Image Steganography Using Frequency and Spatial Domain Techniques for Data Hiding

A project report submitted as a partial fulfillment of the criteria for the degree of Bachelor of Science (Engineering) in Information and Communication Technology

Submitted By

ID:11909013 ID: 11909016 ID: 11909045

Reg:11909013 Reg:11909016 Reg:11909045

Session:2018-19

Department of Information and Communication Technology

Comilla University, Cumilla-3506.

Submission: January 2023

Table of Contents

ABSTRACT……………………………………………………………………………………..5

CHAPTER 1…………………………………………………………………………………6-12

INTRODUCTION………………………………………………………………………...6-12

1.1 Introduction……………………………………………………………………………7
1.2 Overview of Steganography.. …………..8-9
1.3 Taxnomy/Classification of Steganography .... ………9
1.4 Research Motivation .... …10-11
1.5 Project Objectives 11
1.6 Research Methodology... 12
1.7 Project Descriptions 12

CHAPTER 2 13-21

LITERATURE REVIEW 13-21

2.1 Introduction 14
2.2 Related Work.. 14-19
2.3 Techniques of Image Steganography 20
2.3.1 Spatial Domain Based 20
2.3.2 Frequency Domain Based.. 20-21

CHAPTER 3 22-33

MEHODOLOGY AND MODELING.. 22-33

3.1 Introduction of Proposed Design: 23
3.2 Data Hiding Method.. 23-27
3.2.1 Least Significant Bit 23-24
3.2.2 Discrete Cosine Transform 24-26
3.2.3 Discrete Wavelet Transform... 26-27
3.3 Flow Chart Representation:.. 28-30
3.4 Pre-processing Secret Data: 30-31
3.5 Dataset Description: 32
3.6 Software Tools 32-33
3.6.1 Python... 32
3.6.2 Tkinter 32
3.6.3 Pillow.. 33
3.6.4 OS Module.. 33

CHAPTER 4 34-38

RESULT AND DISCUSSION.. 34-38

4.1 Performance Analysis 35
4.2 Experimental Results.. 35-38

CHAPTER 5 39-41

CONCLUSION AND FUTURE TASKS...39-41

5.1 Conclusion.. 40

5.2 Future Work: 40-41

References...42-43

Figures Index

Figure	Page
Fig 1: Model of Steganography	8
Fig 2: Key Generation	28
Fig 3: Flow Chart of Encryption Process	29
Fig 4: Flow Chart of Decryption Process	30
Fig 5: Block Diagram of AES algorithm	31
Fig 6: Original Cover Image	36
Fig 7: MSE Values for three different pictures	37
Fig 8: PSNR for three different images	38

List of Tables

Table	Page
Table 1: Literature Review	18-19
Table 2: Performance of all methods in comparison	36

Abstract

Steganography is described as the art of communicating invisibly. Steganography is concerned with methods of concealing the existence of conveyed data in order to keep it confidential. It keeps the communication private in such a way that no one other than the sender and intended recipient suspects its existence. Secrecy is obtained in picture steganography by embedding data into a cover image and generating a stego-image. There are various steganography techniques, each with its own set of advantages and disadvantages. In this study, we examine the various security and data concealment strategies used to achieve steganography. The most well-known steganographic technique—Least Significant Bit, or LSB—is applied in this project. LSB stands for the final or rightmost bit in a binary number. With this method, some of the cover image's LSBs are exchanged with the fragments of the hidden message's secret data. Three phases make up the suggested algorithm. Initially, the user's input and secret key are used to encrypt the secret message. The Advanced Encryption Standard (AES) algorithm is employed to encrypt the message. Second, the LSB algorithm is used to conceal the encrypted data inside an image that the user provides. Third, the user enters the key and the stego-image (the image containing the hidden message) during the decryption phase. The user then receives the extracted text that has been decrypted by the key. Besides LSB we also use two other different approach DCT (Discrete Cosine Transform) and DWT (Discrete Wavelet Transform).

CHAPTER ONE

INTRODUCTION

1.1 Introduction:

In today’s modern world, communication is a necessary requirement for all developing fields. Everyone is concerned about the security and privacy of their communication data. Although we share and transfer information via the internet and other secure channels on a daily basis, there are limits to how safe these methods can be. To disseminate the information in a hidden two methods could be applied. Steganography and cryptography are these mechanisms. Regarding cryptography, the use of an encryption key known only by the sender and the recipient, the message is changed in an encrypted format. Nobody is able to access the message without the encryption key. On the contrary, the transfer of encrypted communication could quickly raise an attacker's suspicions, making it possible for the encrypted message to be intercepted. Nobody is able to access the message without the encryption key. On the other hand, the transfer of encrypted message could quickly raise an attacker's suspicions, making it possible for it to be intercepted, attacked, or decrypted with force. Steganography approaches have been developed to address the limitations of cryptography systems. Steganography is the practice of communicating in a way that conceals the source of the message exchange of ideas. Steganography, then, conceals the existence of data so that it cannot be discovered. Using the act of concealing informational content within multimedia assets, such as images, music, or videos, is known as a "Embedding." Combining the two strategies can increase the anonymity of data communication.

Steganography is the act of concealing crucial information (the message) from unauthorized users by enclosing it in another carrier's (cover) data. When the secret message is hidden, the cover data undergoes slight alterations that our Human Visual System is unable to recognize. The Human Visual System (HVS) will therefore perceive the stego data as a single piece of data. These days, steganography is utilized for data encryption, e-commerce apps, and watermarking. In order to indicate ownership, watermarking is incorporated into the files or photos. It is useful for safeguarding information on a person's permitted copyright. At the moment, secret data protects application transactions, which are primarily user transactions. A person's identity is combined with their fingerprint photographs in a biometric fingerprint by employing steganography, which enables applications to verify transactions.

1.2 Overview of Steganography:

Steganography, which can be defined as the art and science of hiding information within other data that appears to be secure, becomes an effectual tool in this situation. Greek expression "stegos" (meaning "cover") and "grafia" (meaning "writing") are the source of the word "steganography." It's defined as "writing that is covered." Only images are used to conceal information in image steganography. The bounty of easily approachable instruments that can be used to seize privacy. Threats from malevolent actors are now possible due to data security and integrity issues during transmission, listening in and engaging in other inflammatory behaviors. The most common remedy is data encryption, which involves employing an encryption key to transform the data into a cipher text area. Upon receipt, a decryption key is used to render the encrypted message back to plain message. That is not enough, though, as the presence of human eyeballs causes turbulence and increased solace and consolation. In this regard, Steganography, a recently recognized scientific topic has been accepted as a means of hiding data that is imperceptible to the human eye. Steganography operates on the premise of concealing the continuation of information, as contrast to cryptography, which focuses on providing information meaningless. Steganographic mechanisms have become increasingly promising in the digital age and photographs are a frequent choice for carriers because of their widespread use and ability to cover large amounts of data.

Basic Model of Steganography:

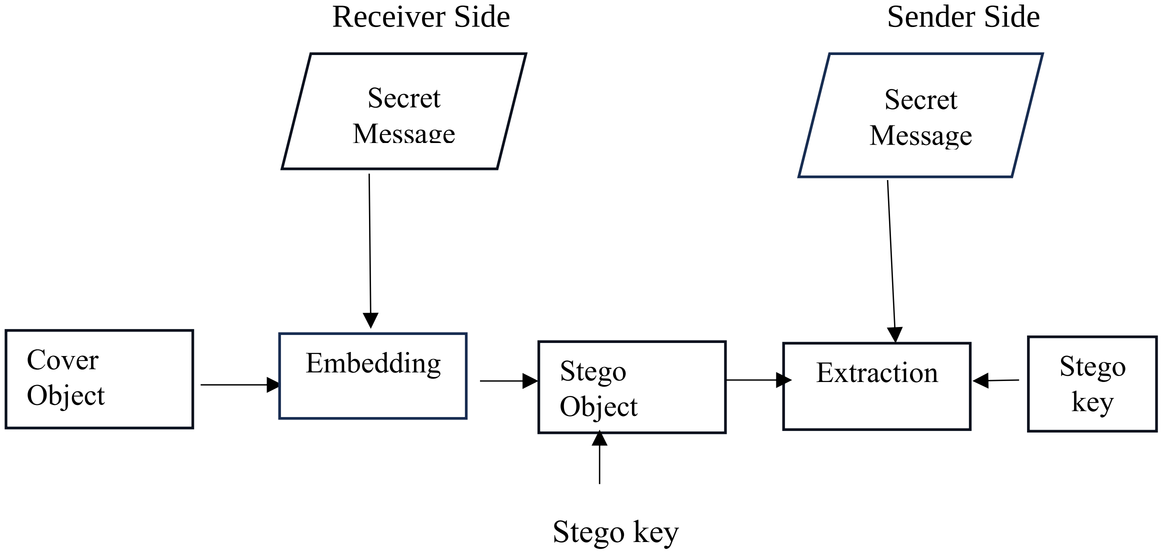


Fig 1: Model of Steganography

It is composed of the following:

1. Cover Object: This is the input image, video, audio, or text file where secret text needs to be hidden.
2. Stego-Object: The cover object turns into the stego-object once secret data has been hidden within the cover medium.
3. Embedding: The creation of a stego-object from a cover object is known as embedding. Alternatively, we could characterize it as the act of hiding a secret message within a digital platform.
4. Extraction: This is embedding done the other way around. The conceded message is retrieved from the stego-object in order to be read throughout this step.
5. Message: For safe transmission, the secret message must be integrated in the cover item.

Image steganography is paramount because it can sneakily insert secret messages into pictures so that uninvited onlookers won't see these information that needs to be hidden. Applications for this secretive communication technique can be found in digital forensics, copyright protection and secure data transfer, among other fields. The need to create strong steganographic methods to protect private data from unwanted access grows as our reliance on digital communication get larger.

1.3 Taxonomy/Classification of Steganography:

Main file format categories like text, images, audio/video, and protocol can all be used with steganography.

- Based on the carrier: audio, video, text, or image.
- Based on message format: text, image, audio, or video.
- Based on domain: spatial domain, frequency domain.
- Based on methods applied: spread spectrum method, statistical method, distortion method, visual cryptography, cover generation method, spatial domain methods (LSB, pseudorandom LSB encoding), frequency domain methods (DCT, DFT, DWT).

1.4 Research Motivation:

Productive and secure means of trading information are essential as digital communication becomes more mainstream. The crucial need to investigate and progress the field of image steganography as a means to improve the certainty of digital communication is the driving force behind this research. We conducted this study in response to the demand for a comprehensive, practical, accurate, and reliable communication technique.

A few terms that aid in our assessment of this section are:

1.Assortment of application:

Image steganography is used in a broad extent of fields, such as digital forensics, military communication and private data interchange. The objective of the research is to help in the creation of adaptable steganographic techniques that can matches the unique requirements of various applications. Into and out of an awareness and reciprocation to the specific difficulties presented by each domain, the project focuses to offer workable solutions for defending various kinds of information and data.

2. Professional developments:

The new paths for innovation in image steganography are build possible by the quick advancements in computational power, machine learning, and digital image processing. This project drives to push the envelope with respect to privacy and effective data hiding within digital images by making use of these automations.

3.Benefaction to Knowledge:

We hope to provide insightful particulars to the academic section and the information security community at large by this research. The project's outputs will come up with the body of knowledge already at hand in the image steganography and offer researchers and practitioners upgrade methods and tools for the safe and secure transmission.

4.Step-analysis-resistant digital forensics:

Contrarily, scientists might be inspired to update the region of digital forensics by generating steganography methods. This requires investigation and developing methods for uncovering hidden data from pictures. Steganographers and those working on steganalysis finish up playing a game of cat and mouse.

Steganography is now completely owned by computers files with digital data as the carrier and networks are monitored as high-speed dispatch routes. The segment illustrating the morphology of steganographic approaches for picture files, as well as a summary of the most relevant steganographic techniques for digital photos.

1.5 Project Objectives:

The goal of this project is to conceal data within an image file. The major objective is to create an algorithm with a high embedding payload at a lower cost that is also more secure and efficient. To achieve the goal, it is crucial to choose the right algorithm to ensure data security, identify specific locations on the sender side where secret data should be embedded, and successfully retrieve the precise secret data from the receiver side. The suggested work accepts.jpg and.png format images as cover objects. Different secret messages are thought to be hidden in different parts of the image. As a result, picture sizes ought to be comparable or sufficient to cover up all user data. Steganography's objective is to conceal communication. As a result, one key requirement of this steganography system is that the hider message transmitted by stego-media be inaudible to humans. The other purpose of steganography is to keep the existence of a hidden message from raising suspicions. This method of information concealment has recently gained popularity in a variety of application areas. This project has following objectives:

- To product security tool based on steganography techniques.
- To explore techniques of hiding data using encryption module of this project
- To extract techniques of getting secret data using decryption module.

When encryption is not authorized, steganography is utilized. Steganography, on the other hand, is widely used to complement encryption. Even if the encrypted file is deciphered, the concealed message is not visible because it is hidden via steganography.

1.6 Research Methodology:

To sum up, we take the succeeding action described below:

- Explain the overview of steganography techniques in formal terms.
- We next collect database from online as well as manually.
- We suggested using a model we had created to carry out the entire procedure.
- After that, first we encrypt the text based upon the user input using AES (Advance Encryption Standard) algorithm.
- After encryption the encrypted message is hidden inside the cover image using three different method such as LSB, DCT, DWT separately.
- Third, the user enters the key and the stego-image (the image containing the hidden message) during the decryption phase. The user then receives the extracted text that has been decrypted by the key.

1.7 Project Descriptions:

Chapter 1 Explains steganography and outlines the goals and objectives.

Chapter 2 Mentions the problem definition, the classification of image steganography, and the previous studies in several areas of image steganography are also covered in this chapter.

Chapter 3 Offers datasets for our suggested methodology's feature extraction and data processing processes. Depicts the implementation of our proposed model. It thoroughly defines each and every techniques that we employ in our study. It also describes about the software we use.

Chapter 4 Contains evaluations of the different techniques performance. It includes all of the outcomes from the techniques.

Chapter5 Shows both the success of our project and its continued development.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction:

The earlier methods of hidden writing were linguistic or language-based. The more recent methods, like invisible, aim to physically conceal messages. A drawback of linguistic steganography is that its users need to be proficient in language. Everything has been rapidly moving toward digitization in recent years. Additionally, smooth network transmission of digital media is now possible thanks to advancements in internet technology. Consequently, messages can be swiftly transferred over the internet after being covertly carried through digital media utilizing steganography techniques. Although steganography can be performed with a wide variety of carrier file formats, picture and video are the most widely employed due to their large embedding capacity. There are numerous steganography techniques available for concealing sensitive information in pictures or videos.

Every technique has its own set of advantages and disadvantages, with some being more complicated than others.The security of the message concealed inside the picture is not taken into consideration in the design of many of the steganography algorithms now in use. These algorithms are therefore designed to be imperceptible, robust, and lacking in security. Furthermore, the majority of approaches do not intelligently process the cover; instead, they use the entire cover equally for hiding data, without adopting any adaptive strategy to determine which areas are appropriate for embedding data.

Furthermore, the entire cover is involved in the concealment process, which has an impact on both the quality of the recovered data and the final stego-object's appearance. In LSB, image steganography is much faster and simpler to use than other image steganography techniques. There is a very small variation between the input and output images. We can embed even huge messages by embedding the message in the final two LSBs rather than only the first. This process serves as the foundation for numerous additional intricate algorithms. We can embed even huge messages by embedding the message in the final two LSBs rather than only the first. A similar technique also conceals the data inside the image without offering sufficient security. To circumvent this, we first encrypt the data using AES before concealing it inside the image.

2.2 Related Works:

Ali AlAtaby and Fawzi AlNaima depicts in their paper that,the purpose of this work is to present a modified high-capacity image steganography method based on wavelet transform that offers a high degree of overall security, acceptable levels of cover image distortion and imperceptibility. In general, steganography and watermarking are related to information concealing. To streamline analysis and save development time, the DWT employed in this paper is constructed using MATLAB functions. While steganography can be used to any redundancy-containing data object, JPEG photographs are the only ones examined in this work. The concealed message's extraction was not shown and is outside the purview of this work. The computational expense is the proposed method's downside [1].

According to Eugene T. Lin and Edward J. Delp, the pictures are embedded covertly. When examined and analyzed casually, the stegoimage ought to resemble the cover image. Furthermore, the encoder typically uses a stego-key to guarantee that the message can only be extracted from a stego-image by recipients who are aware of the matching decoding key [2].

Morkel, T., Eloff, J. H., & Olivier, M. S. attempting to provide an overview of image steganography, including its applications and methods. It also makes an effort to determine what makes a successful steganographic algorithm, and it briefly considers which steganographic methods work better in certain situations. In order to demonstrate the security potential of steganography for both personal and commercial use, this study aims to provide a state-of-the-art review of the various algorithms utilized for image steganography. The resilience of one technique is lacking while the payload capacity of the other is lacking. For instance, the patchwork technique can conceal relatively little information, but it is quite resistant against most types of attacks [3].

Gayathri, C. G., & Kalpana, V. K. discussed are many image steganography techniques, emphasizing their advantages and disadvantages. It is impossible to foresee the ideal procedure. Recent developments in the spatial domain demonstrate that message concealment can be effectively accomplished with just the LSB itself [4]. Another study focuses on information concealing, security, and protection through the use of LSB steganography, pixel value differencing, inverted pattern approach, and information hiding. They employ native Matlab code and only two cover images, Lena and Baboon 256 x 256.Well, it is reaching its zenith since, by itself, it draws no attention [5].

Based on Nagham Hamid and colleagues the taxonomy of the current steganographic methods for image files has been described because the main focus of this paper is on the usage of an image file as a carrier. These methods' capacity to conceal information in image files, as well as how much information they can conceal and how resilient they are to various image processing attacks, are all examined and addressed. Out of all the current image steganographic approaches, the best suitable steganographic method can only be determined by the desired application [6].

The many spatial domain image steganography methods are divided into several groups in this research. There is an increased emphasis on the LSB, RGB, and PVD approaches. Up to four least significant bits can be substituted using LSB methods. Direct LSB replacement can be used to embed the color images. However, by handling them differently, the quality characteristics can be enhanced. While PVD techniques offer great security, LSB techniques offer tremendous capacity. good capacity and good security can be achieved by combining the LSB and PVD methods [7].

Ali, U. M. E., Ali, E., Sohrawordi, M., & Sultan, M. N suggested image steganography technique is presented, which embeds the message in the cover image to protect it from prying eyes by using a pseudorandom number generator to select random pixels and bits. Comparing the experimental findings with the outcomes of the other LSB approaches, it was found that the suggested method offered moderate embedding capacity and medium security. The suggested technique concealed a byte in a pixel of a 24-bit color image using a 3-3-2 method. The technique uses the Pseudo Random Number Generator (PRNG) throughout the embedding

process twice [8]. One of the most basic steganography methods involves altering the container data medium's least significant bits (LSB) plane, which is typically a cover image, in order to immediately conceal the secret message into the spatial domain. The advantages of spatial domain data hiding strategies include high comprehension clarity, efficiency, and the ability to conceal data with the least amount of work [9].

Eight bits of message can be embedded into a single pixel using the authors' in [10] hash-based 2-3-3 approach, which improves and increases the message's capacity to be hidden (only one character for each pixel). As the name implies, this method substitutes any two bits from the least significant nibble (LSN) of the pixel's red value for the first two bits of the message. The last three bits of the message replace the last three bits of the LSN of the corresponding pixel's Blue value, while the second three bits replace the third bit of the LSN of the Green value. In this instance, a hash function is used to help with the random bit selection. This strategy works well in terms of increasing message capacity, but it did not offer a clear answer to the hash function collision problem.

Another study describes the application of an algorithm that combines the LSB steganographic approach—which is statistically improved by image processing—with the AES-CBC cryptographic technology. The algorithm looks for low-contrast regions where the encrypted data would be placed. This hybrid approach was created to transmit a plaintext file concealed within a BMP image, making any alterations to the image imperceptible to the naked eye and impervious to any steganographic

examination. Furthermore, the hybrid algorithm's execution times were assessed for various plaintext and digital image file sizes [11].

This paper discusses several aspects of steganography and cryptography, discussing advancements made through study and observation. Data concealment strategies take great interest in the subject of steganography. An overview of the many steganography techniques that meet the key requirements of steganography design is given in this study.It has been demonstrated that the Haar wavelet transform algorithm has a high-capacity image steganography that can conceal a variety of data of varying sizes. These all have clandestine images that are hidden within stego-images. The cover picture and the stego-image are always equal. In this study, authors explored some of the key ideas, performance metrics, and important variables that affect image steganography. Some of the crucial components of the steganography system, such the choice of the cover picture and image quality measures, have received comparatively less attention due to the earlier pre-send survey articles [12].

The writers of this work suggest improving the application's portability and simplicity of use, thus they created the application for the Android operating system. Several approaches to encrypt and conceal hidden communications in various cover files have already been put forth by Nath et al. An method was used in this work to encrypt the confidential message.The message was then encoded within the LSBs of the cover file's bytes, drawing inspiration from the Vigenère cipher technique. The authors used the LSBs of eight bytes of the cover file without materially altering the file's properties, so that one byte of a secret message can be hidden. The suggested bit exchange is reversible, meaning that the encryption and decryption processes are carried out in reverse. When the authors used the current steganography technique on image files, they obtained a decent result [13].

Table 1: Literature Review

Author Name & Year	**Dataset**	**Algorithm**	**Findings**
Divyansh Sing,2020	Digital image datasets such as training machine learning models, testing algorithms etc.	LSB, Transform domain technique, distortion technique etc.	The paper highlights the evaluation and results of digital image steganography techniques by assessing these algorithms such as LSB, DFT, DT to carry out the results.
Savitha Bhallamudi,2015	StegoDB, Domain specific images, IEEE dataPort.	LSB, parity LSB SteganographyModulation base embedding,DCT domain embedding.	It results in data concealment because it makes use of the basic property that each image can be divided into discrete bit-planes, each of which contains varying degrees of information.
Sharonyah B	BossBase, BOWS2	DCT,Vector Quantization,LSB Insertion	By using the concept of LSB Insertion and DCT algorithm, this paper provides the overview of image steganography process.
Jiaxin Wang et all,2019	BossBase, BOWS2	LSB, PVD, EBE, RPE, DCT, DWT	It shows the impact of technique hybridizing that is brought about by the random attribute and key size boost.

Dr. Asoke Nath et all ,2017	BossBase1.01, Cover10K, Stego100 etc	LSB, DCT, Patch embedding	Image steganography with encrypted messages can be a powerful tool for secure communication as well as it adds an extra layer of security to the hidden message.
S. M. Masud Karim et all,2011	BossBase, HIDE v2, ABCD Dataset	LSB modification, X-OR Based embedding, psedorandom sequences	This paper evaluates the method using a secret key by making it significantly harder for third parties to find out the hidden data.
T. Morkel et all,2005	BOSS Base, BOWS2 & S-UNIWARD	LSB, F5, Spread spectrum DCT & DWT	In this paper researchers typically assess these algorithms based on metrics like Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER). These metrics help quantify the quality of stego images and the extent to which hidden data remains undetectable.
R.Amirtharajan et all,2010	BOSS Base, BOWS2, ImageNet,Custom Datasets,Medical Image Datasets,Remote sensing datasets	LSB Substitution,Optimum Pixel Adjustment Procedure.Inverted Pattern Approach And IP Method Using Relative Entropy.	This paper emphasizes the trade-offs between different steganographic techniques and the importance of choosing the appropriate methods.

2.3 Techniques of Image Steganography:

2.3.1 Spatial Domain Based

These methods encode the message bits directly using the pixel grey levels and their color values. From an embedding and extraction complexity perspective, these methods are among the simplest. The quantity of additive noise that infiltrates the image and immediately impacts the Peak Signal to Noise Ratio and the image's statistical characteristics is the main flaw in these methods. Furthermore, TIFF files and other lossless image compression strategies are the primary applications for these embedding algorithms. Some of the message bits are lost during the compression stage of lossy compression techniques like JPEG.

The Least Significant Bit (LSB) replacement technique, which expresses the message bit using the least significant bit in the binary representation of the pixel grey levels, is the most commonly used algorithm in this family of approaches. The average noise added to the image's pixels while employing this sort of embedding is 0.5p, where p is the embedding rate given in bits per pixel. This form of embedding also causes asymmetry and grouping in the pixel gray values (0,1);(2,3);... (254,255). To overcome this undesirable asymmetry, the least significant bit is altered 12 times at random, which means that if the message bit and the pixel bit do not match, the pixel bit is either increased or decreased by one. This method is usually known as LSB Matching. It should be noted that even with this sort of embedding, an average of 0:5p noise is introduced. To further reduce noise, it has been suggested that the data bits be embedded using a binary function consisting of two cover pixels. For the embedding, a pair of pixels is employed as a unit; the first pixel's LSB holds one bit of information, while the second bit is carried by a function of the two pixels' values. This form of embedding has been shown to reduce the embedding noise generated to the cover signal.

2.3.2 Frequency Domain Based

Using these methods, message bits are attempted to be encoded in the image's transform domain coefficients. Robust watermarking commonly uses data embedding in the transform domain. Large capacity embedding for steganography can likewise be achieved with similar methods. Potential transformations including the discrete Fourier transform (DFT), discrete wavelet transform (DWT), and discrete cosine transform (DCT).

The concealed data is better protected against signal processing since it is dispersed throughout the whole image and is located in more durable regions thanks to its embedding in the transform domain. For instance, we can run a block DCT and select one or more components from each block, based on the requirements for robustness and payload, to create a new data group that is then pseudorandomly scrambled and goes through a second-layer transformation. The double transform domain coefficients are then modified using a variety of techniques. The complexity of the extraction and embedding of these 13 approaches is high. These methods work better for the "Watermarking" part of data hiding due to the resilience qualities of transform domain embedding. Numerous steganographic methods within this field have been influenced by their watermarking equivalents.

CHAPTER THREE

METHODOLOGY AND MODELING

3.1 Introduction to proposed Design:

Within the proposed framework:

- An image presents as the cover;
- A secret message in the form of text may be included;
- The format of cover image is either.jpg or.png.

The expressed system's primary steps are outlined into three steps:

- First of all, the key supplied by the user, the secret text message is encrypted by the AES algorithm.
- Next, the encrypted text message is hidden within the image using various types of spatial domain and transform domain techniques. The techniques are LSB, DCT, DWT.
- At last, the user puts the stego-image (the image with the concealed message) and enters the key in the decryption stage. After that the user retrieves the expelled text that has been decrypted by the previous key.
- Techniques as frequency domain DWT and DCT gives excellent visual quality and large embedding payloads. Furthermore, when compared to frequency domain based techniques, spatial domain based techniques offer greater resistance against attacks.

3.2 Data Hiding Methods:

In this paper we used three different hiding methods. The methods along with their working procedure is described below:

3.2.1 Least Significant Bit:

Least significant bit (LSB) is a most used and straightforward method of hiding information in a cover image. The least significant bit (or the eighth bit) of some or all of the bytes within an image is converted to a secret message bit. As every red, green, and blue color components is represented by a byte, a bit of each color can be used when using a 24-bit image. In other words, each pixel will store three bits. An image with 800*600 pixels can thus store a total of 1,440,000 bits or 180,000 bytes of embedded data. For instance, a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

When the number 200, which has the binary representation 11001000, is inserted in the image's least significant bits, the resulting grid is as follows:

(0010110**1** 0001110**1** 1101110**0**)

(1010011**0** 1100010**1** 0000110**0**)

(1101001**0** 1010110**0** 01100011)

In spite of the number was included in the first 8 bytes of the grid, just the three underlined bits required to be modified in according to the embedded message. Using the maximum cover size, only half of the bits in an image will need to be updated to hide a secret message. Because each primary color has 256 potential intensities, adjusting the LSB of a pixel results in modest variations in the strength of the colors. The human eye cannot identify these changes, hence the message is successfully disguised. With a well-chosen image, one can hide the message in the least significant bit as well as the second to least significant bit and yet not notice the difference.

In the above described example, the information is embedded by using consecutive bytes of image data - from the first byte to the end of the message. This strategy is quite obvious. A slightly more secure solution would be for the transmitter and receiver to share a secret key that specifies only which pixels should be modified. If an enemy suspects the employment of LSB steganography, he has no way of knowing which pixels to target without the secret key.

3.2.2 DCT (Discrete Cosine Transform):

DCT is a well-known approach that is used in a variety of applications, including image and video compression. The DCT divides the signal into three frequency bands: low, medium, and high. The discrete Fourier transform (DFT) is closely connected to the DCT. It is a separable linear transformation, which means that the 2D-DCT is identical to a 1D-DCT in one dimension followed by a 1D-DCT in the other.

DCT which is a transform domain technique, is used in this method to indistinct messages in significant regions of the cover image. Pixels are divided into 8*8 blocks in this method. After that, each block is DCT converted to encodes exactly one secret message bit.

Procedure for hiding:

- The embedding procedure begins with the selection of a block bi that will be utilized to code the i'th message bit.
- Assume that Bi = D{bi} is the DCT-transformed picture block.
- Prior to beginning communication, both sender and receiver must agree on the placement of two DCT coefficients that will be utilized in the embedding process. Let's call these two indices (u1, v1) and (u2, v2).
- Let m(i) be the i‘th message bit.
    - If m(i)=0,
        - if Bi (u1, v1) > Bi (u2, v2) then
          swap Bi (u1, v1) and Bi (u2, v2).
- else if m(i)=1,
    - if Bi (u1, v1) < Bi (u2, v2) then
      swap Bi (u1, v1) and Bi (u2, v2).
- In the last step the stego picture is obtained by taking the inverse DCT of the blocks.
- During retrieval, the stego image is split into 8X8 pixel blocks and DCT converted once again.
- For each block, the preset set of two DCT coefficients is compared.
- if Bi (u1, v1) > Bi (u2, v2) then the message bit=1,
- else 0.

Procedure for Retrieval:

- In the stego-image, a block bi has been chosen.
- The DCT is then applied to the block, Bi=D{bi}.
- The two indices (u1,v1) and (u2,v2) chosen by both sender and recipient are then compared.
- If Bi (u1, v1) > Bi (u2, v2)

  Then data hidden = ‘1’

- Else if Bi (u1, v1) > Bi (u2, v2)

  Then data hidden = ‘0’

- This procedure is repeated for all the blocks in the image.

This strategy is more resistant to attacks such as compression, cropping, and so on. Despite the modest embedding capacity, the image quality is good.

3.2.3 DWT (Discrete Wavelet Transform):

The Discrete Wavelet Transform aids in the detection of sections of a cover image where secret data could be effectively hidden. The DWT separates data into high and low frequency components. The high frequency segment of the signal carries information about the edge components, but the low frequency section contains the majority of the image's signal information, which is further separated into higher and lower frequency sections. In two-dimensional applications, the initial DWT is performed vertically, followed by horizontally. The Wavelets transform (WT) converts data from the spatial to the frequency domain. Because it clearly separates high-frequency and low-frequency information on a pixel-by-pixel basis, the wavelet transform is used in the picture steganographic paradigm. Because of the higher level of resolution afforded by the WT, the discrete wavelet transform (DWT) approach is recommended over the discrete cosine transform (DCT, DWT) decomposes the image into four sub-bands: LL, LH, HL, and HH. The LL section contains the image's most relevant details. Embedding in an LL portion renders stego-image immune to different attacks, however it can cause distortions.

Procedure of embedding:

Step1. Divide the cover image into 4×4 blocks.

Step2. Find the frequency domain representation of blocks by 2D Haar Discrete Wavelet Transform and get four sub bands LL1, HL1, LH1, and HH1.

Step3. Generate 16 genes containing the pixels numbers of each 4×4 blocks as the mapping function.

Step4. Embed the message bits in k-LSBs DWT coefficients each pixel according to mapping function. For selecting value of k, images are evaluated from k=3 to 6. K equal to 1 or 2, provide low hiding capacity with high visual quality of the stego- image and k equal to 7 or 8, provide low visual quality versus high hiding capacity.

Step5. Fitness evaluation is performed to select the best mapping function.

Step6. Apply Optimal Pixel Adjustment Process on the image.

Step7. Calculate inverse 2D-HDWT on each 4×4 block.

Procedure of extraction:

Step1. Divide the cover image into 4×4 blocks.

Step2. Extract the transform domain coefficient by 2D HDWT of each 4×4 block.

Step3. Employ the obtained function in the embedding phase and find the pixel sequences for extracting.
Step4. Extract k-LSBs in each pixel.

3.3 Flow Chart Representation:

- **Key Generation:**

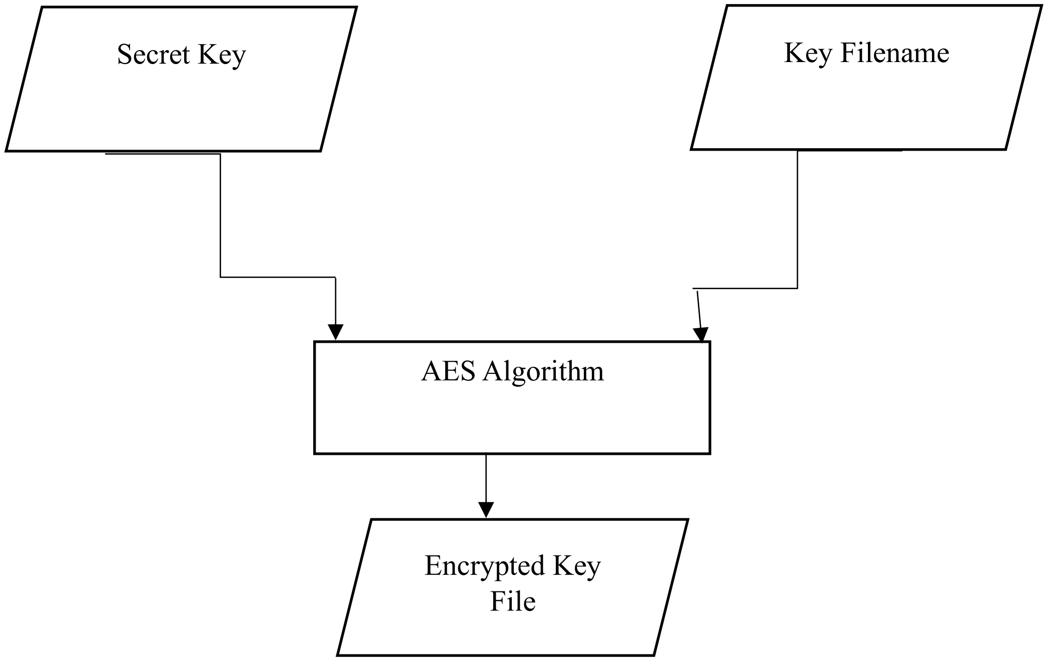


Fig 2: Key Generation

- **Encryption:**

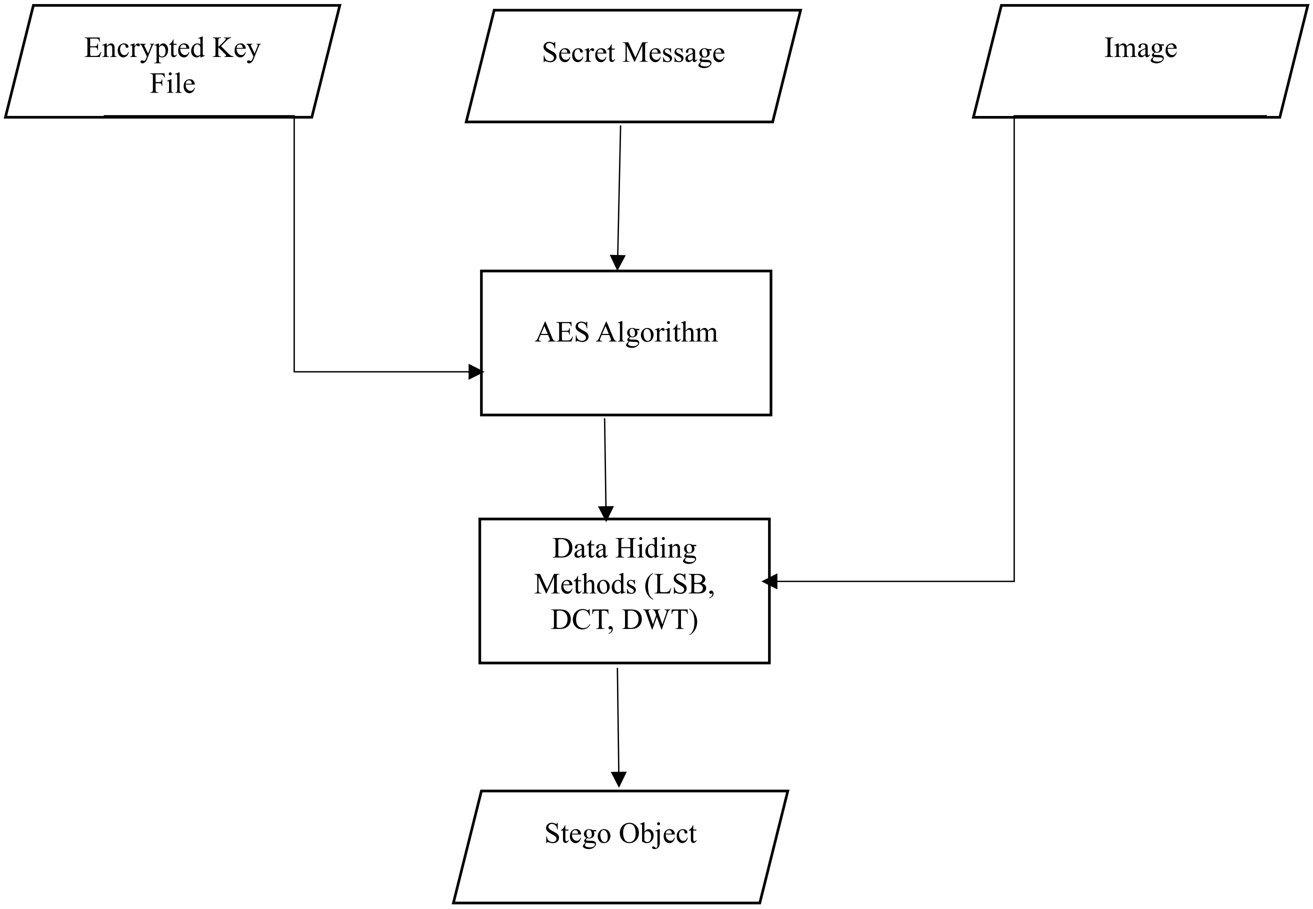


Fig 3: Flow Chart of Encryption Process

- **Decryption:**

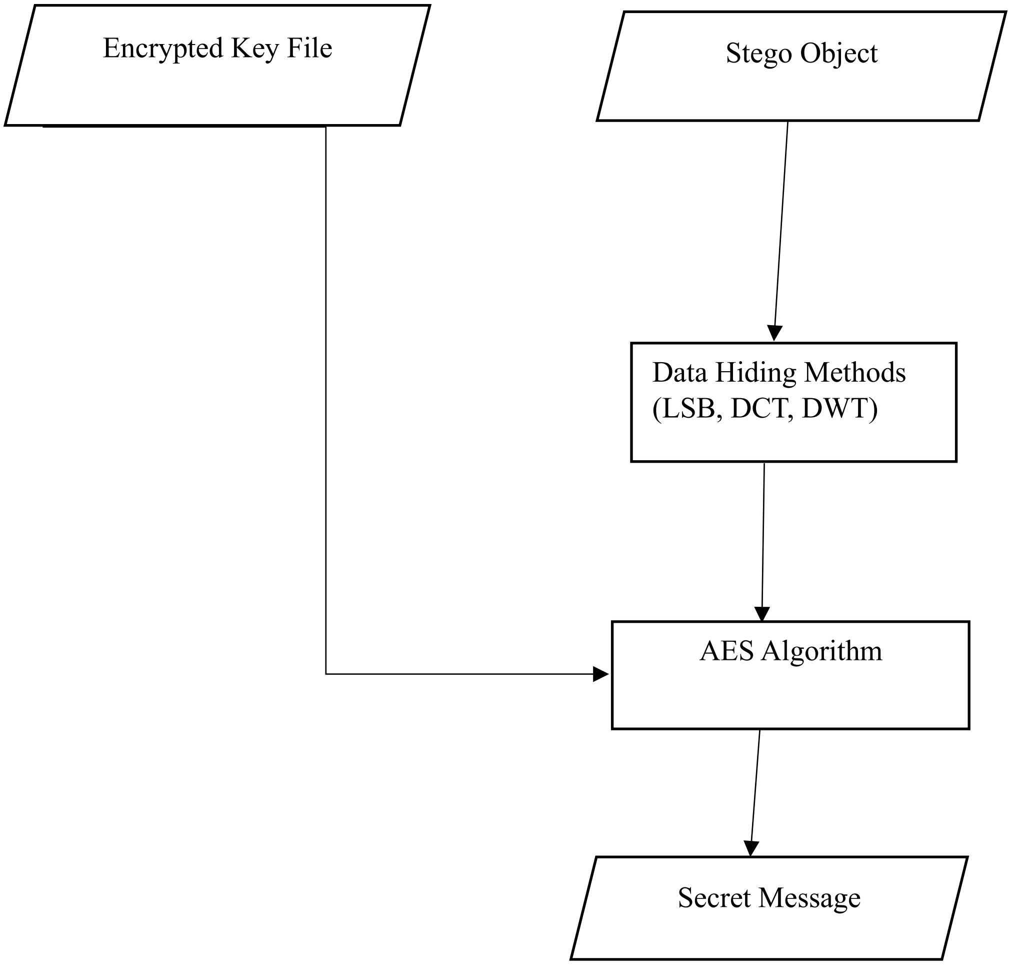


Fig 4: Flow chart of Decryption Process

3.4 Pre-processing Secret Data:

The suggested work uses text as the secret data, which is pre-processed before the embedding phase. During pre-processing, secret data is turned into encrypted text that cannot be read.

Human readable by employing the AES algorithm, the operation of which is described below.

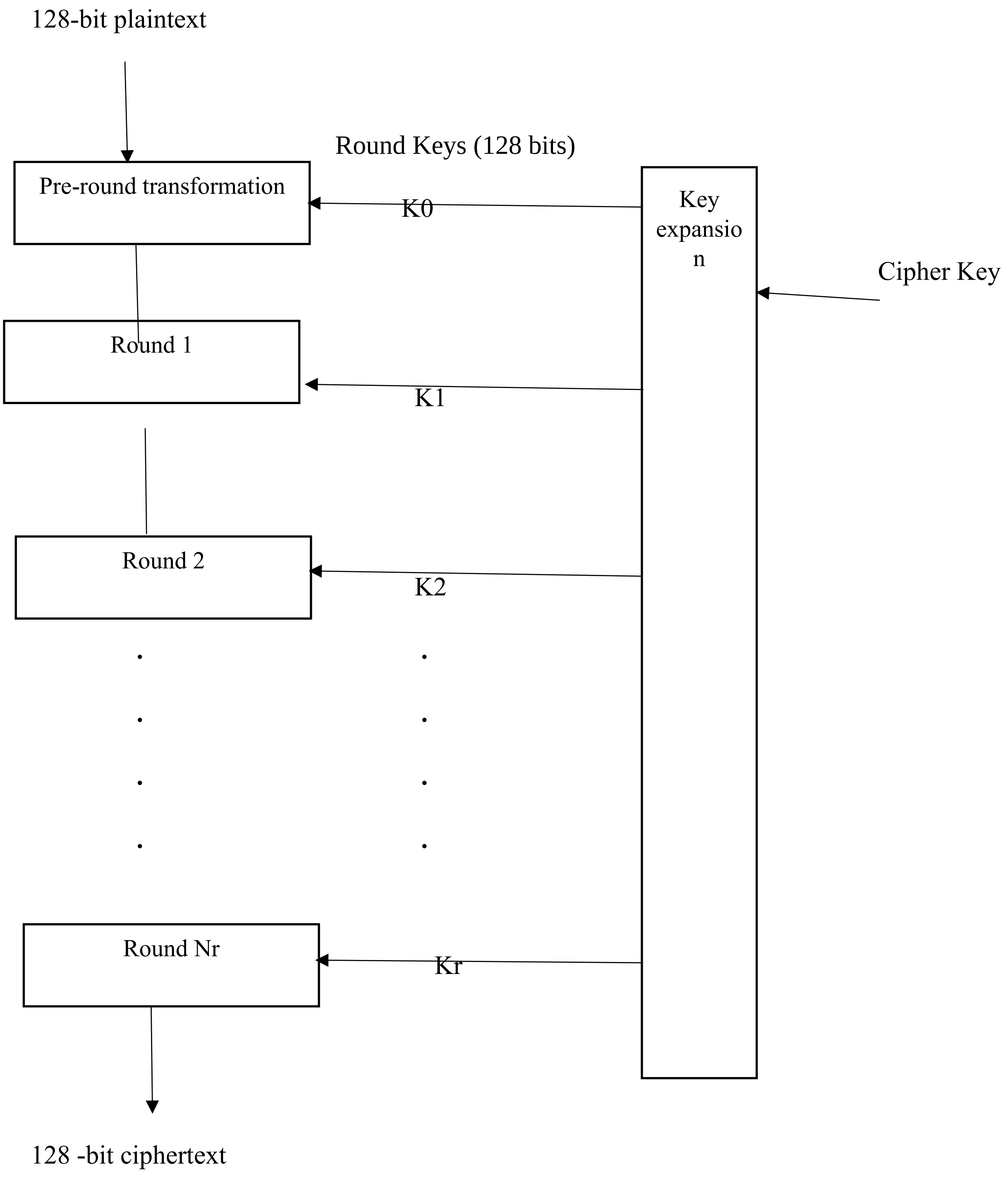


Fig 5: Block Diagram of AES algorithm

3.5 Dataset Description:

We are releasing a massive newly collected dataset -DIV2K- of RGB photos with a wide range of information.

The DIV2K dataset is broken into the following sections:

- Train data: we obtain corresponding low resolution photos from 800 high definition high resolution photographs and give both high and low resolution images for 2, 3, and 4 downscaling factors.
- Validation data: 100 high definition high resolution images are used to generate low resolution corresponding images; the low res images are provided at the start of the challenge and are intended for participants to receive online feedback from the validation server; the high resolution images will be released when the challenge's final phase begins. After the challenge has concluded and the winners have been determined, the winners will be announced.
- Test data: 100 different photographs are used to make low resolution related images; when the final evaluation phase begins, the participants will receive the low resolution images, and the results will be announced once the challenge is completed and the winners are determined.

3.6 Software Tools:

3.6.1 Python: We used python language in this project as programming language. Version of this python in 3.11.2. Actually Python is a programming language that sets itself apart from others by offering the adaptability, clarity, and dependable tools necessary to develop contemporary software. Python is best suited for machine learning since it is reliable and based on simplicity.

3.6.2 Tkinter: Tkinter is Python's de-facto standard GUI (Graphical User Interface) package. It is a thin object-oriented layer on top of Tcl/Tk. Tkinter is not the only GuiProgramming toolkit for Python. It is however the most commonly used one**.**

3.6.3 Pillow: The Python Imaging Library extends your Python interpreter's image processing capabilities. This library supports a wide range of file formats, has an efficient internal representation, and has rather robust image processing features. The core image library was created to provide quick access to data contained in a few fundamental pixel formats. It should be a good starting point for a broad image processing program**.**

3.6.4 OS Module: The OS module in Python provides functions for interacting with the operating system. OS comes under Python's standard utility modules. This module provides a portable way of using operating system dependent functionality. The *os* and *os. path* modules include many functions to interact with the file system.

CHAPTER FOUR

RESULT AND DISCUSSION

4.1 Performance Analysis:

A comparison analysis is performed to demonstrate the efficacy of the recommended methods. The effectiveness of the offered methods has been demonstrated by Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). The most popular metrics used to estimate image quality are the Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE). The mean of the squares of the error between the stego picture and the original image is estimated using MSE.

It is defined as:

$$\text{PSNR} = 10.\log\left(\frac{MAXI^2}{MSE}\right)$$

Where, MAXI represents maximum value of pixel of the image. In the images with pixel having 8 bits per sample, its value is 255. The MSE stands for cumulative squared error between the stego image and the original image.

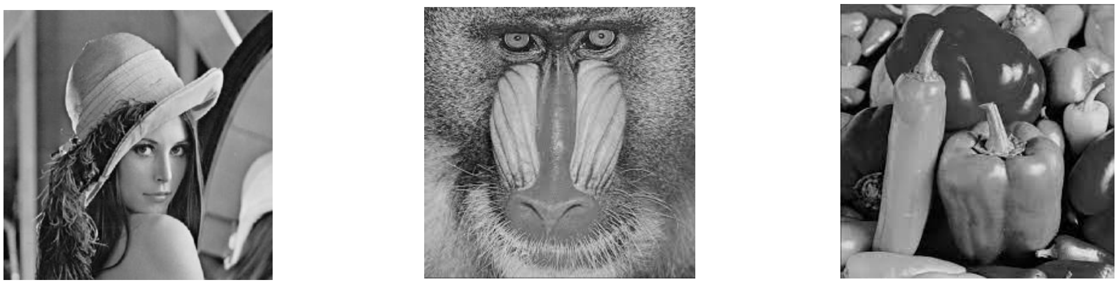
$$\text{MSE} = \frac{I}{MN}\sum_{x=1}^{M}\sum_{y=1(}^{N} S_{xy} - C_{xy\,)}^{\;2}$$

C and S refer to the cover image and stego image respectively. m and n defines as image resolutions.

4.2 Experimental Results:

This section contains experimental results that indicate the effectiveness of our proposed strategy. In this section, the proposed method was tested by examining a message of various lengths using the three most commonly available 24-bit images (Lena, pepper, and baboon) with size 512*512.

The images are:



(a) Lena (b) Baboon (c) Peppers

Fig 6: Original Cover Image

Our proposed methodology has been compared with available methods and the results are tabulated in Table 1 using MATLAB.

Table 2: Performance of all methods in comparison

Method	Cover Image	Size of secret data	MSE	PSNR	Time(s)
LSB	Lena	25KB	0.1503	53.6718	6.78
	Baboon	25.2KB	0.1620	53.6558	6.46
	Peppers	25KB	0.2635	54.6869	6.76
DCT	Lena	25KB	0.0255	51.56	5.89
	Baboon	25.2KB	0.0244	52.0223	5.91
	Peppers	25KB	0.029092	53.45	6.77
DWT	Lena	25KB	0.2835	73.62	6.89
	Baboon	25.2KB	0.29187	63.54	7.45
	Peppers	25KB	0.290838	55.59	6.75

With maximum message capacity, the MSE and PSNR are acceptable given the message's security. The MSE and PSNR for each approach are also compared. LSB-based development approaches usually provide less information than spatial domain algorithms. The LSB approach in the spatial domain is a viable means of concealing information, but it is vulnerable to tiny changes caused by image processing or lossy compression. Although LSB approaches can conceal a huge amount of information, implying a high payload capacity, they typically account for the image's statistical features, resulting in poor resistance against statistical attacks and image manipulation. DCT and DWT are promising strategies that are resistant to attacks, particularly when the hidden information is brief.

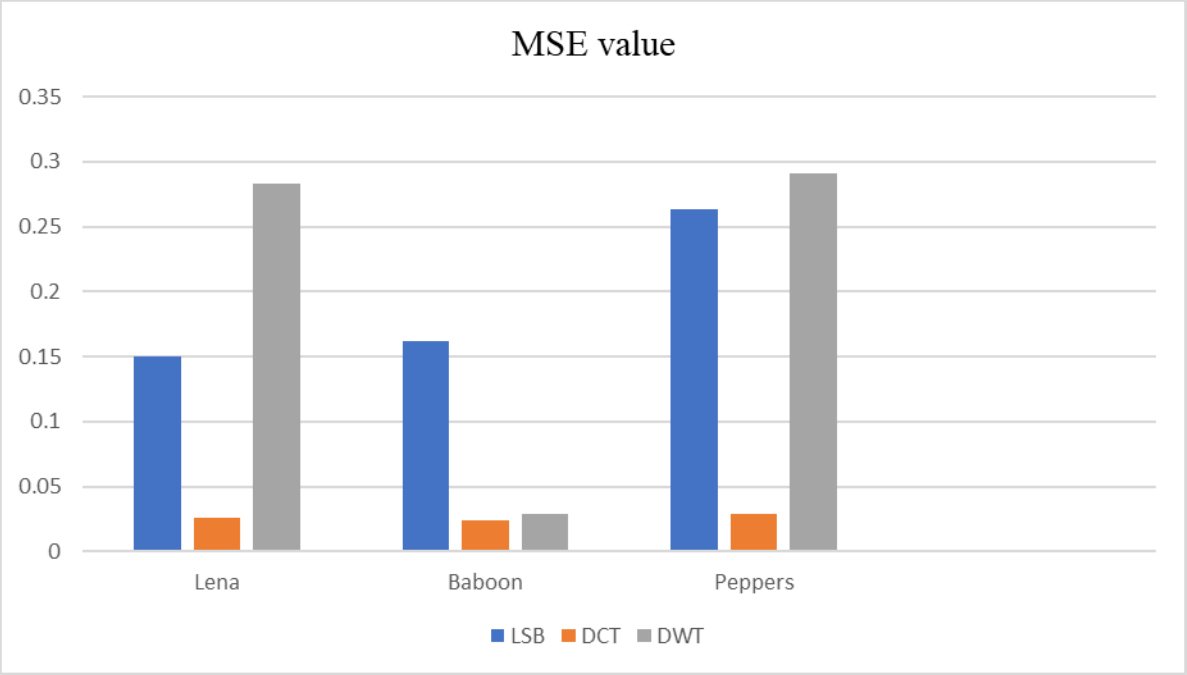


Fig 7: MSE Values for three different pictures

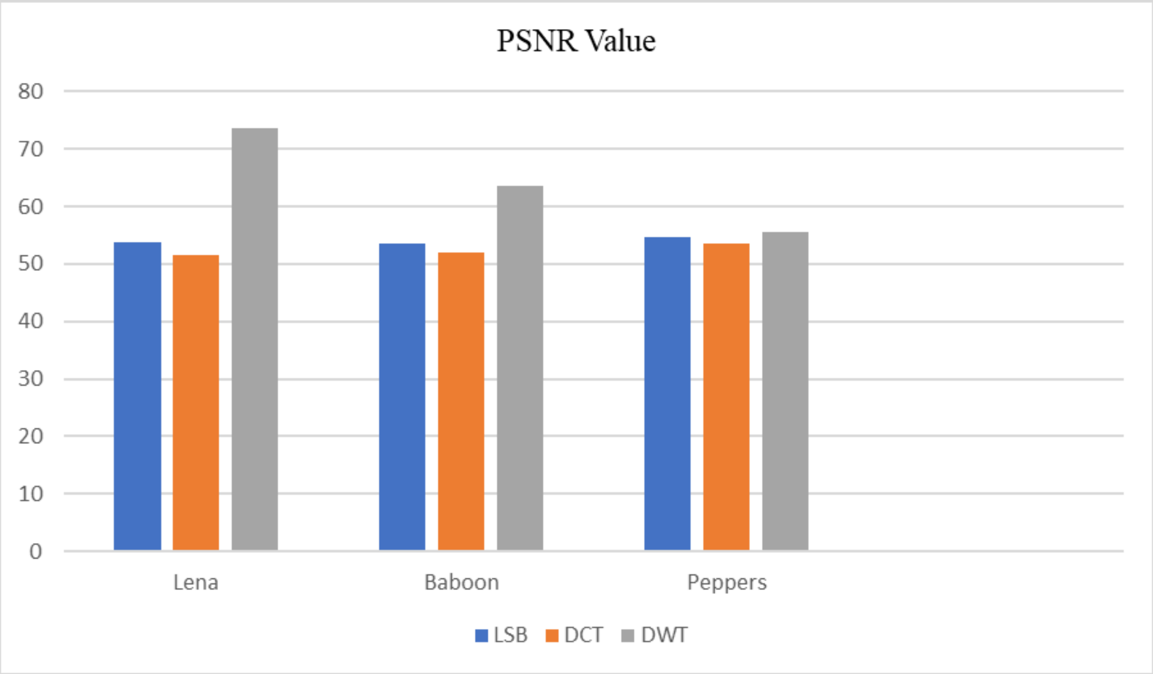


Fig 8: PSNR for three different images

CHAPTER FIVE

CONCLUSION AND FUTURE TASK

5.1 Conclusion:

Steganography is the art and science of composing concealed messages in such a way that no one, other than the sender and intended recipient, suspects the message's existence, a type of security by obscurity. As a result, it is a book about magic. It is at its pinnacle because it does not attract anyone on its own. A comparison examination of numerous methodologies has been effectively implemented in this research, and the findings are presented. This work presents a background discussion and implementation on the key steganography algorithms used in digital imaging. The MSE and PSNR of all the approaches are also compared. The LSB based emerging techniques often carry less information than spatial domain algorithms. The LSB approach in the spatial domain is a feasible means to conceal information, but it is subject to tiny changes caused by image processing or lossy compression. Although LSB approaches can conceal a huge amount of information, indicating a high payload capacity, they frequently compensate for the statistical features of the image, indicating a low robustness against statistical attacks as well as image manipulation.

DCT, DWT are promising techniques that are not vulnerable to attacks, especially when the hidden information is short. This is justified in Image distortion is maintained to a minimal due to the manner they adjust the coefficients in the transform domain. In general, when compared to spatial domain algorithms, such strategies tend to have a lesser payload. The tests on the discrete cosine transform (DCT) coefficients produced some promising and better findings, which shifted the researchers' focus to JPEG images. Working at a level similar to DCT makes steganography far more potent and less vulnerable to statistical attacks. DWT embedding yields constructive outcomes and particularly in terms of compression survivability diverted the researchers' attention away from JPEG images.

5.2 Future work:

Steganography is the transmission of secrets through seemingly benign coverings in order to conceal the existence of a secret. The use and application of digital image steganography and its derivatives is expanding.Citizens are looking to steganography to overcome such policies and pass messages discreetly in regions where cryptography and strong encryption are prohibited. As with the battles between cryptographers and cryptanalysis, security experts and hackers, record companies and pirates, steganography and steganalysis will constantly create new techniques to defeat one other.

The most major use of steganographic techniques in the near future will most likely be in the field of digital watermarking. Content providers are eager to safeguard their copyrighted works from unauthorized dissemination, and digital watermarks enable them to identify the owners of these materials. Steganography may also be restricted by legislation, as governments have argued that criminals utilize these techniques to communicate.

The following are some examples of how steganography can be used:

- Hide data on the network in the event of a breach.
- Private peer-to-peer communication.
- To avoid transmission, covert conversations are posted on the Internet.
- Embedding remedial audio or image data in the event of corrosion caused by a bad connection or transmission.

References

1. Al-Ataby, A., & Al-Naima, F. (2008). A modified high capacity image steganography technique based on wavelet transform. changes, 4, 6.
2. Lin, E. T., & Delp, E. J. (1999, April). A review of data hiding in digital images. In *PICS* (*Vol. 299*, pp. 274-278).
3. Morkel, T., Eloff, J. H., & Olivier, M. S. (2005, June). An overview of image steganography. In *ISSA* (Vol. 1, No. 2, pp. 1-11).
4. Gayathri, C. G., & Kalpana, V. K. (2013). Study on image steganography techniques. Study on Image Steganography Techniques, 1-6.
5. Amirtharajan, R., Akila, R., & Deepikachowdavarapu, P. (2010). A comparative analysis of image steganography. *International journal of computer applications*, *2(3)*, 41-47.
6. Hamid, N., Yahya, A., Ahmad, R. B., & Al-Qershi, O. M. (2012). Image steganography techniques: an overview. *International Journal of Computer Science and Security (IJCSS)*, *6(3)*, 168-187.
7. Swain, G., & Lenka, S. K. (2014). Classification of image steganography techniques in spatial domain: a study. *Journal of Computer Science & Engineering Technology (IJCSET)*, *5(03)*, 219-232.
8. Ali, U. M. E., Ali, E., Sohrawordi, M., & Sultan, M. N. (2021). A LSB based image steganography using random pixel and bit selection for high payload. Int. J. Math. Sci. Comput., 3, 24-31.
9. Karim, S. M., Rahman, M. S., & Hossain, M. I. (2011, December). A new approach for LSB based image steganography using secret key. In 14th international conference on computer and information technology (ICCIT 2011) (pp. 286-291). *IEEE*.
10. Manjula, G. R., & Danti, A. (2015). A novel hash based least significant bit (2-3-3) image steganography in spatial domain. arXiv preprint arXiv:1503.03674.

11. Edwar, J. G., & Holman, M. A. (2022). Enhanced Security: Implementation of Hybrid Image Steganography Technique using Low-Contrast LSB and AES-CBC Cryptography. *International Journal of Advanced Computer Science and Applications, 13(8).*
12. Sidqi, H. M., & Al-Ani, M. (2019). Image steganography: Review study. In Proc. Int. Conf. Image Process., Comput. Vis., Pattern Recognit.(IPCV) (pp. 134-140).
13. Nath, A., Roy, S., Gopalika, C., & Mitra, D. (2017). Image steganography using encrypted message. *International Journal of Advance Research in Computer Science and Management Studies, 5(4).*