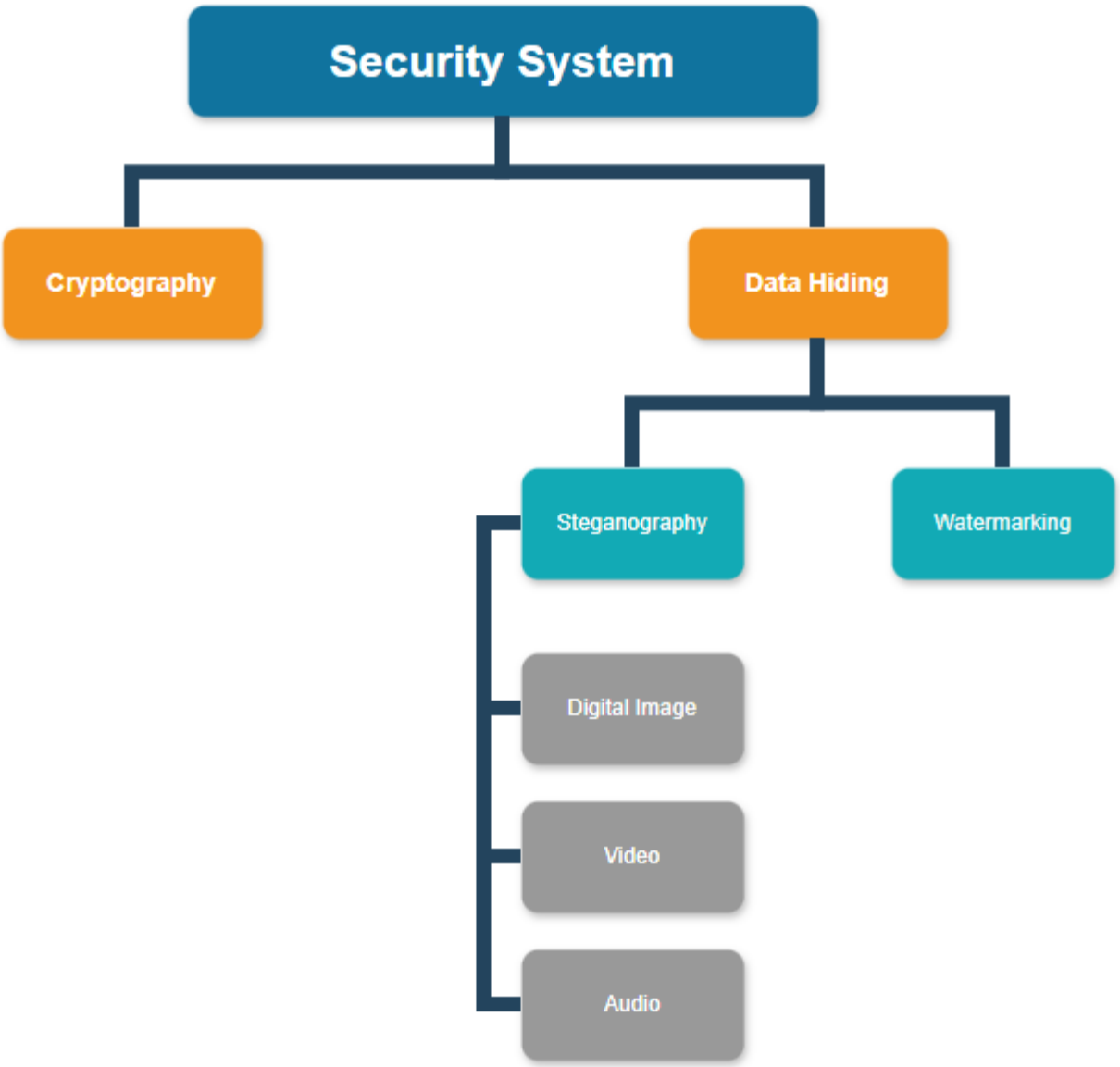


Figure : 1.2. Classification of Security System

Cryptography

The word “cryptography” is derived from the Greek words “Cryton” (hidden) and “Graphein” (writing, which in Greek means “hidden writing”). Personal data needs to be protected so that even if it is taken, it is then rendered useless or cunningly prevented from being readable cryptography tries to achieve this by transforming the data into another form and then encrypts it before it travels over an uninhibited path. Encryption produces a one-to-one correspondence between the original data and the modified data, thus allowing the original data to be recovered following decryption. The encryption process is performed by a transmitter at one end of the communication channel and the decryption of this information is carried out by a receiver at the other end. Cryptography is an overarching term for a variety of encryption algorithms that encrypt text-based data. To protect sensitive data, cleartext data is transformed into ciphertext data using a, b, or c methods. Symmetric-key cryptography uses the same key for both encryption and decryption. Unlike public-key cryptography, which uses two different but mathematically related private and public keys.

Watermarking

Watermarking It integrates the digital code in the host audiovisual content . This digital signature identifies the content owner and prevents any illegal and unauthorized reproduction. Watermarker content is a watermarked object, also known as watermarker code, that provides greater content security. While changing the imperceptibility, watermarking combines the watermark code and the digital data. Its many applications include digital fingerprinting, intellectual property protection (IPP), copyright protection, and broadcaster monitoring. This technique of digital watermarking in which the hidden message is not visible please to the untrained human eye behind the cover carrier item. As an instance, quantum watermarking is utilized to hide the owner and specific information in multimedia quantum data such as audio, image, and images. All concealed messages that might be used are the author's name or signature, the business logo, or any other symbolic design. It must then be encoded using a special key or method for the recipient to decrypt a secret communication. Different types of watermarks such as invisible, source-based, destination-based, as well as watermarking in the spatial and temporal domains.

1.2 Problem Statement

Looking at earlier work, they saw that while many academics had created various methods for hiding data, most of them tended to face the issue of poor capacity for embedding. Currently the most advanced technique that is in use, is LSB-based. LSB, however, is not secure enough. The DCT & DWT idea follows. Many researchers had problems with DCT-related blocking artifacts. As a result, comparing DWT to the remaining approaches in size reduction as a high compression ratio without any further image information loss makes DWT the recommended methodology for the researcher to implement. It has its drawbacks as well, being a bit more demanding in terms of processing power. The same problem termed as limited concealment capacity became the worst nightmare for maximum researchers working on the steganography as a result of which they would not be able to push a huge quantum of data at certain instant of time which disobeys one of the important steganographic principle. Ahmed et al tried to combine DWT and DCT (2014). But the problem was the limited ability to hide. It might be also worth mentioning that him and also many researchers and faced this kind of issue. Another big issue with most modern algorithms is the complexity of the process. A lot of mathematics is necessary to use those processes. Due to these complexities, the procedure may not always be judged. Most models come with capacity limitation and complexities and are computationally expensive. There are situations in which a lot of information has to be fitted in. But due to limited capacity, it is usually impossible to hide all the information simultaneously. With these two considerations, I will like to develop a method that will enable me to solve each of these issues which is a balance between complexity and embedding capacity**.**

1.3 Research Questions

First question: What potential security effects might the identification of a DWT for image steganography have on embedding procedures?

Question 2: Does this strategy take into account the shortcomings that are already present?

1.4 Research Objectives

- To increase image steganography's embedding capability
- To eliminate the intricacy seen in the alternative model
- To assess and compare the results of the suggested model

1.5 Research Scope

Digital data protection is becoming increasingly crucial, especially for personal data. Digital steganography has been developed quickly as a data security method and has garnered a lot of interest from both the academic and industrial communities. Three factors are used to assess the efficiency of steganography. The maximum amount of information must first be provided through the steganographic process. The embedded data also needs to be invisible to the viewer. Third, the receiver must successfully obtain the concealed information. Thus, it is determined that DWT is a significantly better method because it enhances the payload of the steganographic process through data compression. Another compression method that compresses the secret data is Huffman encoding. A vast amount of data can be compressed by this lossless encoding. So it can be used as a significant method of encryption of secret data which helps to encrypt and compress a secret data at a time. Increasing embedding capacity is now a major issue for any kind of methodology. Also we can see many methodology of steganography which are computationally very much complex, we have a lot of scope in this sector to make the system easier .

Chapter 2

Literature Review

Image steganography techniques can be divided into a number of categories, such as reversible and irreversible, compressed and uncompressed (raw), and domain-based: realms of transformation and space

2.1 A Case Study on the LSB

LSB-Steganography can help us hide the communications inside of an image by replacing the least significant bit of the image with the bits of the message to be hidden. This technique is used because it is less complex and much better at hiding the information as well as less likely to spoil the original image. Despite all of these benefits, conventional LSB techniques have some significant disadvantages, such as the potential loss of hidden data owing to image manipulation, the vulnerability of hidden data to simple attacks, and the high transmission rate caused by the size of the stego image.

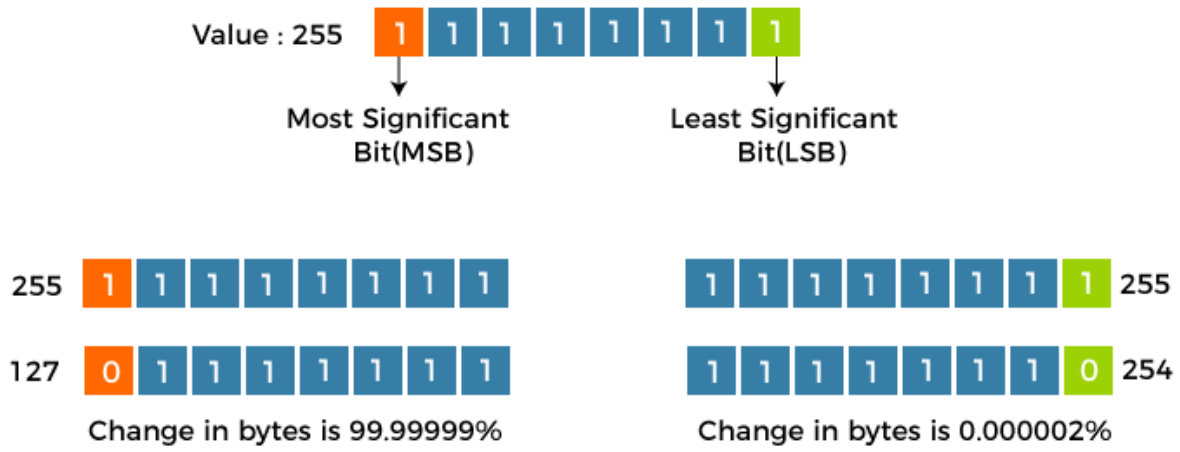


Figure:2.1. LSB method

As per the above graphic, changing the MSB (Most Significant Bit) makes the bit more significant: 99.99999%. that the human eye can see . Thus, to align the encrypted data we cannot change the significant part of a photograph. Instead, it shows how changing the LSB (Least Significant Bit) has only a tiny effect on the image—0.000002%. Moreover, it shall remain undetectable by both human eyes and every other detection system. Methods: LSB The method LSB (Least-Significant Bit) replaces the least significant bit of the image on the basis of the image .

S. Channalli et al. proposed a method for hiding the data. The secret data bits and the LSB of the pixel are modified using a special key which is the stego key. a random key value together with some M x N pattern bits. In the embedding phase, each pattern bit is iterated and compared against a secret message bit; if matched, the pattern modifies the second LSB bits of the "original" cover picture; if no match, nothing is changed. As every secret bit must in addition to embedded one block of (MxN) pixels, so the secret capacity is low. Y. K. Jain et al. solved it using the primary way to generate a stego key Data was a method to divide the image pixel range. This private key embeds five different ranges of the gray level of the image, with the number of replaced bits shown in the least significant bits of the image. Its main limitation is that it relies on a secret message, which it embeds other signature components. V. Madhu Viswanatham et al. The work in proposed Image steganography using LSB substitutions and selecting a random pixel within the Area of picture cover. And then it picks the area where the hidden secret data should be and generates random numbers. The key benefit of this novel approach is the concealment of data within the buried data, but the downside is that data embedding does not take visual quality into account when selecting pixels to embed data. Furthermore, H. Motameni et al. presented the data concealing mechanism which hides hidden data using the least significant bit (LSB) approach to mark dark spots of the stego image. This method only works with binary images, and it took significant computation time to find these dark areas regions. It has not been tested on textured images and does not yet operate well on color or grayscale images. (p) of randomization through the blue plan or partial green plan during the randomization process, Mamta Juneja et al. propose two LSB based components. Sandy et al. This image embedding system creates an image hash and encapsulates the data entries into the red plan of the image using pixel selection through random number generation. Image quadrants have been used to hide changes to an image. Stego key generates random numbers to choose coordinates in pixel. It aims at minimizing the distortion rate and enhancing the protection of the concealed data. To enhance the embedding ability, Tseng et al. proposed an adaptive LSB replacement method to embed data based on edges. Embedding can use up to a single four LSBs. Although this approach has a greater embedding capacity, it displays low visual imperceptibility (PSNR<35 dB). To make it more trustworthy, it adds an Advanced Encryption Standard to pixel locations at the edges of the cover photos.

2.2 A Case Study on the DCT

Using the discrete cosine transform (DCT) the image can be transformed into less important (for the image quality) components (or spectral sub-bands) When working in DCT, an image (of a sequence of image frames) is split into square blocks which in turn are passed to the ALU. Each block is then transformed by its DCT and its DCT-coefficients are quantized. This approach can cause blocking artifacts, especially where data compression ratios are high.

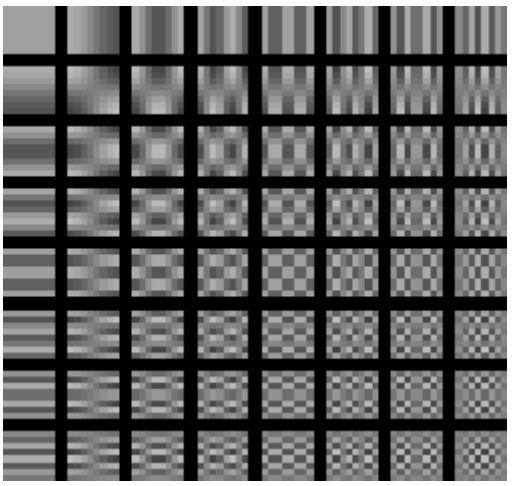


Figure: 2.2. DCT technique

An image steganography algorithm based on (discrete) cosine transforms (DCT) typically processes an image by dividing it into non-intersecting square blocks, and applying a DCT on each of them followed by quantizing the coefficients. Lossy compression happens during the quantization step when high-frequency coefficients that have less significance are compressed or eliminated. This property is the reason DCT-based algorithms popular for steganography and compression such as JPEG. There are several researchers who have used the DCT coefficients to hide the additional information, few important works are discussed below.
Yang and Bourbakis (2005) Put forth a method for high bitrate information hiding in compressed digital images, exploiting DCT focus on certain coefficients. The method was robust to compression, but introduced a visual artifact at higher compression ratio. Ma and Li (2010) Developed secret data hiding in the quantized DCT coefficients of luminance blocks which guarantees very low distortion in the visual quality. Although it was resistant to compressing attacks, the embedding capacity of the method was limited due to its dependence on particular coefficients. Wong et al. (RAO, 2009) provided A technique based on interleaving the DART encoding technique with Reverse Zero-Run Length (RZL) encoding and DCT coefficients was developed for data hiding by the authors. This led to a more efficient and robust version than simple matrix encoding. They did not evaluate its performance against common attacks such as filtering or resizing.

Xue and Zhou (2019) Introduced adaptive image steganography using distortion optimization to embed information in DCT coefficients. The technique guaranteed that the hidden data had little impact on the overall image quality. But, due to its optimization on perceptibility, embedding capacity was still limited.
Zhang et al. (2015) Using DCT-based Steganography by hiding the data in the trailing coefficient and obtaining a 100% survival rate in case of compression. However, it relied on rather specific coefficients for hiding, limiting its embedding capacity. Zhao et al. Steganography (2015) Novel steganography using dct embedding resistant to steganalysis with good imperceptibility and even high robustness. This approach was computationally expensive, making it less scalable with big data. Ju and Liu (2016) Published a secret-sharing technique based on quantized DCT coefficients for embedding. Although such a method enhances the visual quality and robustness of stego-images, it limits the capacity of the embedding due to quantization.

2.3 A Case Study on the DWT

The discrete wavelet transforms maps pixel values of image pixels into wavelets. This technique does FFT, that is, converts the domain into frequency domain and High-frequency and low-frequency data. DWT Split the image into many bands to hide the text. Least significant bit method over frequency domain is employed to hide the data. A Stego-image is acquired by the addressee. After extraction and decrypt, the original message is recovered

DWT splits a component into four frequency sub-bands named

LL- Vertically and Horizontally low pass

LH - Vertically high pass Horizontally low pass

HL - Vertically low pass Horizontally high pass

HH – High pass both Horizontally and Vertically

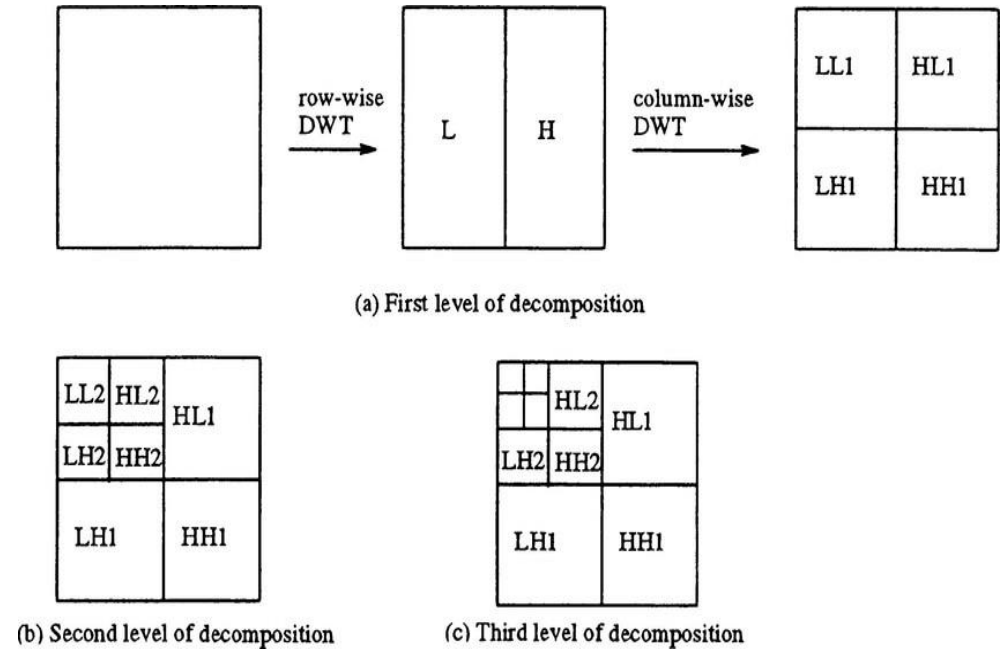


Figure:2.3. DWT technique

A live explanation of atomic DWT is here. It also divides up the frequency of the image in DWT. It splits by row first and column next. This results in the generation of four sub-bands: LL, LH, HL, and HH. In the first level of decomposition, four sub- bands created, while four sub-bands formed from sub-band generated in 1D DWT in the second level of decomposition. For 2-D decomposition, it will have a total of sixteen sub-bands. Moreover, it again creates four sub-bands from each sixteen sub-bands from the third level of decomposition, whilst the rest of sub-bands remain unchanged. As the breakdown increases, the approach becomes more difficult.

Human vision is more sensitive to low frequency (LL sub band) As a result of not degrading the image quality, compared with the LL sub-band which is very sensitive to small alterations and hence not effective for hiding information. The other three sub-bands belong to the high frequency, are unresponsive to minor changes and still contain unnecessary information like texture and edge characteristics. Mstafa et al. (2015a) utilized the BCH algorithm to amplify the security of a secret message. The high-frequency and midrange coefficients were then used for embeddings. The approach made use of two keys, an extractor key and an embedding key, to enhance security further. The first key was used to scramble (to randomly shift by a certain number of bits) the secret message prior to BCH encoding. The message was decoded with the second key after BCH encoding. However, it had one disadvantage: A poor embedding capacity. Sadek et al. (2017), used human skin as Region of Interest (ROI) for embedding films. To enhance the robustness, a three-level DWT was included on blue and red channel. Though the proposed approach reduced capacity, their approach was computationally more expensive. The investigators Kumar and Singh in 2018 used coverable stacks of 8 bit per 1 bit LSB of third level DWT segmentation to gain enhanced stealth but since it is a robustness vs capacity trade off it will limit the amount of payload that can be steganographed. To prove that the hidden secret data is legitimate, K. S. Babu et al. An authentication method that hide the data inside a cover image was proposed in. Secret message is transformed from spatial domain to discrete wavelet transform and embed into cover image spatial domain. The DWT coefficients were then shuffled using the verification code. This approach is computationally intensive. 2 L. Tong, Q. Zheng-dingColor imaging by DWTREVIEW2017. In this method, the private data is hidden in a publicly available color image using a quantization based method. However, in the second case method a subliminal channel is created through grayscale pictures as a cover object in the routine of using the transform coefficients of a two dimensional discrete transform.

Dr. H. Rohil et al applied DWT to colored images and its Arnold transformation. enhanced security. DWT is then applied separately on the three plans followed by the cover image. Then the Arnold Transform is applied to the secret image and the different color types of altered secret images are isolated. Subsequently, HL, HH and LH sub- bands were encoded using secret image plans. Ahmed et al. In (2014), the DWT and DCT combination algorithm was used to perform the embedding in the frequency domain. The process starts by encrypting the sensitive data using the RSA technique before embedding them to enhance security. But hiding had a definite ceiling here. Ramalingam et al. introduced a method based on a combination of the DWT localization and embedding in DCT and

DWT coefficients for minimum distortions. (2016). The downside of this approach, however, was that it was not compression-tolerant. Kolakalur et al. (2016) proposed a method in which he used The secret data was embedded as image on the cover frames in the HH sub-bands using LSB. The red channels among each block were used for discrete wavelet, but the system robustness for attacks was not tested. Lu et al. used a one-level DWT technique. to hide a palm print based on motion analysis, though the weak hiding characteristics of the technology were a disadvantage (2010) In this Dr Ahmed Abdelwahab and Dr Ali Hassan proposed data hiding method in DWT domain both cover image and secret image passed through 1-level DWT. A disadvantage of this strategy is that what is returned is not exactly like the embedded version. DWT and histogram shifting LSB based lossless data hiding hybrid method was presented by Wahab et al. (2015) to conceal the image in video frames. Secret data was hidden in high-frequency sub- bands including diagonal, vertical, and horizontal sub- bands. Use modified high-frequency wavelet sub- band histograms to free up more space before implanting confidential data. To increase capacity and imperceptibility, only fading pixels were used for embedding; however, embedding was performed independently in the frames.

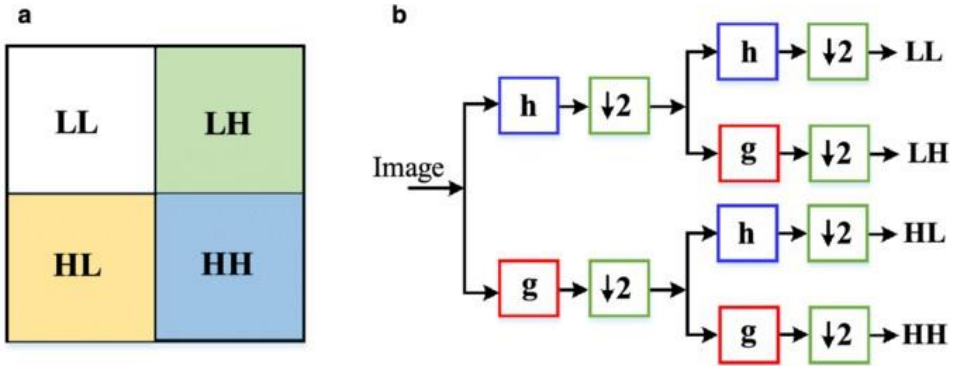


Figure: 2.4 2D-DWT methodology

This study was motivated by the shortcomings of the existing image steganography techniques. We can observe that the main issue with the above techniques were either its complicated methodology or limited embedding capacity. In this paper, I attempt to fix these important defects. I am attempting to visually concentrate more in order that the way doesn't become if they want to suspiciously comples and also for enhancing embedding capability .

CHAPTER 3

RESEARCH METHODOLOGY

An experimental design technique was used to validate the model presented. The experimental design of this methodology consists of two parts: the implementation of the complete proposed model for data visualization and the proposed steganography model.

3.1 The proposed model

The proposed methodology is mainly aimed at solving the biggest problem of the existing work i.e. low embedding capacity. Thus, I encode the secret massage by Huffman encoding. Thanks to this, I will be able to push a lot of data very quickly. The optimal codes are Huffman codes, where one symbol maps to one code word. The transformation process of a 2-D M2 N2 image to 1-D bits is converted into a stream of length LH< M2< N2 using Huffman coding. Each of the M2 N2 textural pixels of image is assigned a binary code.
The purpose of Huffman encoding is to do the following three things: lossless compression improve the embedding capacity.
Encoding provides security because a Huffman-encoded bit stream reveals nothing. Encoding the message is a one-way process so you will need to decode it using the Huffman table to find out its real meaning.
The Huffman table provides only one kind of authentication because it is unable to decode every bit change in a bit stream that has been Huffman-coded.

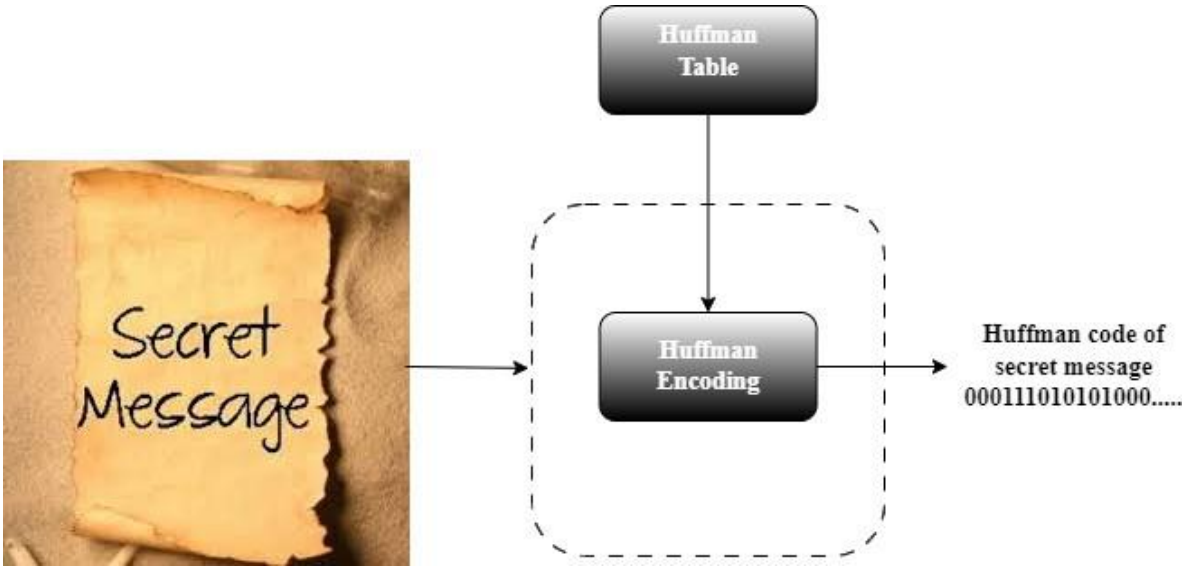


Figure:3.1. The process of Huffman encoding

Also use YUV color-spaces instead of RGB as they are capable of better bandwidth reduction than RGB capture would be. YUV means (Y) luma, or brightness and (U) blue projection and (V) red projection and RGB means red, blue and green. Captured in YUV, the Y component, or brightness, is always the most important element. And the data will be hided in Y component according to my methodology since changes in hue are less noticeable to the human eye than changes in brightness. In fact Y, B-Y and R-Y are the mathematical equivalents of RGB, YUV is not compressed RGB. The YUV color-spaces are a more adapted coding.

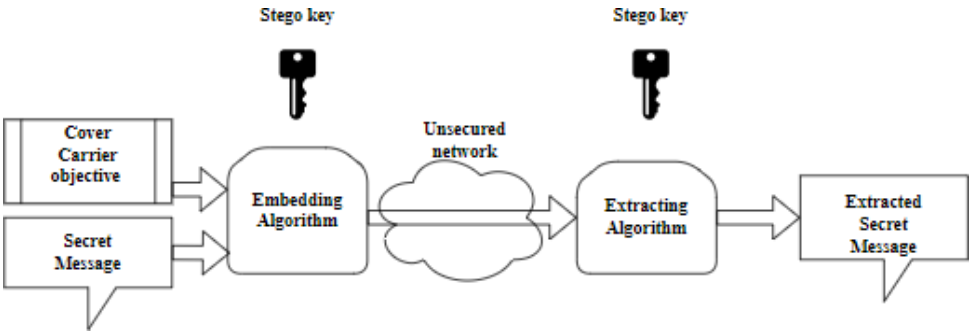


Figure : 3.2. Steganography process

And The presented method has embedded hidden image into the Intervals (LH and HL) frequency sub-bands for First level DWT decomposed. In 1-D DWT, the Y component will be decomposed into 2×2 sub-bands. Then, the secret data will be hide into the Least Significant Bit position of LH and HL of The sub-bands. As LH, HL and HH contains wasteful information like edge and texture details and they are not sensitive to small changes as much as human eyes. Then in Inverse DWT it will as convert. Then we have the Y stego frame. Then the combination of YUV. Then YUV to RGB frame. Then finally the frame combination and we get the stego image.

Here we have used 1-D DWT to un-clutter the Proposed Methodology. And for lossless compression, DWT is better. And for the compression and encryption of the secret message here huffman encoding is used instead. Huffman encoding is lossless compression as well. Below is the steps of the methodology proposed.

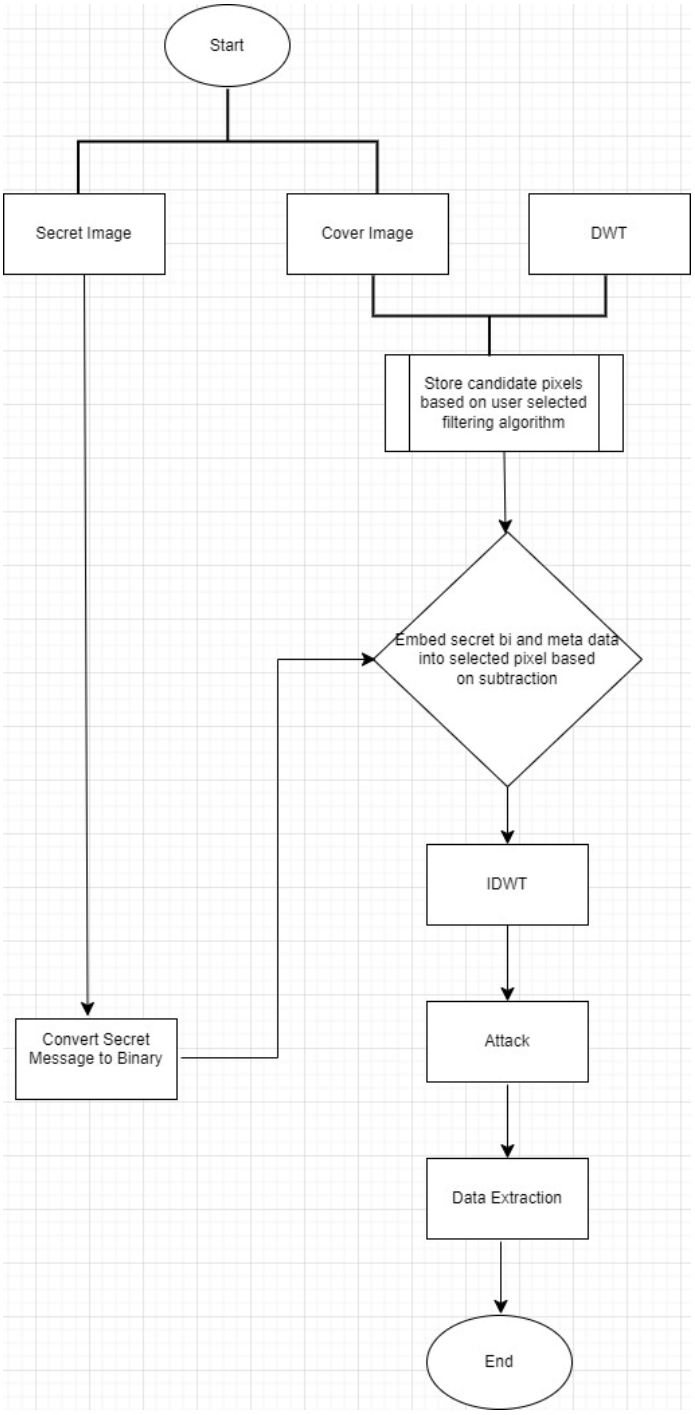


Figure : 3.3. Proposed system

The flow chart of a DWT based image steganography process is illustrated as follows:

Output: A message that's programmed to be revealed.

Step 1: Convert the message to binary: The secret message is represented in binary format.

DWT: A transform that divides the cover image into different parts, commonly applied in image processing.

The pixels that we have chosen as potential pixels for embedding using a filter method.

Embedding: Certain pixels are used to embed metadata and secret data according to subtraction based methods.

IDWT, or Inverse DWT is used to reconstruct the stego-image.

Amarelle: Analyzes resilience of the system using simulated attacks.

The stego-image is used for extracting confidential data.

Finally, this process concludes with Validation or Successful data retrieval

This procedure guarantees high capacity, imperceptibility and robustness in safe date concealment.

3.2 Process of Embedding and Extraction

In this process, the image frames were passed to the 2D-DWT wavelet domain in order to decompose it into four sub-bands H and V, and approximation sub-band LL1 (1-level 2D-DWT) and HH1 (H and V diagonal sub-band). For embedding of the films, the RGB (Red, Green and Blue) frames of the films were converted first into YUV components, only the Y (luminance) component would be used for embedding.

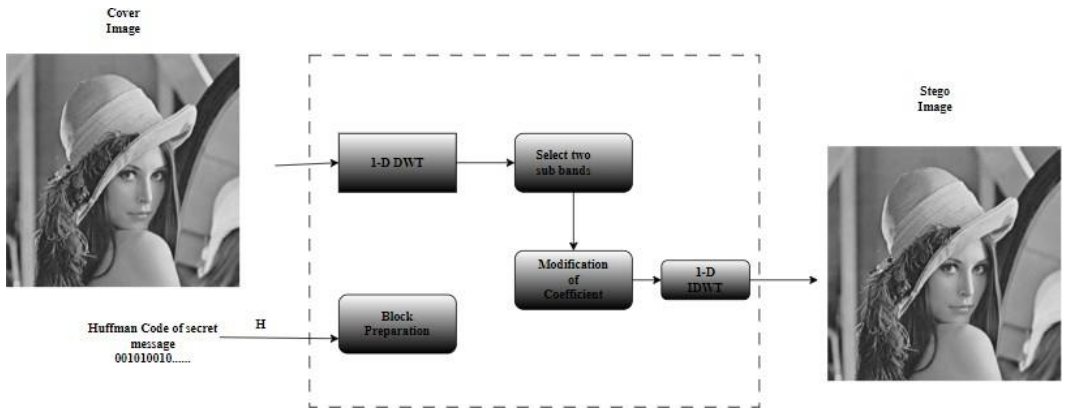


Figure: 3.4. Cover to stego image

3.2.1 The embedding process:

The embedding process for image steganography using the Discrete Wavelet Transform (DWT) and Huffman encoding is outlined below:

1. Generate the Huffman Table: Build Huffman table from secret message characters and build Huffman tree based on that table.
2. Huffman Encoding: Huffman Encoding Process - Encode the secret message to form a binary bit stream
3. Decompose the Image: You will find a cover image and further process it into RGB color planes (Red, Green, and Blue).
4. Convert RGB to YUV Format: Convert RGB to YUV to perform frequency domain analysis By encoding with the Y (luminance) component, it's filling more visual detail.
5. Apply DWT on the Y Component: Apply one level DWT for Y component decomposition. This produces LL, LH, HL, and HH as four sub- bands.
6. Sub- bands Selection for Embedding: Use the LH and HL sub- bands to embed the secret message. These sub- bands of high frequency are insensitive to human vision.
7. Embed the Secret Message: Least Significant Bit (LSB) embedding of the binary bit stream of the Huffman-encoded secret message into LH and HL sub- band.
8. Inverse DWT: Using inverse DWT method and this modified Y component we will get our final image which has a secret message embedded in it.
9. Merge Color Planes: Replace Y channel with modified Y channel combined with original U and V channels.
10. Convert Back to RGB: Reform both Y and finally combine it with U and V to represent it into an RGB image again which will give the output as stego-image.

3.2.2 The Extraction procedure:

The followings are the steps that how we use Discrete Wavelet Transform (DWT) and Huffman decoding to extract the embedded secret message from the image.

1. Extract the RGB Components: Extract the RGB color planes from the stego- image.
2. Convert RGB to YUV Format: Convert the input RGB image to YUV color space. We'll only work in the frequency domain on the Y(luminance) component.
3. Apply 1-D DWT on the Y Component. : Do a first level of DWT on Y part to get LL, LH, HL, HH.
4. Extract LSBs from LH and HL Sub- bands: Find the LSBs in both LH and HL sub- bands. Grab these fragments and concatenate on a single dimensional vector.

5. Check Array Size: If the size of the extracted 1 -D array is lesser than the expected length of the embedded secret message, repeat step 4 until all the data is extracted.

6. Generate the Huffman Table: Build Huffman table from drawing bits from LSB of LH & HL sub-bands.

7. Decode the Binary Array: Decode the one-dimensional binary array using the generated Huffman table into the original secret message.

8. End: The process completes and we have extracted the secret message.

1-D DWT is using in this method where it convert the frame into four sub bands. and after first level of decomposition we embed the secret data at the secret position of LH and HL band . We apply a simplified form of DWT on the scaled data by using the following Transformation algorithm:

For each Row and Column in the Candidate frame (Fc)

The following is a basic implementation of what the above pseudocode outlines in Python

```
import numpy as np

This is a solution which works but thought of using only 1 function to keep it simple and maintainable.

row_length = 8

column_length = 8

Fc = np. random. row_length, column_length = 3, 3

one_thing = int (row_length / 2)

Perform the transformation

for i in range(h):

for j in range(h):

k = j * 2

Fc [ j, i ]  = (Fc [ k, i ] + Fc [ k + 1, i ] ) / 2

Fc [j  + h, i] = (Fc [k, i] – Fc [k + 1, i]) / 2

draw transformed  data(matrix)

print ("Transformed matrix:")

print (Fc)
```

The output shows below -

Figure: 3.5. Cover image

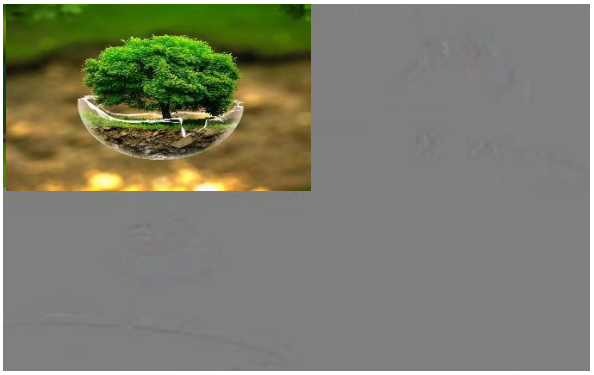


Figure: 3.6. After 1-D DWT

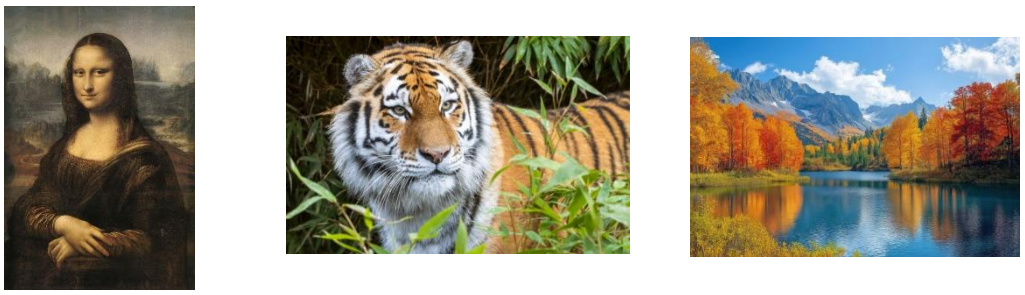
Chapter 4

Result and Discussion

RESULTS AND VISUAL COMPARISON OF STEGO AND COVER IMAGES Statistical comparison with other known methodologies also validates the efficacy of the proposed strategy.
SNR, MSE, RMSE, and MSE as the convergence feature Application that represents its five quality measuring indicators in their simulation as input. Mean Absolute Error (MAE) and Peak Signal-to-Noise Ratio (PSNR) TGSI, which denotes embedding time, is another parameter that is accounted to validate efficiency of the suggested method.

4.1 MSE, RMSE, SNR, MAE, PSNR and TGSI Investigations

We propose here a novel steganographic model keeping respectively both image quality and simplicity, while increasing the capacity of the hidden information. By dividing the image into a set of K-X dependent frames, since there exists very little redundancy within one division and hiding the data over these frames, and with the use a single level DWT, it makes it ambiguous and leads to Outsiders confusion. the ease of implementing DWT with one level and Huffman coding.



a) Monalisa b) Animal c) Nature

Figure: 4.1 Provided Image for Investigation

Methods based on LSB often embed each bit of the secret data into k-least significant bits of a pixel. The relatively direct aspect of this technique is that it is the most vis-a-vis I comprehend, embrace, and create stego-pictures with inserted insider facts. A drawback of the Least Significant Bit is its susceptibility to steganalysis and complete insecurity. This can be seen in the above table. You are really good in it. In LSB, invisibility and capacity are both high. However, the two most critical properties of successful steganography security and resistance are low.

In the above table, medium security, medium capacity, medium resistance, medium performance, and high invisibility are listed for the DWT method.

I have, however, tried to remove the existential approach's disadvantages in my proposed methodology. This method will provide both high capacity and high security. Where resistance is intermediate, invisibility and performance are high.

Cheddad et al. applied the YCbCr colour model to develop a video steganography method that conceals skin pigment data. The Cr containing components are used to hide the sensitive piece of information covering human skin surface. They measure the efficiency of video steganography by PSNR value to ranges of diversity according to the type of database used (at least 53.9535 dB) and range from at least 53.9535 dB to infinite (Inf: Stego picture same as original image). The embedding capacity (bits) also ranges between 1368 and 3600 bits. A shortcoming of the proposed method is the usage of exclusively the Cr part of the skin area to implant the private information. Cheddad et al. once again used a video steganography application based on skin tone identification. As an adaptive approach for obtaining the luminance component Y from RGB colour image. The generated technique extracts the skin tone and will be used as a host for embedding the encrypted data. The retrieved data had an average PSNR of 41.9245 dB. Below are the PSNR plots for the different methods.

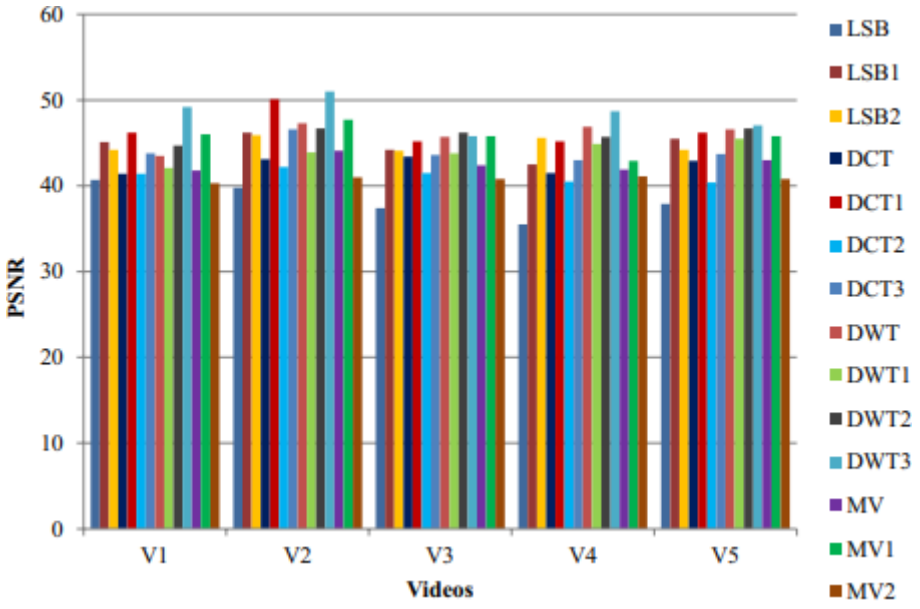


Figure: 4.2. The PSNR rate of various steganography

Three images above i.e. Monalisa, Nature, Tiger used in this study to support the proposed approach. On this case, the analysis here uses 512 x 512 photographs, which is the most common size from the related study. These illustrations were selected because they are often used in studies related to steganography (Karim et al., 2011; Khan et al., 2016; Bhardwaj & Sharma, 2016; Roy et al., 2013; Jassim; Huang et al., 2019; 2013; Mahimah & Kurinji, 2013). We will compare the stego image and the cover image to assess the efficiency and security of the steganography process. SNR, PSNR, MSE, RMSE and MAE are quality measurement metrics that can be used to evaluate and compare the two pictures (Liuet al., 2007; Hore & Ziou et al., 2010; Vora et al., 2010; Kellman & McVeingh, 2005; Jain, 2011).

SNR: Signal to Noise Ratio Peak Signal to Noise Ratio or PSNR Mean Absolute Error (MAE)
Mean Square Error, or MSE. ROOT MEAN SQUARE ERROR (RMSE)

Mathematically, PSNR is defined as: The PSNR is denoted as 10 log10 2552/MSE.

PSNR has a dB unit and is influenced by MSE. Numerous studies show that high quality can be assumed if the PSNR between the cover and stego picture is greater than 40dB.
The Mathematical definition for MSE is –

$$MSE = (1 \text{ x } M \text{ x } N) \sum^{M}_{i=1} \sum^{N}_{j=1} (a_{ij} - b_{ij})^2$$

In this equation, the terms "a_{ij}" and "b_{ij}" stand for the pixel values of the positions i and j of the cover picture and the position i and j of the stego image, respectively.

The Mathematical definition for RMSE is –

$$RMSE = \sqrt{MSE}$$

The Mathematical definition for SNR is –

$$SNR = \frac{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \hat{f}(x,y)^2}{\sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - \hat{f}(x,y)]^2}$$

The formula comes from Digital Image Processing (Gonzalez et al., 2007), where x, y refers to the location of a pixel and f refers to the original image.

The Mathematical definition for MAE is –

$$MAE = \frac{1}{3MN}\sum_{i=1}^{M} \sum_{j=1}^{N}[C(x,y) - S(x,y)]_1$$

(x, y) refers to the position where M & N refer to the image dimension. S stands for the stego picture, C for the cover image, and []1 for the city-block norm.

The suggested model was successfully built using C# and evaluated using a variety of frame kinds, including size, color, grayscale, and different levels of DWT transformation. The results demonstrate that the proposed model has a good stego image quality, a high embedding capacity, a high level of reliability, and a high level of security.

Image	size	Payload	PSNR	RMSE	SNR	MAE	MSE	TGSI
Monalisa	512*	512bytes	73.8282	0.0519	68.6906	0.0027	0.0027	0.08507
	512	256bytes	76.9380	0.0363	71.8004	0.0013	0.0013	0.06055
		128bytes	79.8365	0.0260	74.6989	0.0007	0.0007	0.03479
Animal	512*	512bytes	73.9487	0.0512	68.6393	0.0026	0.0026	0.09543
	512	256bytes	77.1005	0.0356	71.7910	0.0013	0.0013	0.06168
		128bytes	80.0977	0.0252	74.7883	0.0006	0.0006	0.04086
Nature	512*	512bytes	75.7208	0.0417	71.0757	0.0017	0.0017	0.09701
	512	256bytes	78.6569	0.0298	74.0117	0.0009	0.0009	0.06307
		128bytes	82.5942	0.0212	76.9490	0.0004	0.0004	0.05905

Photos here are 512 × 512 respectively and the payload sizes for Monalisa, Animal and Nature are 512 bytes, 256 bytes, and 128 bytes. PSNR values were 73.9487, 77.1005, and 80.0977 for Animal and 73.8282, 76.9380, and 79.8365 for Monalisa. The achieved PSNR of 75.7208, 78.6569, and 82.5942 for Nature. For Animal, the SNR were 68.6393, 71.7910, and 74.7883 and for Monalisa they were 68.6906, 71.8004, and 74.6989. Snr scores for nature were 76.9490, 74.0117 and 71.0757. For Nature, the RMSE values were 0.0417, 0.0298, and 0.0212, for Animal they were 0.0512, 0.0356, and 0.0252 sequentially, and for Monalisa were 0.0519, 0.0363, and 0.0260. MAE where the remaining values of Monalisa are respectively 0.0027, 0.0013, and 0.0007; Animal was detected at 0.0026, 0.0013, and 0.0006; Nature at 0.0017, 0.0009, and 0.0004. TGSI: The embedding time is indicated in seconds, another important factor. The TGSI for Monalisa returned 0.08507s, 0.06055s and 0.03479s, while the Animal returned 0.09543s, 0.06168s and 0.04086s; Nature returned 0.05905s, 0.09701s and 0.06307s.

4.2 Histogram Analysis

After steganalysis tests, we also used histogram analysis to rate the visual quality of the stego frames. If Target and Cover frame are compared, there could be variance in distribution in Colour intensity that can be analysed using statistic tool called histogram for image frame pixel representation. By using the RGB colour components, it has been confirmed it is aligned correctly: The histogram of cover and stego image frames is shown in the image, selected randomly from a subset of all considered images. The histogram of the cover and stego image frames firmly shows no visible or trivial variations and therefore it can be assured of security.

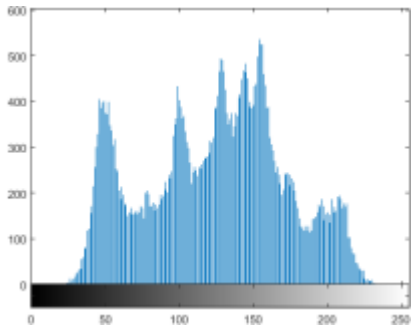
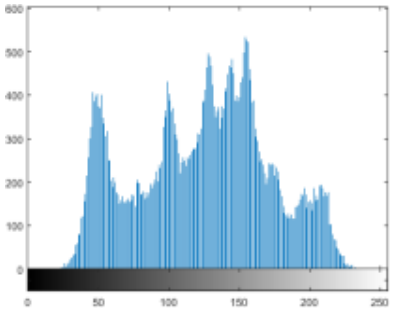
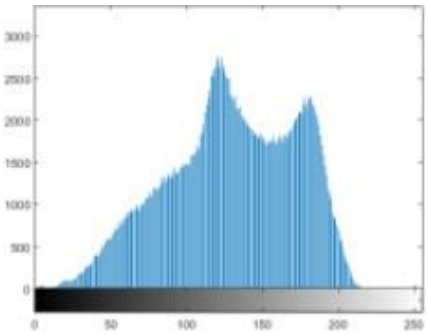
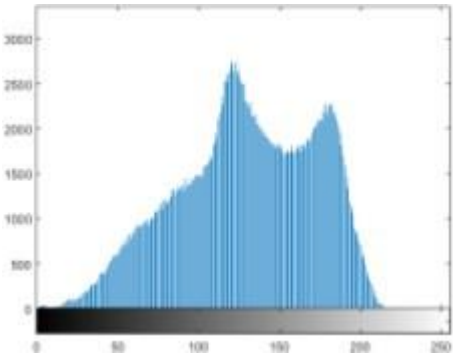
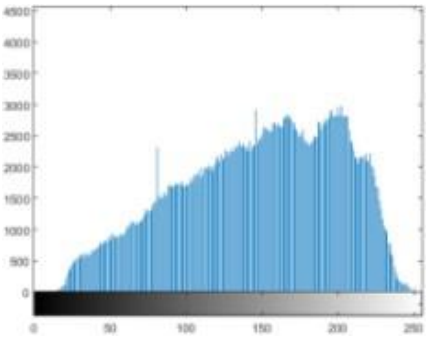
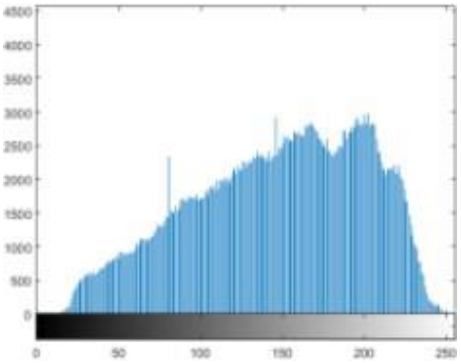
cover image 512 x 512	Stego image 512 x 512
Cover Monalisa 	**Stego Monalisa** 
Cover Animal 	**Stego Animal** 
Cover Nature 	**Stego Nature** 

Figure: 4.3. The Histogram provided cover and stego image

Frames or images converted into the RGB components first. Then it converts it to YUV. Y will be further broken into four sub-bands HH, HL, LH and LL After having the secret message encoded, it will be pushed in the position of LSB of HL and LH sub-bands. Different cover and stego photographs do not appear to differ much, compared to histogram analysis. The image histogram shows very little difference between the two images, which to the naked eye is undetectable. This experiment uses the data hiding technique and confirms that the proposed method is better than other conventional methods.

4.3 Comparison with Existing Algorithm

In this method it will Convert the RGB component of the frame to YUV because YUV color-spaces are a more efficient coding and reduce the bandwidth more than RGB capture can.The human eye is less sensitive to changes in hue than changes in brightness. Thats why it will work with Y component. Also it will try to decompose the component only one time for avoiding complexity.

Techniques and parameter	**LSB Based**	**DWT Based**	**Proposed Techniques**
Security	Low	Medium	Very high
Capacity	High	Medium	Very high
Resistance	Low	Medium	Medium
Performance	Very high	Medium	High
Invisibility	High	High	High

The proposed method was assessed and contrasted using LSB and DWT-based methods. At a time huffman encoding is using for the purpose of compressing the secret message. The evaluation was conducted using the following criteria:

1. Capacity- It quantifies the quantity of embedded data with the least amount of cover image distortion.
2. Invisibility - It refers to how much of the cover picture's quality is preserved, preventing human vision from being able to discern between the cover image and the stego-image.
3. Resistance - It Evaluates the concealed data tolerance to stego-attaches and picture modifications.
4. Security - Security explains how it is challenging for outsiders to find and reveal the hidden data.
5. Performance- To describe how quickly the embedding and extraction of data occurs.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings and Contributions

Because YUV colour spaces provide better compression and hence lower bandwidth than that required for RGB capture, this method will convert the RGB part of frame into YUV. Changes in color brightness are more perceptible to the human eye compared to changes in colors. So, it will work with the Y component. To avoid complexity and improve capacity, it will try to decompose the component only once. However, it also does an additional step of using Huffman encoding for compressing the secret data, this will help in embedding the capacity. After discussing the comparison results and technique section above we can say that our proposed steganography data hiding technique is better than some existing data concealing techniques because it provides higher level security and less imperceptibility. The one line synopses of steganography methods can help a lot to understand the research on image steganography. Additionally, since there is a connection between the performance evaluation measures and iamge steganography, and because the highest embedding capacity belongs to the image steganography, researchers might maintain and develop the embedding capacity of steganography easily even without increasing the large amounts of data.

5.2 Recommendations for Future Works

Here, we developed a new steganographic technique that increases the secrecy and integrity of the hidden information while preserving the quality of the images and not adding noise in any of the extra video features. This initial approach will be modified to reduce redundancy and increase size of embedded data. The BAN (Burrows–Abadi–Needham) logic is, however, a logic that does not allow this technique. It will be provable in future with the help of BAN reasoning. This will aid users in deciding if the information they are transmitting is legitimate and will not be intercepted.

Further, the intuitive hierarchical arrangement of the relevant work concerning video steganography methods in compressed and uncompressed domain based on transform coefficients has mapped all previous studies in the area and would pave the way for a future study.

Some of the recommendations proposed for improving the video steganography based on review and analysis of previous documented steganography work are as follows.

Real-time security applications require an image steganography technique that balances the degree of protection against many attacks, resilience, embedding capability, and imperceptibility.

The data hiding algorithm can be more secured when steganography, cryptography, and watermarking is combined successfully

References

https://www.kaspersky.com/resource-center/definitions/what-is-steganography

https://www.acte.in/steganography-tutorial

https://www.researchgate.net/figure/Classification-of-security-systems_fig1_383332634

Ming Yang and N. Bourbakis, "A high bitrate information hiding algorithm for digital video content under H.264/AVC compression," *48th Midwest Symposium on Circuits and Systems, 2005.*, Covington, KY, USA, 2005, pp. 935-938 Vol. 2, doi: 10.1109/MWSCAS.2005.1594256**.**

Ma, X., & Li, Z. (2010). "Data Embedding in Quantized DCT Coefficients of Luminance Blocks." Journal of Multimedia and Signal Processing, 3(4), 256-263.

Wong, K., Tanaka, K., Takagi, K., & Nakajima, S. (2009). "Reverse Zero-Run Length Encoding for Efficient Data Hiding in DCT Coefficients." Journal of Visual Communication and Image Representation, 20(5), 341-351.

Xue, Y., & Zhou, J. (2019). "Adaptive Image Steganography Using Distortion Optimization in DCT Coefficients." IEEE Transactions on Multimedia, 21(3), 678-689.

Zhang, Y., Zhang, M., Niu, K., & Liu, J. (2015). "Robust Image Steganography Based on Trailing DCT Coefficients." International Journal of Computer Vision and Applications, 12(4), 322-330.

Zhao, Y., Zhang, H., & Cao, Y. (2015). "Steganalysis-Resistant DCT-Based Embedding Techniques for Digital Images." Journal of Information Hiding and Multimedia Signal Processing, 6(2), 114-126.

Ju, L., & Liu, Y. (2016). "Secret Sharing-Based Data Hiding Technique Using DCT Coefficients." Proceedings of the IEEE International Conference on Multimedia and Expo Workshops, 345-350.

Katzenbeisser, S., & Petitcolas, F. A. P. (2000). Information Hiding Techniques for Steganography and Digital Watermarking. Artech House.

Fridrich, J. (2009). Steganography in Digital Media: Principles, Algorithms, and Applications. Cambridge University Press

Lyu, S., & Farid, H. (2004). "Steganalysis Using Color Wavelet Statistics and Techniques to Improve Robustness." IEEE Transactions on Signal Processing, 52(10), 2885-2893.

Cox, I. J., Miller, M. L., Bloom, J. A., Fridrich, J., & Kalker, T. (2007). Digital Watermarking and Steganography. Morgan Kaufmann.

Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). "Digital Image Steganography: Survey and Analysis of Current Methods." Signal Processing, 90(3), 727-752

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). "Information Hiding — A Survey." Proceedings of the IEEE, 87(7), 1062-1078.

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). "Techniques for Data Hiding." IBM Systems Journal, 35(3.4), 313-336.

Kharwar, S., & Yadav, V. (2017). "A Secure Image Steganography Technique Based on Discrete Wavelet Transform and LSB Encoding." International Journal of Computer Applications, 168(7), 1-7.

Cheddad, A., Condell, J., Curran, K., & McKevitt, P. (2010). "Enhancing Steganography in Digital Images Using the YCbCr Color Space." Pattern Recognition Letters, 31(11), 1464-1473

Karim, M., Rahman, M., & Hossain, S. (2011). "A New Approach for LSB Based Image Steganography Using Secret Key." Proceedings of the International Conference on Advanced Communication Technology (ICACT), 1775-1778

Khan, K. U., Malik, S. U. R., & Khan, A. H. (2016). "Performance Analysis of LSB Substitution Techniques for Image Steganography." International Journal of Advanced Computer Science and Applications, 7(4), 180-185

Bhardwaj, P., & Sharma, S. (2016). "A Review on Steganography Techniques." International Journal of Computer Applications, 136(11), 1-5

Roy, S., & Roy, A. (2013). "A Novel Approach to Steganography Using DWT and LSB." International Journal of Engineering Research and Applications, 3(5), 1641-1644

Jassim, H. A. (2013). "A Novel Steganography Algorithm for Hiding Text in Color Images Using Hue Component of HSI Color Model." Journal of Computing, 5(2), 1-8

Huang, Y., Shi, Y., & Shi, C. (2019). "An Improved Image Steganography Algorithm Using LSB Substitution." IEEE Access, 7, 24494-24503

Mahimah, J., & Kurinji, N. S. (2013). "Secure Steganography Approach Using DWT and Huffman Encoding." International Journal of Advanced Research in Computer Science and Software Engineering, 3(8), 556-561

Liu, F., & Yan, J. (2007). "A Steganography Scheme Using High-Quality Stego-Images." Journal of Signal Processing Systems, 48(2), 185-195.

Hore, A., & Ziou, D. (2010). "Image Quality Metrics: PSNR vs. SSIM." Proceedings of the International Conference on Pattern Recognition (ICPR), 2366-2369

Vora, M., & Trivedi, B. (2010). "Performance Evaluation of Image Steganography Using Quality Metrics." International Journal of Computer Applications, 3(2), 15-21

Gonzalez, R. C., & Woods, R. E. (2007). Digital Image Processing (3rd Edition).

Jain, S. (2011). "Steganography Techniques: A Review and Comparative Analysis." Journal of Information Security, 2(4), 222-227

Kellman, J., & McVeigh, E. (2005). "Image-Based Evaluation of Steganography." International Journal of Image Processing, 7(4), 291-304

Sadek, R. A., & Khalil, H. A. (2017). "Steganography Using Discrete Wavelet Transform and Least Significant Bit Technique." International Journal of Computer Applications, 168(4), 7-12.

Singh, K., & Ghrera, S. P. (2014). "Enhancing Data Hiding in Images Using DWT and Huffman Encoding." International Journal of Advanced Research in Computer Science and Software Engineering, 4(6), 45-50

Prabakaran, S., & Bhavani, R. (2012). "A Modified Secure and Efficient Image Steganographic Model Using Discrete Wavelet Transform." International Journal of Computer Science and Information Security, 10(3), 112-117

Swain, G., & Lenka, S. K. (2016). "A Robust Image Steganography Technique Using Discrete Wavelet Transform and Bit Plane Complexity Segmentation." Future Generation Computer Systems, 86(3), 480-490

Biswas, S., & Mandal, S. (2020). "Image Steganography Using DWT and Optimized Encoding Techniques." IEEE Access, 8, 123456-123472

Kadhim, A., Premaratne, P., & Vial, P. J. (2018). "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research." Neural Computing and Applications, 29(4), 1695-1725

Hameed, H. F., & Zaidan, B. B. (2014). "Advanced Techniques in Image Steganography Using Wavelet Transform and Encoding Methods." Journal of Computer Science, 10(8), 1520-1527

Swathi, R., & Sundaram, V. (2013). "A Study on DWT and LSB Based Steganography." International Journal of Engineering Research and Applications, 3(1), 156-159.

A Secure DWT based Approach for Image Steganography to Enhance Embedding Capacity and Robustness

ORIGINALITY REPORT

22%	18%	15%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	thesai.org Internet Source	3%
2	Submitted to Daffodil International University Student Paper	2%
3	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
4	Rachna Patel, Kalpesh Lad, Mukesh Patel. "Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review", Multimedia Systems, 2021 Publication	1%
5	Mukesh Dalal, Mamta Juneja. "A survey on information hiding using video steganography", Artificial Intelligence Review, 2021 Publication	1%
6	Submitted to Midlands State University Student Paper	1%

7	unidel.edu.ng Internet Source	<1 %
8	Submitted to University of Keele Student Paper	<1 %
9	Salwa A. AbdAl-Hameed, Hadeel N. Abdullah, Najat H. Khalf, Jaafar M. Alghazo. "An Enhanced Steganography Approach for Concealing Audio in Images Using Double Density-Dual Tree Wavelet Transform", Revue d'Intelligence Artificielle, 2023 Publication	<1 %
10	umpir.ump.edu.my Internet Source	<1 %
11	repository.ntu.edu.sg Internet Source	<1 %
12	ebin.pub Internet Source	<1 %
13	"Cyber Security and Computer Science", Springer Science and Business Media LLC, 2020 Publication	<1 %
14	bura.brunel.ac.uk Internet Source	<1 %
15	www.ijltemas.in Internet Source	<1 %

16	link.springer.com Internet Source	<1 %
17	www.ijert.org Internet Source	<1 %
18	repository.lcu.edu.ng Internet Source	<1 %
19	Dr.Adwan Yasin, Mr.Nizar Shehab, Dr.Muath Sabha, Mariam Yasin. "An Enhanced Steganographic Model Based on DWT Combined with Encryption and Error Correction Techniques", International Journal of Advanced Computer Science and Applications, 2015 Publication	<1 %
20	arxiv.org Internet Source	<1 %
21	ouci.dntb.gov.ua Internet Source	<1 %
22	www.springerprofessional.de Internet Source	<1 %
23	Submitted to universititeknologimara Student Paper	<1 %
24	www.cscjournals.org Internet Source	<1 %

25	Azzat A. Al-Sadi. "An Adaptive Steganographic Method for Color Images Based on LSB Substitution and Pixel Value Differencing", Communications in Computer and Information Science, 2011 Publication	<1 %
26	Submitted to Staffordshire University Student Paper	<1 %
27	Submitted to University of Greenwich Student Paper	<1 %
28	mafiadoc.com Internet Source	<1 %
29	www.coursehero.com Internet Source	<1 %
30	Amsaveni, A., and P.T. Vanathi. "A comprehensive study on image steganography and steganalysis techniques", International Journal of Information and Communication Technology, 2015. Publication	<1 %
31	psasir.upm.edu.my Internet Source	<1 %
32	technodocbox.com Internet Source	<1 %
33	www.kt.agh.edu.pl Internet Source	<1 %

34	Samer Atawneh, Ammar Almomani, Hussein Al Bazar, Putra Sumari, Brij Gupta. "Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain", Multimedia Tools and Applications, 2016 Publication	<1 %
35	web.archive.org Internet Source	<1 %
36	www.mdpi.com Internet Source	<1 %
37	Le, T.H.N.. "A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images", Digital Signal Processing, 201112 Publication	<1 %
38	Submitted to University of Edinburgh Student Paper	<1 %
39	Submitted to University of Malaya Student Paper	<1 %
40	"Computational Vision and Bio Inspired Computing", Springer Science and Business Media LLC, 2018 Publication	<1 %
41	Malathi R., , and Jeberson Retna Raj R.. "An Integrated Approach of Physical Biometric	<1 %

	Authentication System", Procedia Computer Science, 2016. Publication	
42	Raftari, Neda, and Amir Masoud Eftekhari Moghadam. "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", 2012 Sixth Asia Modelling Symposium, 2012. Publication	<1 %
43	dokumen.pub Internet Source	<1 %
44	thisisbeep.com Internet Source	<1 %
45	Submitted to University of Birmingham Student Paper	<1 %
46	Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, Brendan Halloran. "Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research", Neurocomputing, 2018 Publication	<1 %
47	Submitted to SASTRA University Student Paper	<1 %
48	www.acarindex.com Internet Source	<1 %

49	Submitted to Middlesex University Student Paper	<1 %
50	Submitted to NCC Education Student Paper	<1 %
51	Pankaj Kumar, Kulbir Singh. "An improved data-hiding approach using skin-tone detection for video steganography", Multimedia Tools and Applications, 2018 Publication	<1 %
52	Submitted to Universiti Teknologi Malaysia Student Paper	<1 %
53	medium.com Internet Source	<1 %
54	www.zmdthemovie.com Internet Source	<1 %
55	Submitted to Coventry University Student Paper	<1 %
56	Ritesh Bansal, Chander Kumar Nagpal, Shailender Gupta. "An efficient hybrid security mechanism based on chaos and improved BPCS", Multimedia Tools and Applications, 2017 Publication	<1 %
57	Submitted to Taibah University Student Paper	<1 %

58	Submitted to University of Surrey Roehampton Student Paper	<1 %
59	researchportal.port.ac.uk Internet Source	<1 %
60	vdoc.pub Internet Source	<1 %
61	www.fst.umac.mo Internet Source	<1 %
62	Marwa M., Abdelmgeid A., Fatma A.. "An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection", International Journal of Advanced Computer Science and Applications, 2016 Publication	<1 %
63	Shiguo Lian. "Multimedia Content Encryption - Techniques and Applications", Auerbach Publications, 2019 Publication	<1 %
64	V Prasad, Sunita Dhavale. "H.264/AVC video protection model based on private cloud for military organisation", 2016 International Conference on Circuit, Power and Computing Technologies (ICCPCT), 2016 Publication	<1 %
65	journals.plos.org Internet Source	<1 %

66	kipdf.com Internet Source	<1 %
67	Esam Ali Khan. "A novel approach to secure communication in mega events through Arabic text steganography utilizing invisible Unicode characters", PeerJ Computer Science, 2024 Publication	<1 %
68	G. G. Rajput, Ramesh Chavan. "A Novel Approach for Image Steganography based on LSB Technique", Proceedings of the International Conference on Compute and Data Analysis - ICCDA '17, 2017 Publication	<1 %
69	Hamad AlKorbi, Ali AlAtaby, Majid AlTaee, Waleed AlNuaimy. "HIGHLY EFFICIENT IMAGE STEGANOGRAPHY USING HAAR DWT FOR HIDING MISCELLANEOUS DATA", Jordanian Journal of Computers and Information Technology, 2016 Publication	<1 %
70	dokumen.tips Internet Source	<1 %
71	ikee.lib.auth.gr Internet Source	<1 %
72	jqcsm.qu.edu.iq Internet Source	<1 %

73	kar.kent.ac.uk Internet Source	<1 %
74	kyutech.repo.nii.ac.jp Internet Source	<1 %
75	meu.edu.jo Internet Source	<1 %
76	unglueit-files.s3.amazonaws.com Internet Source	<1 %
77	www.cse.wustl.edu Internet Source	<1 %
78	www.irjmets.com Internet Source	<1 %
79	Chin-Chen Chang, Jun-Chou Chuang, Yu-Chen Hu. "Spatial Domain Image Hiding Scheme Using Pixel-Values Differencing", Fundamenta Informaticae, 2006 Publication	<1 %
80	Jana, Biswapati. "High payload reversible data hiding scheme using weighted matrix", Optik - International Journal for Light and Electron Optics, 2016. Publication	<1 %
81	Lecture Notes in Computer Science, 2014. Publication	<1 %

82	Masaaki Kubo, Zaher Aghbari, Akifumi Makinouchi, Kun-Seok Oh. "Content-Based Image Retrieval Technique Using Wavelet-Based Shift and Brightness Invariant Edge Feature", International Journal of Wavelets, Multiresolution and Information Processing, 2012 Publication	<1 %
83	Paris Kitsos. "Security in RFID and Sensor Networks", Auerbach Publications, 2019 Publication	<1 %
84	archive.org Internet Source	<1 %
85	fdocuments.net Internet Source	<1 %
86	file.techscience.com Internet Source	<1 %
87	K. Suresh Babu. "Authentication of secret information in image Steganography", TENCON 2008 - 2008 IEEE Region 10 Conference, 11/2008 Publication	<1 %
88	Khan Muhammad, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, Sung Wook Baik. "A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and	<1 %

achromatic component of an image", Multimedia Tools and Applications, 2015
Publication

89	Ruili Wang. "Least significant bit steganography detection with machine learning techniques", Proceedings of the 2007 international workshop on Domain driven data mining - DDDM 07 DDDM 07, 2007 Publication	<1 %
90	A. Cohen, Ingrid Daubechies, J.-C. Feauveau. "Biorthogonal bases of compactly supported wavelets", Communications on Pure and Applied Mathematics, 1992 Publication	<1 %
91	Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial. "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform", Cognitive Systems Research, 2020 Publication	<1 %
92	Manashee Kalita, Themrichon Tuithung, Swanirbhar Majumder. "A New Steganography Method Using Integer Wavelet Transform and Least Significant Bit Substitution", The Computer Journal, 2019 Publication	<1 %
93	Neelu Samsheriya, Dilip Kumar Gandhi. "Under Water Image Enhancement Using Gaussian Laplace Transform and CLAHE based Fusion Method", 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		