SECURE IMAGE STEGANOGRAPHY

IN SPATIAL DOMAIN

By

IHTISHAM UR REHMAN

A thesis submitted to the faculty of Electrical Engineering Department, Military College of Signals, National University of Sciences and Technology, Islamabad, Pakistan, in partial fulfillment of the requirements for the degree of MS in Electrical (Telecommunication) Engineering

DECEMBER 2019

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis written by Mr/MS **Ihtisham Ur Rehman,** Registration No. **00000172271** of **Military College of Signals** has been vetted by undersigned, found complete in all respect as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial, fulfillment for award of MS/MPhil degree. It is further certified that necessary amendments as pointed out by GEC members of the student have been also incorporated in the said thesis.

Signature: _____

Name of Supervisor: **Lt Col Hasnat Khurshid, PhD**

Date: _____

Signature (HoD): _____

Date: _____

Signature (Dean): _____

Date: _____

CERTIFICATE FOR PLAGIARISM

It is certified that MS Thesis titled **"Secure Image Steganography in Spatial Domain"** by Regn No: **00000172271 Ihtisham Ur Rehman, MSEE-22 Course** "has been examined by us. We undertake the follows:

a. Thesis has significant new work/knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.

b. The work presented is original and won work of the author (i.e. there is on plagiarism). No idea, processes, results, or words of others have been presented as Author own work.

c. There is no fabrication of data or results which have been compiled / analyzed.

d. There is no falsification by manipulating research materials, equipment, or process, or changing or omitting data or results such that the research is not accurately represented in the research record.

e. The Thesis has been checked using TURNITIN (copy of originality report attached) and found within limits as per HEC Plagiarism Policy and instructions issued from time to time.

Signature: _____

Name of Supervisor: **Lt Col Hasnat Khurshid, PhD**

Dated: _____

ABSTRACT

Steganography technique is the art of concealing information or data into a digital media that hides the existence of the information in the digital media. Media with and without hidden information are called stego media and cover media, respectively. Digital images have high degree of redundancy in representation thus likeable for hiding data. Image steganography can be mainly classified into spatial domain and transform domain. The very basic technique for image steganography is least significant bit (LSB).

There exist a large number of steganography techniques for hiding the secret information or data into digital images. Every method has respective strong and weak points. This work aims to propose an algorithm that increases the hiding capacity with better visual quality, the proposed technique initially compresses the secret information using the lossless Huffman compression technique; furthermore the similarity of the blocks obtained from the cover image and the secret information are measured so that to minimize the alteration of the bits in cover image.

Results of the proposed technique are compared with that of existing techniques, the values obtained for the parameter, PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), and NCC (Normalized Cross Correlation) are superior to existing techniques.

DEDICATION

This thesis is dedicated to my parents, whose prayers and support makes it possible for me, to do this research work.

ACKNOWLEDGEMENT

Foremost, I would like to express my gratitude to Allah Almighty who gives me the opportunity and the strength for the completion of this research work.

I would like to thank my advisor Lt Col Hasnat Khurshid, PhD for the support of my master's study and research work, for the patience he showed towards me, for the best environment he provided during the research and the writing of the thesis. It wouldn't be possible without his kind help and efforts.

Beside my advisor, I would like to thank the committee members of my research work; Lt Col Muhammad Imran and Asst. Prof Muhammad Imran, PhD and my friend Sajjad haider for their special encouragement, and help throughout the research. I also owe a gratitude to Military College of Signals, NUST, for providing such a great research environment within the institute.

Table of Contents

ABSTRACT v
DEDICATION vi
ACKNOWLEDGEMENT vii
LIST OF FIGURES xi
LIST OF TABLES xii
LIST OF ACRONYMS xiii
Chapter 1 1
INTRODUCTION 1
1.1 Overview 1
1.2 Cryptography 2
1.2.1 Secret Key Cryptography (SKC) 3
1.2.2 Public Key Cryptography (PKC) 3
1.2.3 Hash Functions 3
1.3 Steganography 4
1.3.1 Requirements for a Steganography Technique 6
1.4 Research Motivation 7
1.5 Problem formulation and thesis layout 7
Chapter 2 9
IMAGE STEGANOGRAPHY–AN OVERVIEW 9
2.1 RELATED TERMS 9
2.1.1 Cover Image 9
2.1.2 Stego Image 9
2.1.3 Stego Key 10
2.2 Cover Image Selection 10
2.3 Embedding Domain 10
2.3.1 Frequency Domain 10
2.3.2 Spatial Domain 11
2.4 Existing Techniques 12

2.4.1 DCT Based Steganography 12
2.4.2 JPHide/Jsteg 12
2.4.3 YASS 12
2.4.4 F5 13
2.4.5 Steganography Based On DWT 13
2.4.6 Least significant bit (LSB) 14
2.4.7 Pixel indicator technique 15
2.4.8 Pseudo-Random LSB Encoding Technique 16
2.4.9 Distortion Technique 17
2.4.10 Pixel value differencing (PVD) 18
2.4.11 Pixel Ranking and Particle Swarm Optimization 19
2.4.12 LSB+DWT 19
2.4.13 LSB Based Steganography Using AES Algorithm 20
2.4.14 Enhanced LSB Substitution Technique [17] 21
2.4.15 LSB Based Color Image Steganography [18] 22
2.4.16 Optimized Pixel Value Differencing 22
2.4.17 Hybrid image steganography based on IWT-LSB techniques [22] 23
Chapter 3 24
PROPOSED METHODOLOGY 24
3.1 Compression through Huffman encoding 25
3.2 Cosine Similarity 29
3.3 Embedding process 31
3.4 Extraction Process 32
Chapter 4 34
RESULTS AND DISCUSSION 34
4.1 Parameters 35
4.1.1 Hiding Capacity 35
4.1.2 MSE and PSNR 35
4.1.3 Normalized Cross-Correlation (NCC) 36
4.2 Results 37

4.2.1 Embedding rate versus MSE, PSNR and NCC 37
4.3 Comparison of Proposed Technique with the existing Techniques 41
Conclusion 45
References 46

LIST OF FIGURES

Figure 1.1: Information hiding techniques 1

Figure 1.2: Cryptography..... 2

Figure 1.3: Basic block diagram for steganography in digital media 5

Figure 1.4: Steganography in different digital media 6

Figure 2. 1: Pseudo-Random LSB technique. 17

Figure 2.2: Distortion technique. 18

Figure 2.3: Transmitter end[16] 20

Figure 2.4: Receiver end[16] 21

Figure 3.1: Embedding and Extracting phases of the proposed approach 25

Figure 3.2: Flowchart of Huffman encoding..... 28

Figure 3.3: Huffman binary tree for (image steganography) 29

Figure 3.4: (a) 8×8 cover LSB matrix (b) 8×8 binary matrix of secret information I 30

Figure 3.5: Cover blocks (a) A_1 (b) A_2 (c) A_3 (d) A_4 30

Figure 3.6: Secret information Blocks, (a) B_1 (b) B_2 (c) B_3 (d) B_4..... 31

Figure 4.1: Grayscale cover images of size 512×512. 34

Figure 4.2: Cover and their respective Stego images at different embedding rate. 40

Figure 4.3: Comparison (a) PSNR, (b) MSE, (c) NCC..... 43

LIST OF TABLES

Table 2.1: Indicator values Based action..... 16

Table 2.2: Basis for Selection of number of Bits to replace [17] 21

Table 4.1: PSNR, MSE and NCC values for maximum capacity 1.6 bits per pixel..... 38

Table 4.2: PSNR, MSE and NCC values at embedding rate of 1 bit per pixel..... 38

Table 4.3: PSNR, MSE and NCC values with embedding rate of 0.5 bit per pixel 39

Table 4.4: Values of NCC, MSE and PSNR at the embedding rate of 1 bpp 42

LIST OF ACRONYMS

Bits per pixel	BPP
Least significant bit	LSB
Most significant bit	MSB
Discrete Cosine Transform	DCT
Discrete Wavelet Transform	DWT
Human Visual System	HVS
Fast Fourier Transform	FFT
Mean Square Error	MSE
Peak Signal to Noise Ratio	PSNR
Particle Swarm Optimization	PSO
Pixel value differencing	PVD
Integer Wavelet Transform	IWT
Advanced Encryption Standard	AES

Chapter 1

INTRODUCTION

1.1 Overview

Internet plays a key role for the past few decades in data communication due to its fast and cheap transmission of the data through the web, although internet lacks the security required for the data to be transmitted over internet. The transmitted data through the web can be of any kind of data like casual data and confidential data i.e. financial data, medical diagnostics and military data etc. To address the information security issue there should be way or a mechanism for safeguarding the confidential data to be sent over the internet. Cryptography and steganography both are used for overcoming the confidentiality and security problem of the data transmission through the internet.

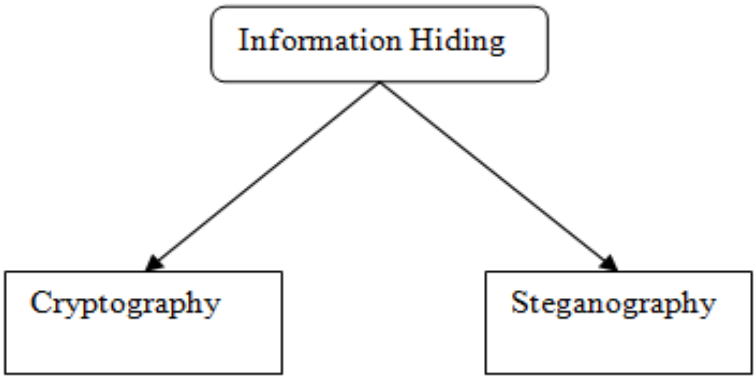


Figure 1.1: Information hiding techniques

1.2 Cryptography

Cryptography techniques are used for protecting the confidentiality of the information and communication, cryptography is used by information security on various levels. Codes are generated for the secrecy of the information called encryption key, using secret encryption key, and the information data is converted into another form which is unreadable and inaccessible to unauthorized users, the secret encryption key is required for the decryption of the encrypted information data. A block diagram of basic cryptography is presented in the figure 1.2.

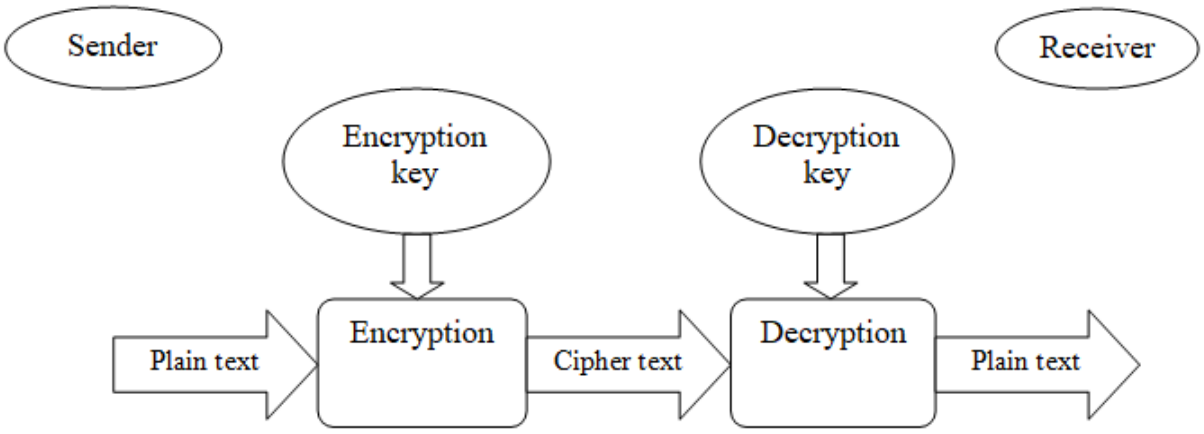


Figure 1.2: Cryptography

Cryptography aims for four objectives discussed below.

Confidentiality: The encrypted secret information cannot be read or understood by an unintended user; hence the confidentiality of the secret information remains.

Integrity: The secret information can't be altered in a storage space or the transmission path between the sender and an authorized receiver without the altered information being detected.

Non-repudiation: The sender of the secret information at a later stage can't deny his/her intentions while transmitting the secret information.

Authentication: Sender and the receiver can authenticate their identity for a secure and confidential communication.

Few cryptography algorithms are discussed below.

1.2.1 Secret Key Cryptography (SKC)

Secret key cryptography uses the same encryption key for decryption. Such type of encryption can be termed as symmetric key encryption.

1.2.2 Public Key Cryptography (PKC)

Two keys are used in Public key cryptography, also known by asymmetric encryption. One key termed as public key and is in everyone's access. Other one is termed as private key, who can be only accessed by the owner; information at the transmitter side is encrypted by the public key of the receiver. At the receiver end information is decrypted using the private key of the receiver.

1.2.3 Hash Functions

Unlike, Secret key cryptography and public key cryptography, hash functions uses no keys and is termed as one way encryption, Hash functions are used for the originality of the file.

Cryptography changes the format of the original information and cannot be understandable for unintended users which draw attention of the attackers. But nowadays the increase in demand for security leads the researcher to the use of steganography for a secure communication between intended users.

1.3 Steganography

Steganography is the combination of the Greek words “stego” means “covered” and “graphia” means “writing” which defines steganography as covered writing. Since decades, steganographic methodologies has been used but its introduction in to digital information security is rather novel. There is close relation between steganography and cryptography, both having a common goal of information security, cryptography changes the format of the information providing security to the information while steganography hides even the existence of the information. Unlike cryptography, steganography safeguards secret data or information using a medium to hide the existence of secret data or information which can only be accessed by the authorized receiver [1]. Another candidate for information or data hiding is water-marking, steganography and water-marking both are the techniques for embedding the data but there are various differences between them. Comparison is presented in [2]. Figure 1.3 shows block diagram for steganography in digital media.

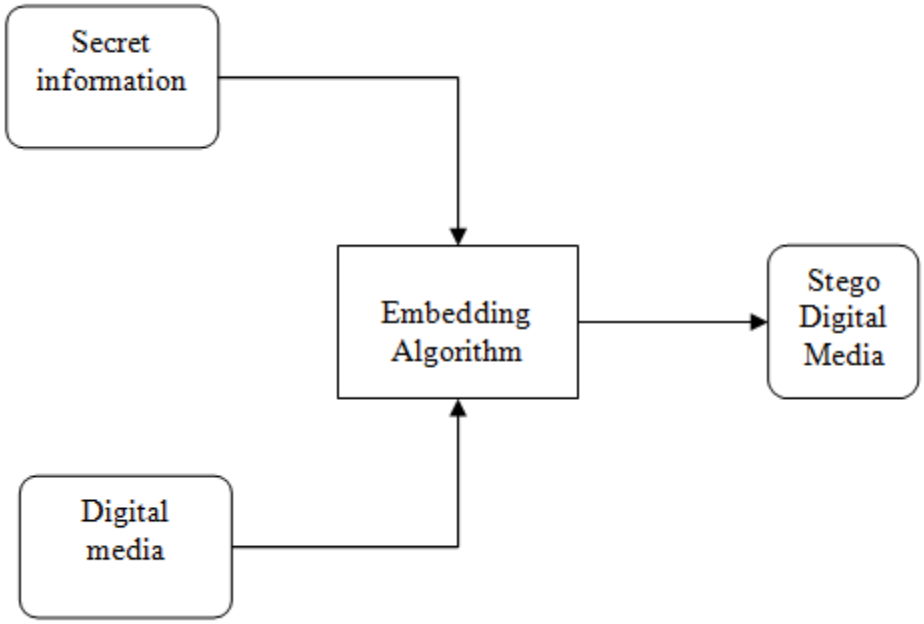


Figure 1.3: Basic block diagram for steganography in digital media

Several digital multimedia like audio, video, text, images show in figure 1.4 can be of good use for steganography. Text based steganography involves the modification of the text layout, usage of the i^{th} character from the text or the alteration of few rules like spaces etc. another technique uses codes have combinations of page number, line and characters. However, these techniques lack security. Audio based steganography is done using that part of the frequency which is inaudible to human ears. Steganography in video files can be done as video is a combination of sound and images, a small amount of modification may not be visible to human eye as the information flows continuously. High payload capacity can be achieved using video based steganography. Another popular file format for steganography are images, images have higher redundancy in their representation, hence the most suitable candidate for steganography. Steganogrphy based on images gives better imperceptibility and a high payload capacity.

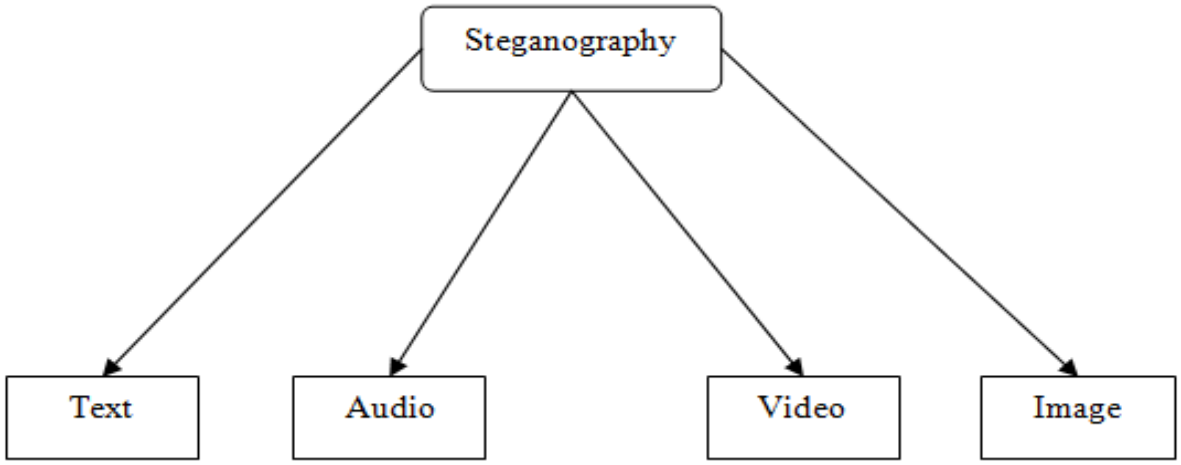


Figure 1.4: Steganography in different digital media

1.3.1 Requirements for a Steganography Technique

Requirements for steganography techniques are capacity, security, undetectably and robustness. However, it is difficult to fulfill all the requirements; there is always a tradeoff between them.

- **Capacity:** The amount of secret information data to be embedded, relative to the size of the cover medium with tolerable degradation. And the secret information can extract later correctly without any visual change the cover medium. Embedding rate is either the size of the data to be embedded or in bits/pixel etc.
- **Security:** Steganography technique is said to be more secure if an attacker cannot remove the concealed information after detection. Without knowing the technique and the secret key, the attacker will not be able to retrieve the hidden secret information.

- **Undetectibility:** Undetectibility mean embedding of the secret information must not create any visual artifacts, there must be no visual difference between original cover medium and stego medium .
- **Robustness:** A stego cover object is robust against signal processing if the cover object undergoes a transformation like cropping, scaling, filtering, and rotation etc.

Usually high payload embedded into the cover increase the vulnerability of detection of the stego object, the key requirement of a steganography technique is undetectability, which means the cover object and the stego object should be statistically and visually similar while the embedding rate to be kept as high as possible.

1.4 Research Motivation

The use of internet is increasing exponentially from the past decade; a lot of information is being shared everyday over the internet, information can be of any kind like casual information or confidential information. This confidential information to be shared on the internet is vulnerable to stealing and eavesdropping, which becomes an important issue for the confidentiality of the information. To safeguard the confidentiality of the confidential information, steganography offers cheapest and a reliable way.

1.5 Problem formulation and thesis layout

Internet is the most preferred and reliable source for the transmission of data and communication as the internet provides the cheapest and fastest way of data transmission through the World Wide Web. The data to be transmitted over the World Wide Web can be of any kind i.e.-e casual data and confidential data which include

financial, medical diagnostic, military data etc. However there may be a threat to the sensitive and confidential data from eavesdroppers, hence the confidentiality of the confidential data does not remain.

Addressing these threats, cryptography and steganography has been introduced in order to keep integrity of the confidential data. Cryptography changes the shape of the secret information into indistinct form called ciphered secret information. Unlike cryptography, steganography uses cover medium to hide the existence of secret information [3]. Images are considered to be the best candidates as cover medium for safeguarding the secret information in steganography due to the higher degree of redundancy in their representation and the broad usage of the images throughout the internet, however there is a tradeoff between the visual quality and the payload capacity.

The basic idea of this thesis is that the LSB plane of the cover image is utilized for the replacement of the secret information in such a way that the probability of altering the LSBs is decreased. The lesser the difference of bits between the cover image and the stego image the higher the PSNR. Payload capacity can be increased by the addition of Huffman compression.

Chapter 2

IMAGE STEGANOGRAPHY– AN OVERVIEW

Digital images are the most appealing and suitable candidates for steganography, as digital images in their representation have higher degree of redundancy, redundancy refers to the redundant bits with in an image that can be altered without any degradation to the digital image and a vast use of digital images in our daily life throughout the internet.

2.1 RELATED TERMS

Image steganography's basic related terminologies are as follow.

2.1.1 Cover Image

Image used for embedding or hiding the secret information or data is known as cover image, any image can be selected as cover image by a sender for embedding or hiding the secret information or data within the image.

2.1.2 Stego Image

Stego image is obtained after embedding the secret information into the cover image, the visual difference between the cover image and the stego image is approximately zero. Stego image is required for the correct extracting of the secret information at the receiver end.

2.1.3 Stego Key

The key to allocate the positions to secret information data bits in cover image pixels is termed as stego key. This stego key is required for the extraction of the secret information or data at receivers end. It could be a pseudo-random number generated or some featured values extracted by some mathematical operation between secret information and cover image pixels.

2.2 Cover Image Selection

Steganography aims to hide the existence of the secret information within the cover image, the main goal is to modify cover image such that neither the existence of the secret information is revealed nor the secret information itself, steganography aims to increase payload capacity and decrease the probability of detect ability of the stego image, cover image selection helps in achieving these goals. Cover image selection can be done by any mathematical operation from the available image database, suitable image is selected from the database and embedding of the secret information is carried out in the selected cover image.

2.3 Embedding Domain

The characteristics exploited of a cover image for embedding the secret information within the cover image is known as embedding domain, the domain may be further divided into spatial domain and transform domain.

2.3.1 Frequency Domain

Digital images are composed of 2 types of frequencies, high frequencies and low frequencies. Smooth areas within an image are represented by low frequency whereas

high frequency represents the edges and sharp transitions within the image. Unlike high frequencies, low frequencies represent plan regions of the image, so modification above certain level can be transparent to Human Visual System (HVS). Pixels in smooth region (Low Frequency) are strongly are strongly correlated to their neighbors while at the edges (High Frequency) pixels deviates from its neighbors, low frequencies contain significant features of the image whereas high frequency corresponds to less important details of the image.

Transformation of the pixel values from spatial domain to frequency domain is done through some transform techniques such as DWT and DCT etc. The transform coefficient obtained after the transformation of the image can be altered by replacing the secret information, the immunity to signal processing is more and less vulnerable to stego attacks. Following are various method to achieve embedding in frequency domain.

2.3.2 Spatial Domain

In spatial domain the secret information data directly modifies the pixel values of the selected cover image. The modification of the cover image pixel values offers attractive features of low complexity and a high embedding capacity. The drawbacks of direct modification of cover image pixel values are that the immunity of the stego image to certain image processing is very low and the vulnerability to stego attacks.

2.4 Existing Techniques

2.4.1 DCT Based Steganography

The input data to DCT is correlated data and its energy is concentrated into the first few transform coefficients [4]. The distribution of frequency in Discrete cosine Transform block suggests that the suitable place for data hiding is higher frequency components as higher frequency components after quantization become zero and hence these coefficient remains unchanged if the input data for embedding is zero, higher frequency components shows more visually resistant towards noise than lower frequency components [4]. Various DCT based steganography tools are discussed below.

2.4.2 JPHide/Jsteg

Embedding of the secret information data in JPHide steganography technique is done by altering the LSBs of the obtained quantized DCT coefficient, the quantized coefficient are selected randomly for embedding, the random selection is done by a pseudorandom number generator which can is controlled by a special key. DCT coefficient having values 0, +1, -1 are not selected for embedding for correct extraction of secret information at the receiver end. JPHide technique has a capacity equal to the number of coefficient having values other than 0, +1, -1 [5], [6].

2.4.3 YASS

Yet another steganography scheme is a DCT based steganography technique in which image is sliced into sub-blocks called big or B blocks. These B blocks are further divided into 8×8 sub blocks, DCT coefficients by QIM of the sub blocks are used for

embedding the secret information. Performs good against steganalysis tool known as self calibration [7]

2.4.4 F5

Westfield introduced the F5 steganography algorithm in which DCT is applied to obtain the coefficients of DCT, if the obtained coefficient value is needs to be alter the absolute value of the DCT coefficient is to be decreased by 1. Matrix encoding is employed to the randomly selected DCT coefficient, non zero coefficients and the maximum length of secret information for embedding is used for employing matrix embedding. Chi square attacks and extended chi square attacks are defended successfully because of randomized selection of the DCT coefficient [8].

2.4.5 Steganography Based On DWT

Image decomposition by DWT gives 4 sub-bands. The most important information is in the lowest sub-band while finer details are in the higher sub-band, the first few transform coefficients are associated with most of the energy, and an entropy coder locates them and encodes them [4]. DWT has better energy compaction than that of DCT with no blocking artifact, the image is decomposes as L level dyadic wavelet pyramid by DWT and resultant wavelet coefficient can easily be scaled in resolution as wavelet coefficients can be discarded at levels finer to a given threshold and thus reconstructs the image with less details [4].

Another steganography technique based on dual transform use a combination of DWT and IWT for embedding secret information into the cover image, high

imperceptibility has achieved and PSNR ranges from 35 to 54 dB is obtained using dual transform method [9].

Several other frequency transformations like integer transform, slant let transform, curve let transform, dual tree DWT, contour let transform can also be combined with DWT for steganography, the choice for the combination of transforms for embedding data, depends on the need of application and the requirements of the user.

2.4.6 Least significant bit (LSB)

Least significant bit (LSB) replacement is one of the famous techniques among steganographic techniques, the main idea of LSB replacement is that to embed the N bits of secret data to the least significant N bits of a grey scale cover image pixels. The binary form of a grey scale image pixel can be represented as $P = (b_0 b_1 b_2 b_3 b_4 b_5 b_6 b_7)$ where b7 is the Most significant bit and b0 is Least significant bit having smallest weight of ±1, since altering the least significant bit of a pixel can only have a change of ±1 to the pixel value so the produced distortion is perceptually transparent.

(11000101 11101001 11001100)

(10101011 11001000 11001101)

(10110100 01100111 11000101)

(01001101 10101101 01101011)

Let we have 4*3 block of binary pixel taken from a cover image, embedding secrete binary data (100110100101) into the LSBs will results in following bits,

(1100010**1** 1110100**0** 1100110**0**)

(1010101**1** 1100100**1** 1100110**0**)

(1011010**1** 0110011**0** 1100010**0**)

(0100110**1** 1010110**0** 0110101**1**)

Replacement of LSBs method the simplest and the easiest method for embedding the secret data into the cover image, LSB embedding method has less computations, large amount of data can be inserted without any major image quality degradation. However the more the LSBs used for insertion the greater will be the distortion produced. This method is most vulnerable to noise or image processing operation like scaling, cropping etc, the tolerance to change in the pixels values of an image is different for different pixels. Changes of pixels grey value in smooth areas within images are easily noticeable by human eyes [10]. Stego attacks can easily detect the LSB insertion.

2.4.7 Pixel indicator technique

PIT in [11] for color images uses the two LSBs of red plane as an indicator for the secret information bits to be embedded in the other two green and blue planes, the indicator bits depends on nature of the image. Relation between secret information bits and the indicator is presented in table 2.1.

Table 2.1: Indicator values Based action

Plane 1	Plane 2	Plane 3
00	No data bits	No data bits
01	No data bits	2 bits of data
10	2 bits of data	No data bits
11	2 bits of data	2 bits of data

Indicator plane is not fixed. Selection of the indicator plane is done by some sequence which results in a better security of the secret information embedded inside the cover image. This technique is not robust and hence can be easily detected by steg analysis.

2.4.8 Pseudo-Random LSB Encoding Technique

The technique uses a random key for random selection of pixels for embedding, where the secret data bits to be embedded [10]. This makes it difficult for unauthorized user to find the secret data bits without have the random-key. Since color images have three planes, secret data bits can be hiding randomly in LSBs of any plane of the color image pixels. Randomizing the selection of pixels, a layer of security is added so it becomes difficult for unauthorized user to identify the pattern of the secret data bits. The random key is also embedded within cover image for extracting the original secret data bits at the receiver end. This technique is not robust against cropping, scaling, translation etc.

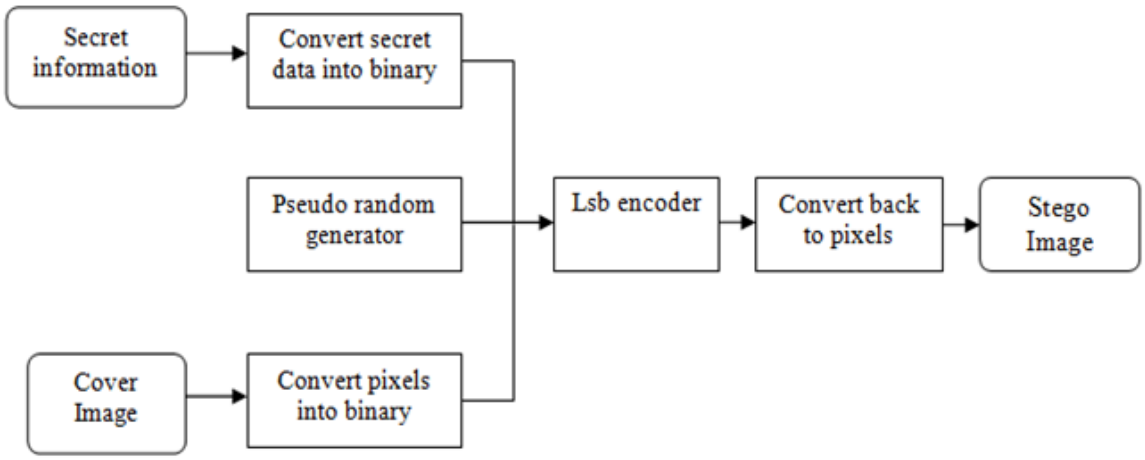


Figure 2. 1: Pseudo-Random LSB technique

2.4.9 Distortion Technique

Distortion Technique in [12] is the modified form of LSB substitution. In this method the LSBs of the pixel values are only modified when the secret data bit is 1 otherwise the pixel value is not changed unlike LSB method where every pixel value is modified with secret data bits. Pseudorandom generator is used for selection. By embedding bit 1, random value of *x* is subtracted or added to the pixel value, value of *x* is chosen so that the change in cover image is minimized [12]. At receiver end comparison of stego image and original cover image is done. If the pixels are different the corresponding secret data bit is 1; else, the secret data bit is 0**.**

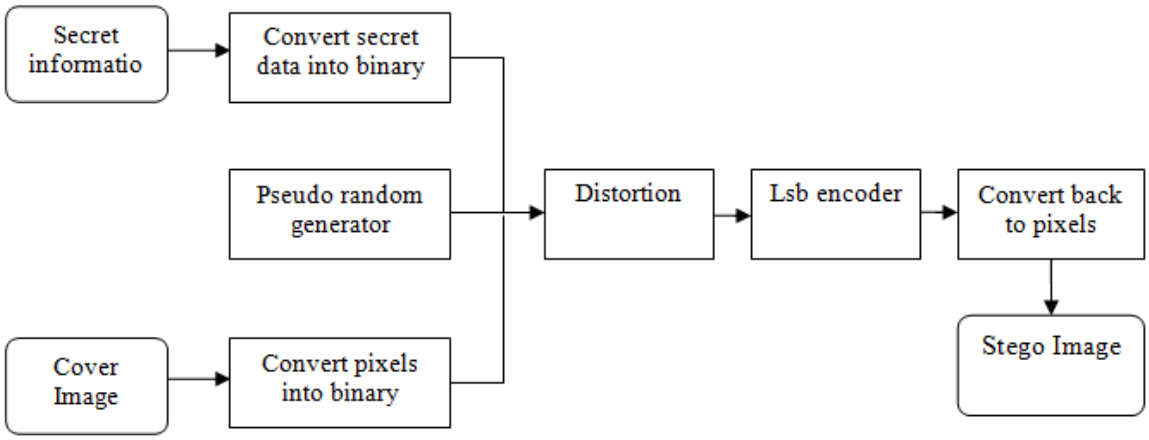


Figure 2.2: Distortion technique.

2.4.10 Pixel value differencing (PVD)

To address these problems, Da-Chun Wu, Wen-Hsiang Tsai in [13] proposed a new steganographic technique pixel value differencing (PVD) for embedding secret information data in to cover image based on the capabilities of human visual perception. In the proposed method cover image is divided two pixel blocks, these blocks are categorized by the differences of the two pixel grey values of each block. Smooth regions have a small difference of the pixel grey values while a large difference indicates edge region of an image. Since edge regions can tolerate large changes compare to smooth regions, so this proposed method embeds large amount of data in to the edge regions and small amount of data into smooth regions. The method provides better way of hiding large amount of data in to cover images with imperceptions, and also provides an easy way to accomplish secrecy [10]. The problem with this approach is that a block of two pixels cannot determine the features of edges

properly; images have more smooth regions which are less tolerable to large amount of changes which affects the embedding capacity.

2.4.11 Pixel Ranking and Particle Swarm Optimization

Another steganographic method proposed in [14] based on Pixel Ranking and PSO, an improvement to the simple LSB. Cover image pixels having LSBs which are most similar to the MSBs in the secret image are identified by four features and respective coefficients [14]. The (MSBs) of the secret data is embedded into the (LSBs) least significant bits of the cover image by using PSO to rank the pixels. Four features are extracted with their corresponding coefficients, using these features pixels are ranked and the optimal order is selected. The bits are then embedded to the LSBs of the selected order.

2.4.12 LSB+DWT

Focusing the embedding capacity, a new technique was proposed in [15] which compress secret data before embedding, two dimensional DWT is performed on the blocks of the cover image to obtain the DWT coefficients of the blocks of the cover image, Huffman encoded bit stream is than embedded to the LSBs of the obtained coefficients. Huffman dictionary and size of the bit stream encoded by Huffman encoder is also embedded to the cover image for retrieval of the secret data at the receiver end. Privacy and capacity is obtained by the Huffman encoding while secrecy is obtained by the transformation of the cover image. This technique is robust to geometrical distortion like scaling, cropping, translation etc. however the PSNR doesn’t reach the expected value.

2.4.13 LSB Based Steganography Using AES Algorithm

An Improved technique [16] based on modification of the pseudorandom LSB embedding technique was proposed in 2017, the length of the secret data is reduced by lossless deflate algorithm which couples the Huffman and LZ77 algorithm. One more important characteristic of this technique that it protects the secret data by AES algorithm, the secret passes through 3 different processes before embedding into cover image. At first stage the secret data is encrypted by AES algorithm for security purpose; second phase is to compress the encrypted secret data using deflation algorithm for increasing the capacity, the bits of the encrypted compressed data is then embedded into the LSBs of the cover image using a random key for choosing the pixel randomly for bits insertion.

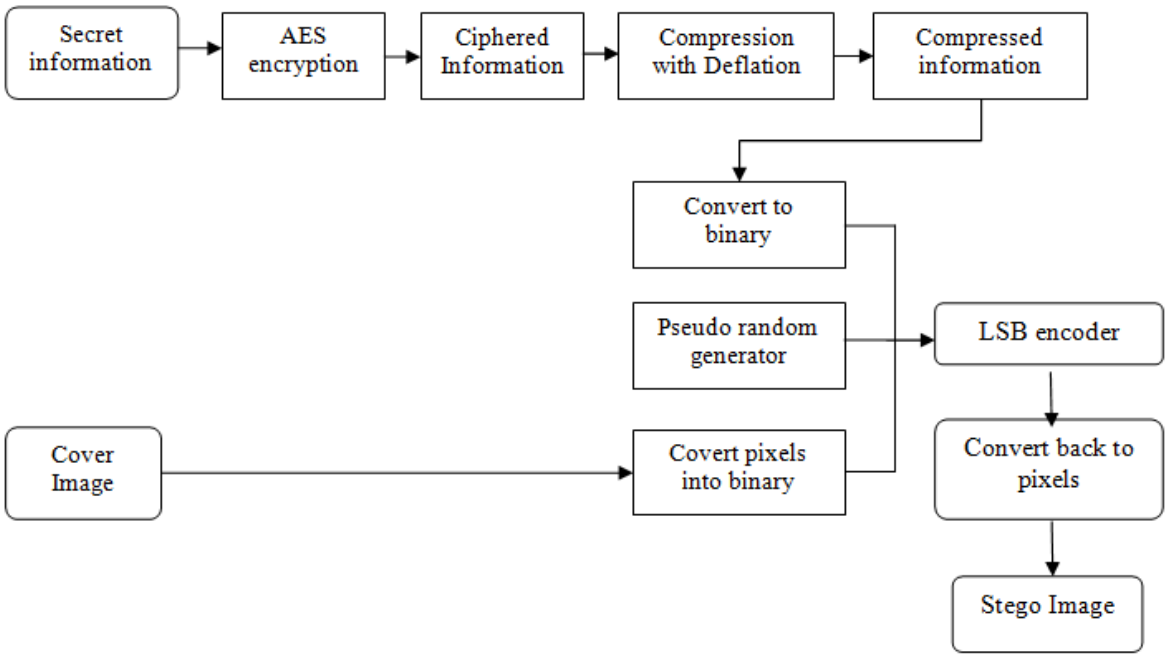


Figure 2.3: Transmitter end [16]

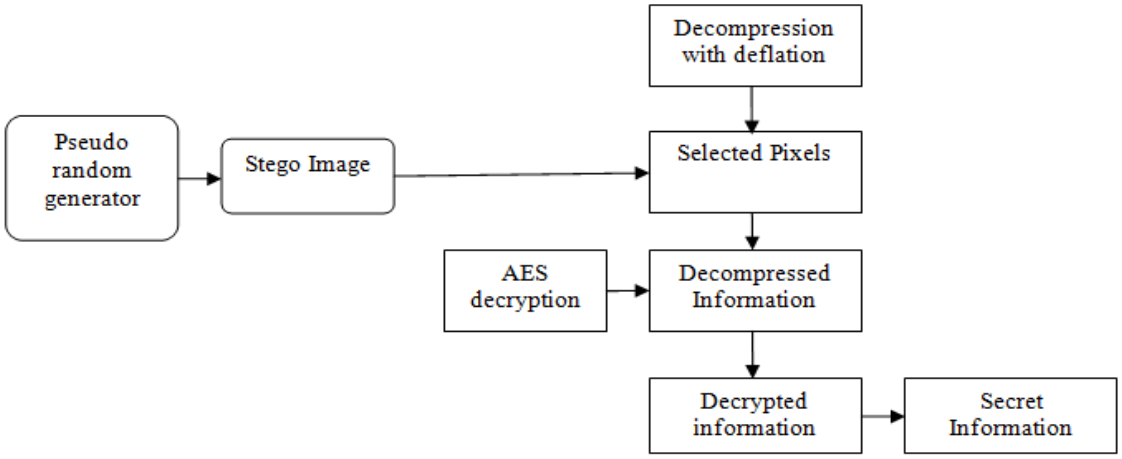


Figure 2.4: Receiver end [16]

2.4.14 Enhanced LSB Substitution Technique [17]

Another enhanced version of LSBs substitution technique was proposed in [17], secret data is encrypted before embedding using AES 256 bit encryption. The number of bits to be stored in the LSBs of a pixel depends on the position of the first set bit of that pixel. The basis for selection of no. of bits to be replaced is presented in table 2.2 [17].

Table 2.2: Basis for Selection of number of Bits to replace [17]

Bit number	Replace number of Bits
7-8	4
5-6	3
3-4	2
1-2	1

Security is doubled as the data is encrypted before embedding; the increased embedding capacity results in a poor PSNR of the original image and the stego-image.

2.4.15 LSB Based Color Image Steganography [18]

An improved LSB hiding method proposed in 2016 [18] combining secret data hiding and cryptography, digital signature and encryption has done before embedding into cover image. The three components of the color image have different sensitivity; the most sensitive to be is green, the modest sensitive to red, the least sensitive to blue [18]. So bits of the encrypted secret data do XOR with the LSB of green plan and embed in either corresponding red or blue plane. If the result of XORING is 1, bit is replaced in red LSB plane. When the result is 0 blue LSB plane is replaced with the bit and so on. Combination of the signatures and encryption with a random LSBs embedding improves the security of the secret information.

2.4.16 Optimized Pixel Value Differencing

A High-capacity and secure information Data hiding technique using encryption, compression and modified pixel value differencing is presented in [19]. Compression is carried out by Arithmetic coding [20]. On average, round about 22 percent higher payload capacity can be achieved using Arithmetic Coding [19]. Output of the Arithmetic coding is the input to AES based encryption [21], which ensures a higher level of security.

This compressed and encrypted information bits are embedded in to the LSBs of the cover image using LSB+PVD method. An increased payload capacity of 3 percent more than existing techniques has achieved by MPVD, MPVD and arithmetic coding as

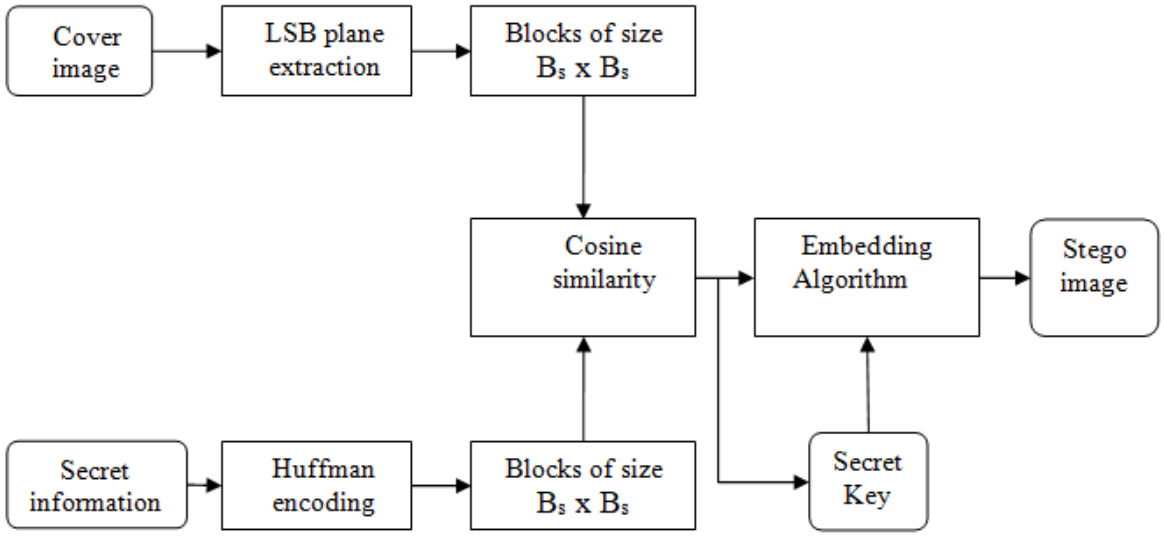
a combo resulted in 25 percent higher payload capacity [19]. However the PSNR value is not considerably good.

2.4.17 Hybrid image steganography based on IWT-LSB techniques [22]

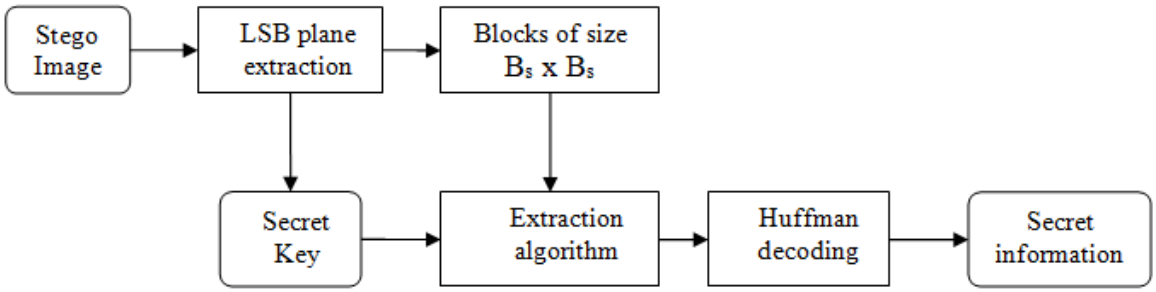
The hybrid approach presented in [22] is a comb of the IWT and LSB approaches, in this method the cover image is IWT transformed before embedding. After transforming cover image, approximation coefficients of cover image is obtained, the bits of the secret information is than embedded in to the LSBs of the approximation confident using the traditional LSB approach, inverse IWT transform is applied to obtain the stego image. Reverse of this process will retrieve the original secret information. This hybrid approach results in good PSNR but the capacity of the proposed approach is low.

PROPOSED METHODOLOGY

The proposed approach combines Huffman encoding algorithm with LSB's insertion on the bases of similarity between the secret information I and the LSB plane of the cover image C. The proposed approach has two phases: embedding phase and the extracting phase, the secret information in embedding phase I is compressed using Huffman compression and is then embedded into the LSB plan of cover image C using cosine similarity to form a Stego image S, a secret key K is generated in the embedding phase and is inserted within the Stego image S for the extraction of the secret information I from the LSB plane of the Stego Image in the extraction phase. The proposed technique is shown in figure 3.1.



(a) Embedding phase



(b) Extraction phase

Figure 3.1: Embedding and Extracting phases of the proposed approach

3.1 Compression through Huffman encoding

In this study a chapter of this thesis is taken as secret information I which includes different characters, these characters are represented by ASCII (stands for American Standard Code for Information Interchange) codes, Many programming languages uses these ASCII codes for the representation of characters. In ASCII coding, each character is represented by the same eight numbers of bits. With 8-bits 256 different levels can be represented and the ASCII character set contains 256 different characters [23]. Given the fact that some of the characters have high probability of occurrence while some characters have less probability of occurrence, Huffman compression algorithm uses these characteristics of high probability and low probability of occurrence for compressing the data. The most frequent characters are encoded by lower number of bits, while characters with less frequency are encoded with high number of bits. Huffman algorithm works by building a tree called binary tree, beginning from the leaves representing the characters or symbols which adds up on certain rules to make a single node and the process goes on until a single node reaches, this final node is termed as

root of the tree. Each leaf of the tree represents a particular character and the occurrence of that particular character with in the data.

For this study Huffman binary tree and the compressed binary bits stream H(I) of the secret information I is obtained by the following steps.

- Number of occurrences of every character with in secret information I (chapter of this thesis) is counted.
- Leaves representing characters and number of occurrence are formed from left to right in ascending order.
- Two leaves having smallest weights combined to form a node whose weight is equal to the sum of the weights of the two leaves also called parent nodes.
- Node obtained in step 3 is reconsidered in step 2.
- Repeat step 2 and 3 until single node left. The last one node is called the root of the optimal encoding tree.
- Starting from the root obtained in step 5, every step from the root towards the leaves is either to the left or to the right at every node, movement towards the left of the node is considered to be zero while to the right is considered to be one.
- Since all the character nodes are seen to be the leaves and the path from the root ends up here and does not go further, this feature ensures prefix-free property of the compression scheme, when a leaf is reached that means next bit in the encoded sequence is the first bit from the next encoded character.
- Characters are represented by leaves so code words for all the characters are obtained by tracing back the path from the root towards the leaves where each leaf represents a particular character.

- A table is constructed for the characters and their specific variable length code words known as Huffman table also called Huffman dictionary.
- Secret information is encoded using Huffman dictionary obtained in step 9, resulting in a compressed bits stream H(I), hence the output is a bit stream H(I), and Huffman dictionary H(D) which is required for decoding of the bit stream.

Huffman compression has a property and is known as the prefix free property which means that there is no sequence encoding of any character which is the prefix for the bit sequence encoding for another character. This property also makes it possible for decoding of a bit stream using the encoding tree by following root to leaf paths, figure 3.2 shows the flowchart of Huffman compression.

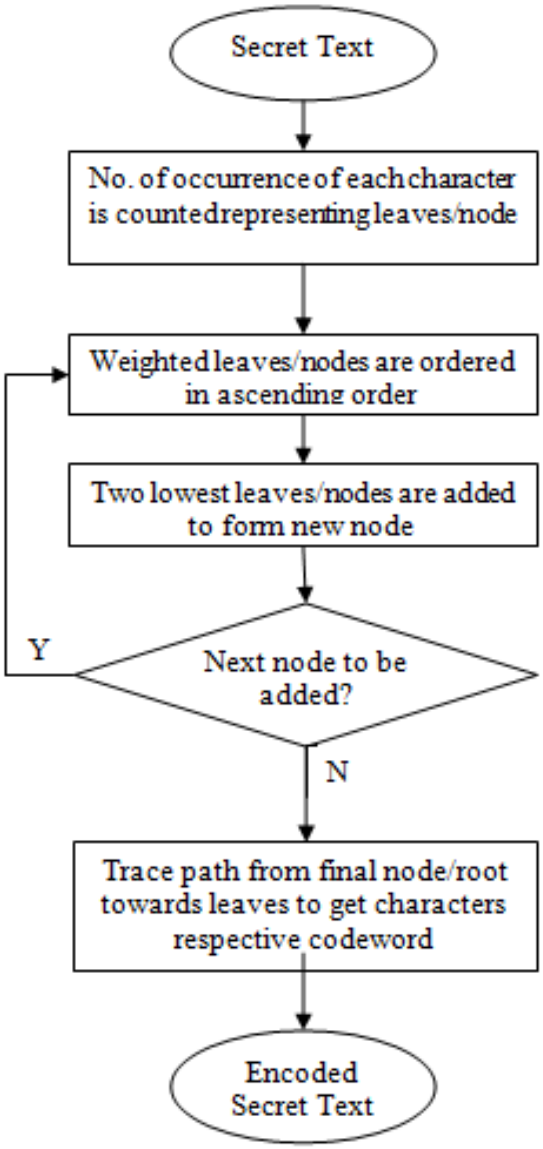


Figure 3.2: Flowchart of Huffman encoding

As an example Figure 3.3 shows the basic idea for constructing a binary Huffman tree and their respective code words for (**image steganography**). There are 19 characters in “image steganography” and every character is represented by 8 numbers of bits, hence a total of 152 bits are required to represent “image steganography”. With Huffman compression these 152 bits representation is reduced to 55 bits, which means the data is compressed by almost 63% of its original length or size.

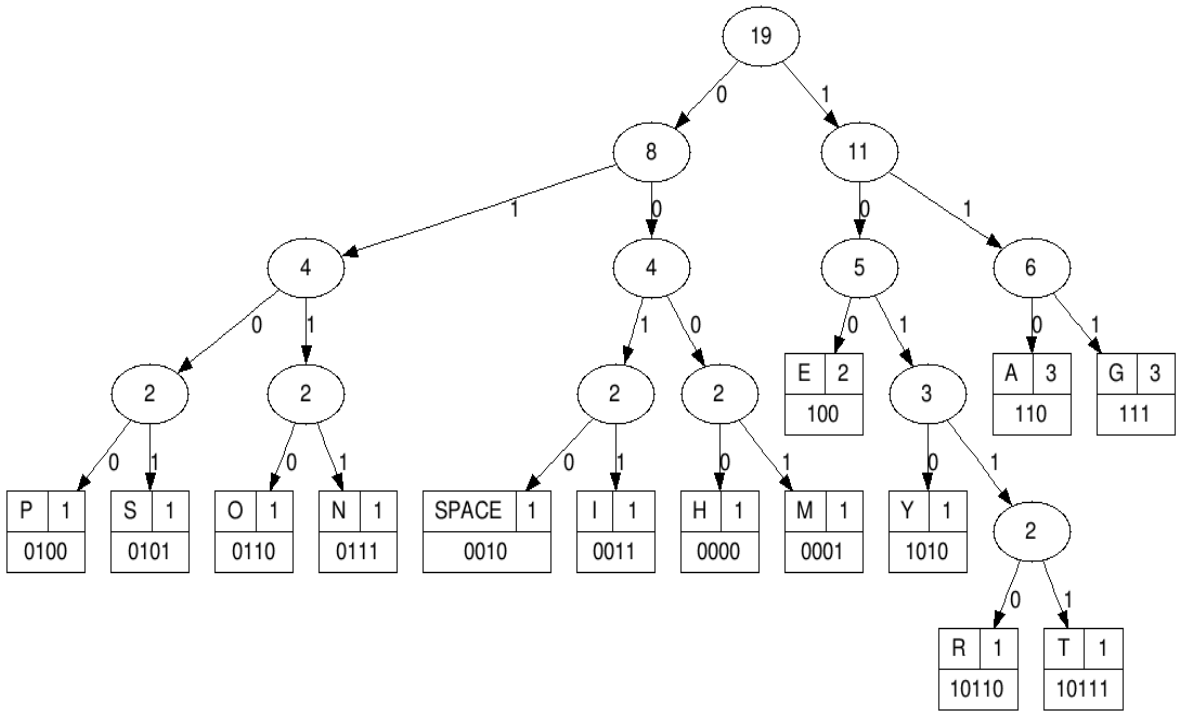


Figure 3.3: Huffman binary tree for (image steganography)

3.2 Cosine Similarity

Cosine similarity is a similarity measuring metric used to calculate the similarity between two documents or data, mathematically, cosine similarity calculates the cosine of the angle between two matrices or vectors projected in a multi dimensional space, if the angle between two vectors A and B is zero, similarity between them is one, the larger the angle between vector A and vector B, the smaller their similarity. Cosine similarity between A and B can be calculated by the equation 3.1.

$$\boldsymbol{sim(A,B)} = \frac{\boldsymbol{A \cdot B}}{\boldsymbol{|A||B|}} = \frac{\sum_{\boldsymbol{i=1}}^{\boldsymbol{k}} \boldsymbol{Ai \times Bi}}{\sqrt{\sum_{\boldsymbol{i=1}}^{\boldsymbol{k}} \boldsymbol{(Ai)^2}} \times \sqrt{\sum_{\boldsymbol{i=1}}^{\boldsymbol{k}} \boldsymbol{(Bi)^2}}} \qquad (3.1)$$

As an illustration two 8×8 binary matrices has takes as cover LSB matrix and secret information I matrix shown in figure 3.4 (a) and (b).

1	0	1	1	1	1	1	1
0	0	1	0	0	0	1	0
0	1	1	1	0	1	0	0
1	1	0	0	1	0	0	1
1	0	1	0	1	0	1	0
1	0	0	0	0	1	1	0
0	0	0	0	1	0	0	1
1	1	1	1	1	0	1	0

(a)

1	0	1	1	0	0	1	0
1	0	0	1	0	0	1	0
0	0	1	1	0	0	1	0
1	0	0	1	0	0	1	0
0	0	1	0	1	0	1	0
1	0	0	0	0	0	1	0
0	1	0	0	1	0	1	0
1	0	0	1	1	0	1	0

(b)

Cover Plane

Secret information I

Figure 3.4: (a) 8×8 cover LSB matrix (b) 8×8 binary matrix of secret information I

Both cover matrix C and secret information I matrix were divided into A_n and B_m sub-blocks of size $B_s \times B_s$, where the sub-block size B_s is taken as 4, are shown in figure 3.5 and figure 3.6 respectively, where A_n and B_m is totally dependent on B_s, in this example n and m=1,2,3,4.

1	0	1	1
0	0	1	0
0	1	1	1
1	1	0	0

(a)

1	1	1	1
0	0	1	0
0	1	0	0
1	0	0	1

(b)

1	0	1	0
1	0	0	0
0	0	0	0
1	1	1	1

(c)

1	0	1	0
0	1	1	0
1	0	0	1
1	0	1	0

(d)

Figure 3.5: Cover blocks (a) A_1 (b) A_2 (c) A_3 (d) A_4

1	0	1	1
1	0	0	1
0	0	1	1
1	0	0	1

(a)

0	0	1	0
0	0	1	0
0	0	1	0
0	0	1	0

(b)

0	0	1	0
1	0	0	0
0	1	0	0
1	0	0	1

(c)

1	0	1	0
0	0	1	0
1	0	1	0
1	0	1	0

(d)

Figure 3.6: Secret information Blocks, (a) B_1 (b) B_2 (c) B_3 (d) B_4

Now to find the similarity between blocks given in figure 3.4 and 3.5, equation 3.1 is used to calculate the similarity of each B_m block in secret information I with every A_n cover block, i.e. similarity between B_1 and A_1 is 0.6667, B_1 and A_2 is 0.5893, B_1 and A_3 is 0.6299 and B_1 and A_4 is 0.4714, similarly the similarity values between B_2 and A_1, A_2, A_3 and A_4 are 0.5000, 0.3536, 0.3780 and 0.5303 respectively, and that of B_3 and A_1, A_2, A_3, and A_4 are 0.4472, 0.6325, 0.6761 and 0.3162 respectively, for B_4 and A_1, A_2, A_3 and A_4 the cosine similarity values calculated are 0.6299, 0.5345, 0.5714 and 0.8018 respectively.

Cosine similarity suggests that the more the value approaches to 1, the greater the similarity between the two vectors A and vector B, where as the value approaches to zero, that means the two vectors or matrices are dissimilar.

3.3 Embedding process

Following steps shows how embedding of the proposed technique is carried out.

- Cover image of size M x M is first converted into binary pixel values, LSB plan is extracted from these binary pixel values of size M x M and divided into sub-blocks of size B_s x B_s resulting in A_n sub-blocks.

- The compressed bit stream H (I) from the Huffman encoder is then reshaped into a square matrix of size N x N, where N x N is the nearest greater value to the size of H (I). The compressed secret data bit stream H (I) is padded with zeros if the product of its size is less than the product N x N which is the nearest greater value to the size of H (I), the compressed secret information matrix is then divided into sub-blocks of size B_s x B_s resulting in B_m sub-blocks of the secret information.
- Cosine similarity is calculated by equation (1) between A_n and B_m (where $n \geq m$), cosine similarity of each block in B_m is calculated with every block in A_n, most similar blocks to each other are mapped which is used for embedding and extracting the B_m blocks from A_n blocks, this mapping is termed as secret key K.
- A_n blocks are replaced by B_m blocks according to the secret key K obtained in step 3, which results in a new set of blocks R_n.
- Secret key K is embedded in a specific know region of the cover image for the correct extraction of the secret data H (I) hidden in the cover image.
- Now replacing LSB plane of the cover image by the reshaped R_n blocks, results in a stego image.

3.4 Extraction Process

Extraction of the secret data involves the following steps.

- Read the stego image.
- Secret key K is extracted from a specific known region of the cover image.

- After extracting the key, pixel values of the stego image of size M x M is first converted into binary pixel values, LSB plan is extracted from these binary pixel values of size M x M and divided into sub-blocks of size B_s x B_s to get R_n blocks.
- Using secret key K B_m blocks are extracted from R_n blocks, these blocks are then reshaped to get the compressed bit stream H(I).
- H (I) is decoded using Huffman table which results in secret information I.

Chapter 4

RESULTS AND DISCUSSION

Results of the proposed information hiding technique are evaluated in this section. Implementation and evaluation of the proposed technique were carried out using MATLAB. Grayscale cover images of 512x512 pixels shown in figure 4.1 are used for experimentation. The secret information I for embedding is the text from this thesis. The performance evaluation parameters, hiding capacity, MSE (Mean squared error), PSNR and NCC (Normalized cross correlation) were used for the evaluation of the proposed information hiding technique with existing information hiding techniques including simple LSB and IWT-LSB [22]. Experimental results were examine and disused in the following sub-sections.

Lena

(b) Barbara

(c) jet plane

Figure 4.1: Grayscale cover images of size 512×512

4.1 Parameters

4.1.1 Hiding Capacity

The payload capacity of any steganography technique is calculated as the total number of secret information I bits to be embedded in cover image. The embedding rate bit per pixel bpp is measured using equation 4.1.

$$\boldsymbol{BPP} = \frac{\text{Embedding capacity}}{\text{M}\times\text{N}} \tag{4.1}$$

Where M and N represents the size of the cover image, test images used for experimentations are of size 512 x 512, embedding is done only on the LSB plane of the cover image, so the maximum secret information I characters that can be embedded are 32768 characters or (32768 x 8 = 262144bits)or 1 bit per pixel bpp.

However, with the addition of the Huffman compression technique which compresses the secret information I before embedding, the capacity can be increased up to 1.6 bpp.

4.1.2 MSE and PSNR

The MSE calculates the cumulative squared error between the cover image and stego image, where as the PSNR is the measure of the peak error, these two parameters are used for measuring the quality and imperceptibility of the stego image. Equation 4.2 and 4.3 are used for calculating MSE and PSNR of the stego image S and the cover image C.

$$MSE = \frac{1}{M\times N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[S(i,j) - C(i,j)]^2 \tag{4.2}$$

$$PSNR = 10log\left(\frac{\boldsymbol{Cmax^2}}{\boldsymbol{MSE}}\right) \quad (4.3)$$

Where M and N represents the size of the cover image C and stego image S respectively, while C_{max} represents the maximum value in the cover image. Smaller the MSE value the higher will be the PSNR value which results in better quality and imperceptibility. Research shows that for good quality of stego image, the PSNR value should be greater than 40 dB.

4.1.3 Normalized Cross-Correlation (NCC)

NCC is known technique for evaluating the degree of similarity or closeness between two functions or images, this evaluation determines the extent that how much the stego image S has been deviated from the original cover image C. Equation 4.4 show the formula for calculating the Normalized cross-correlation NCC.

$$NCC = \frac{\sum_i \sum_j (\boldsymbol{c(i,j)} - \boldsymbol{X})(\boldsymbol{s(i,j)} - \boldsymbol{Y})}{\sqrt{\left(\sum_i \sum_j (\boldsymbol{c(i,j)} - \boldsymbol{X})^2\right)\left(\left(\sum_i \sum_j (\boldsymbol{s(i,j)} - \boldsymbol{Y})^2\right)\right)}} \quad (4.4)$$

Where $c(i,j)$ and $s(i,j)$ are the intensity values of i^{th} row and j^{th} column of the cover image C and stego image S respectively, while $\overline{X}$ represents the mean of the cover image C and $\overline{Y}$ represents the mean of the stego image.

The value for NCC ranges between -1 and 1. If NCC value falls in negative range, that means relation between the two function or images are negatively correlated, as the value approaches to -1 the two functions becomes the opposite of each other. And if the value is in the positive range, that means the relation between the two function or images are positively correlated, as the value approaches to 1 the correlation between

the two functions or images become stronger and the two functions or images become identical copies of each other.

4.2 Results

In this section a detailed analysis of the parameters is carried out, images given in figure 4.1 are taken as Cover images for experimentations. Unlike the traditional LSB embedding, the proposed technique make sub-blocks of the secret information S and that of cover image C, these blocks are made in such a manner that brings randomness in the secret information to be embedded which ensures security of the secret information, block size $B_s \times B_s$ is taken as 32×32 throughout the experimentation. Replacement of the cover blocks by secret information blocks are done by cosine similarity, cosine similarity finds the most similar blocks in cover blocks to the blocks of secret information, hence number of difference bits decreases.

4.2.1 Embedding rate versus MSE, PSNR and NCC

Embedding rate versus MSE, PSNR and NCC of this proposed technique is carried out for the cover images given in figure 4.1. PSNR, MSE and NCC are evaluated for the proposed technique for the images Lena, baboon and jet with different embedding rate. Table 4.1 shows that at maximum capacity of the proposed technique 1.6 bits per pixel, the PSNR, MSE, and NCC values for the image Lena are 51.1828, 0.5002 and 0.99 respectively, and for the image Barbara PSNR, MSE and NCC values are 51.1837, 0.5001 and 0.99 respectively, and for the image jet the values of PSNR, MSE, and NCC are 51.1779, 0.5002 and 0.99 respectively.

Table 4.1: PSNR, MSE and NCC values for maximum capacity 1.6 bits per pixel

Cover image	MSE	NCC	PSNR
Lena	0.5002	0.99	51.1828
Barbara	0.5001	0.99	51.1837
Jet	0.5002	0.99	51.1779

Table 4.2 contains the PSNR, MSE and NCC values for the cover images Lena, Baboon and Jet at 1 bit per pixel embedding rate. At 1 bit per pixel embedding rate for the image Lena the PSNR, MSE and NCC values are 53.5699, 0.28 and 0.99 respectively, and for the image Barbara the PSNR, MSE and NCC values are 53.4566, 0.28 and 0.99 respectively. For jet plane the PSNR, MSE and NCC values are 53.5648, 0.27 and 0.99 respectively.

Table 4.2: PSNR, MSE and NCC values at embedding rate of 1 bit per pixel

Cover image	MSE	NCC	PSNR
Lena	0.28	0.99	53.5699
Barbara	0.28	0.99	53.4566
Jet	0.27	0.99	53.5648

The embedding rate 0.5 bit per pixel gives more better PSNR and MSE, for Lena the PSNR, MSE and NCC values are 56.2757, 0.153 and 1, for Barbara the values are 56.2750, 0.152 and 1, for jet plane the values are 56.2841, 0.150 and 1 respectively. Table 4.3 summarizes the parameters for the cover images Lena, Barbara and Jet at embedding rate of 0.5 bit per pixel.

Table 4.3: PSNR, MSE and NCC values with embedding rate of 0.5 bit per pixel

Cover image	MSE	NCC	PSNR
Lena	0.153	1	56.2757
Barbara	0.152	1	56.2750
Jet	0.150	1	57.2841

Figure 4.2 shows covers image and their respective stego images at the maximum embedding rate 1.6 bits per pixel, at 1 bit per pixel and at 0.5 bit per pixel.

(Cover Image) (Stego-Image 0.5Bpp) (Stego-Image 1Bpp) (Stego-Image 1.6Bpp)

(Lena original) (Lena Stego) (Lena Stego) (Lena Stego)

(Barbara original) (Barbara Stego) (Barbara Stego) (Barbara Stego)

(Jet original) (Jet Stego) (Jet Stego) (Jet Stego)

Figure 4.2: Grayscale Cover and their respective Stego images at different embedding rate

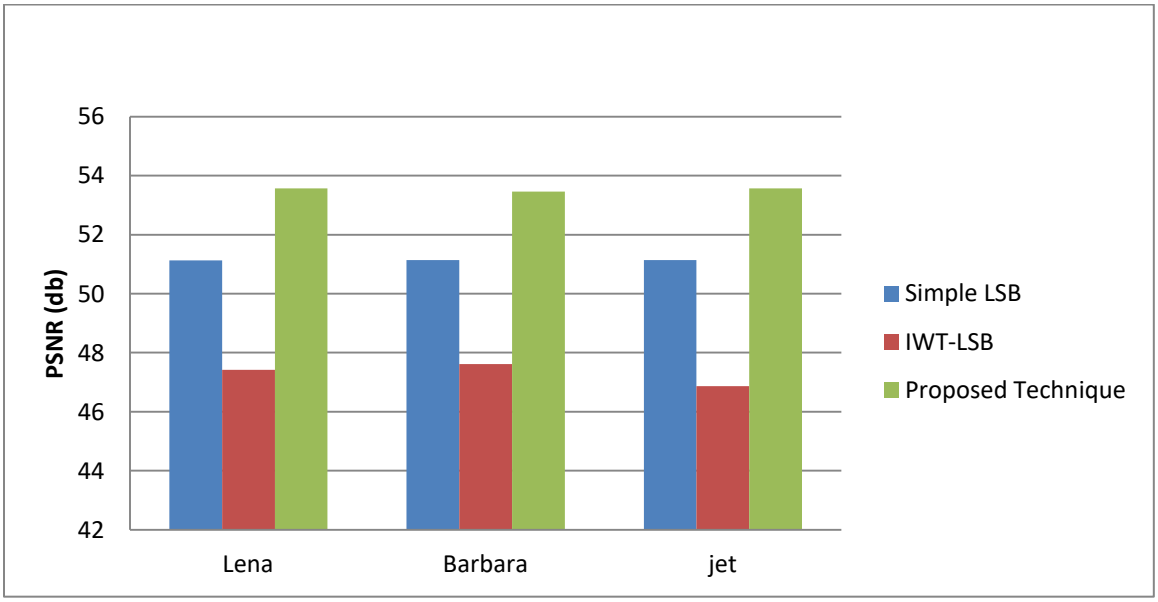
4.3 Comparison of Proposed Technique with the existing Techniques

Comparison of the proposed technique with other existing techniques i.e. simple LSB and the technique IWT-LSB presented in [22] is carried out, Table 4.4 presents the PSNR, MSE and NCC values of simple LSB, technique presented in [22], and the proposed technique at the embedding rate of 1 bit per pixel. Grayscale images Lena, Barbara and jet of size 512×512 shown in figure 4.1 are used as cover images, for the image Lena, the PSNR value calculated for the existing techniques simple LSB, IWT-LSB and the proposed technique are 51.13, 47.42 and 53.569 respectively, the MSE value for simple LSB, IWT-LSB and proposed technique is 0.501, 1.084 and 0.28, the normalized cross correlation NCC value for the simple LSB, IWT-LSB and the proposed technique is the same 0.99. For the image Barbara the PSNR values calculated for simple LSB, IWT-LSB and the proposed technique are 51.14, 47.61 and 53.4566 respectively, the MSE value of simple LSB, IWT-LSB and the proposed method are 0.498, 1.081 and 0.28 respectively, the NCC value for the simple LSB is 0.98 and 0.99 for IWT-LSB and the proposed technique. For the image jet the PSNR values calculated for simple LSB, IWT-LSB and the proposed technique are 51.14, 46.87 and 53.5648 respectively, the MSE value of simple LSB, IWT-LSB and the proposed method are 0.491, 1.086 and 0.27 respectively, the NCC value for the simple LSB is 0.98 and 0.99 for IWT-LSB and the proposed technique.

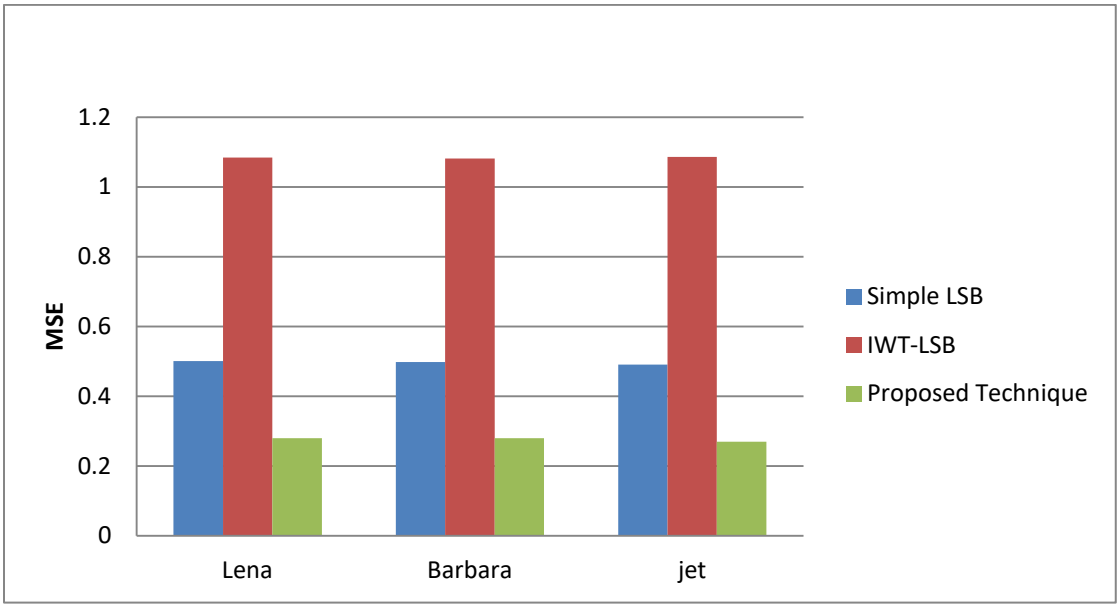
Table 4.4: Values of NCC, MSE and PSNR, of the proposed steganography technique applied to grayscale cover images at the embedding rate of 1 bpp

Cover image	Simple LSB			IWT-LSB[12]			Proposed Technique		
	NCC	MSE	PSNR	NCC	MSE	PSNR	NCC	MSE	PSNR
Lena	0.99	0.501	51.13	0.99	1.084	47.42	0.99	0.28	53.569
Barbara	0.98	0.498	51.14	0.99	1.081	47.61	0.99	0.28	53.456
Jet	0.99	0.491	51.14	0.99	1.086	46.87	0.99	0.27	53.564

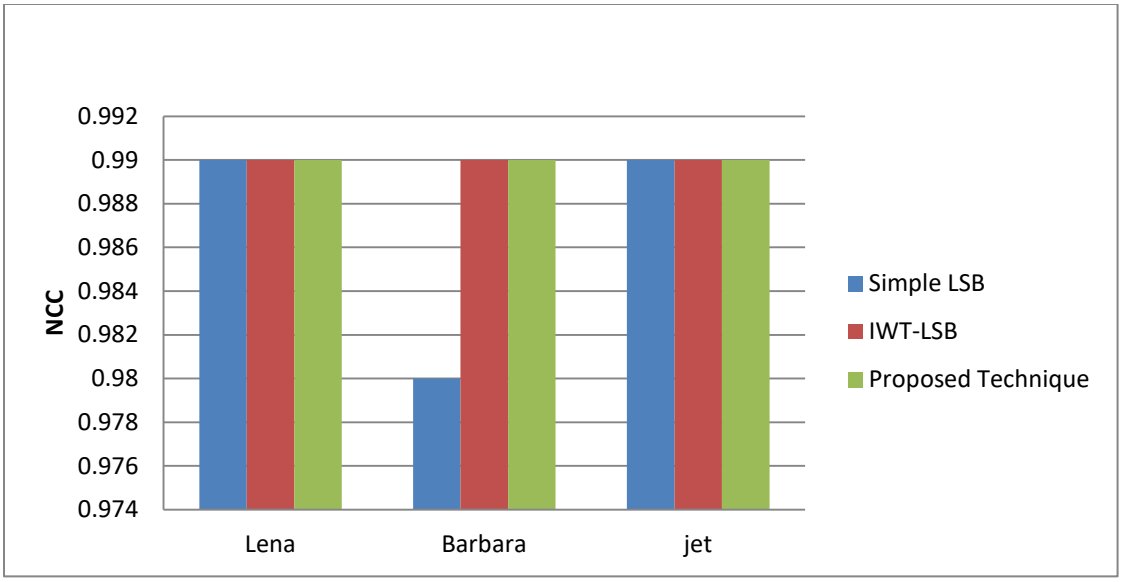
Comparison of PSNR, MSE and NCC of proposed technique with existing techniques including Simple LSB, IWT-LSB is graphically represented in figure 4.3.



(a)



(b)



(c)

Figure 4.3: Comparison (a) PSNR (b) MSE (c) NCC

Experimental results shows that the proposed technique can hide a large payload capacity with better PSNR and MSE compare to other existing techniques, better PSNR and MSE value ensures imperceptibility of the stego media. The NCC value shows the closeness between the original cover and the stego image. The proposed technique has better PSNR, MSE and NCC values than previous techniques.

Conclusion

In this thesis, the proposed steganography technique for hiding the secret information or data in the digital image is based on cosine similarity. The proposed technique is performed using MATLAB 2017. Before embedding, the secret information is compressed by using Huffman compression which increases the payload capacity of the proposed technique, after compression the secret information blocks and the cover blocks are evaluated using cosine similarity, the most similar blocks are replaced in the cover blocks, the blocks from the secret information are taken randomly to ensure security of the secret information, with the use of cosine similarity the alteration of bits in within the cover image is minimized.

Three different cases has been studied with three different embedding rates on three different cover images, results shows that the proposed technique give better PSNR with greater payload capacity than the previous existing techniques. Experimental results shows that the technique proposed in this thesis has a maximum payload capacity of 1.6 bpp with PSNR value of 51.1828, which means a total of 57000 characters, can be embedded into a grayscale image of size 512×512, the maximum PSNR value achieved is 57.2841 at 0.5 bpp. The proposed technique also results in better MSE value of 0.25 and normalized cross correlation NCC value of 0.99. The results of the parameters of the proposed technique surpasses the existing techniques, hence a better steganography technique.

References

[1] Rai, Pooja, Sandeep Gurung, and M. K. Ghose. "Analysis of image steganography techniques: a survey." *International Journal of Computer Applications* 114.1 (2015).

[2] Cheddad, Abbas, et al. "Digital image steganography: Survey and analysis of current methods." *Signal processing* 90.3 (2010): 727-752.

[3] Crandall, Ron. "Some notes on steganography." *Posted on steganography mailing list* (1998): 1-6.

[4] Subhedar, Mansi S., and Vijay H. Mankar. "Current status and key issues in image steganography: A survey." *Computer science review* 13 (2014): 95-113.

[5] Vijay H. Mankar , D. Upham, Jsteg, 1993 http://zooid.org/paul/crypto/jsteg. html (accessed: 2013-07-05).

[6] Mansi S, A. Latham, Jphide, 1999 http://linux01.gwdg.de/alatham/ stego.html (accessed: 2013-07-05).

[7] Solanki, Kaushal, Anindya Sarkar, and B. S. Manjunath. "YASS: Yet another steganographic scheme that resists blind steganalysis." *International Workshop on Information Hiding*. Springer, Berlin, Heidelberg, 2007.

[8] Westfeld, Andreas. "F5—a steganographic algorithm." *International workshop on information hiding*. Springer, Berlin, Heidelberg, 2001.

[9] Prabakaran, G., R. Bhavani, and K. Kanimozhi. "Dual transform based steganography using wavelet families and statistical methods." *2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering*. IEEE, 2013.

[10] Hossain, J. "Information-hiding using image steganography with pseudorandom permutation." *Bangladesh Research Publications Journal* 9.3 (2014): 215-225.

[11] Gutub, Adnan, et al. "Pixel indicator high capacity technique for RGB image based Steganography." (2008).

[12] Sumathi, C. P., T. Santanam, and G. Umamaheswari. "A study of various steganographic techniques used for information hiding." *arXiv preprint arXiv:1401.5561* (2014).

[13] Wu, Da-Chun, and Wen-Hsiang Tsai. "A steganographic method for images by pixel-value differencing." *Pattern Recognition Letters* 24.9-10 (2003): 1613-1626.

[14] Nickfarjam, Ali Mohammad, and Zohreh Azimifar. "Image steganography based on pixel ranking and particle swarm optimization." *The 16th CSI International Symposium on Artificial Intelligence and Signal Processing (AISP 2012)*. IEEE, 2012.

[15] Vijay, M., and V. VigneshKumar. "Image steganography algorithm based on Huffman encoding and transform domain method." *2013 Fifth International Conference on Advanced Computing (ICoAC)*. IEEE, 2013.

[16] Chikouche, Sofyane Ladgham, and Noureddine Chikouche. "An improved approach for lsb-based image steganography using AES algorithm." *2017 5th*

International Conference on Electrical Engineering-Boumerdes (ICEE-B). IEEE, 2017.

[17] Arora, Aman, et al. "Image steganography using enhanced LSB substitution technique." *2016 Fourth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. IEEE, 2016.

[18] Zhou, Xinyi, et al. "An improved method for LSB based color image steganography combined with cryptography." *2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS)*. IEEE, 2016.

[19] Shukla, Awdhesh K., et al. "A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing." *IEEE Access* 6 (2018): 51130-51139.

[20] Witten, Ian H., Radford M. Neal, and John G. Cleary. "Arithmetic coding for data compression." *Communications of the ACM* 30.6 (1987): 520-540.

[21] Dworkin, M. J., et al. "Advanced Encryption Standard (AES)(NIST FIPS- 197)." (2001).

[22]. Emad, E. L. S. H. A. Z. L. Y., et al. "A secure image steganography algorithm based on least significant bit and integer wavelet transform." *Journal of Systems Engineering and Electronics* 29.3 (2018): 639-649.

[23] Javed, Muhammad Younus, and Abid Nadeem. "Data compression through adaptive Huffman coding schemes." *2000 TENCON Proceedings. Intelligent Systems and Technologies for the New Millennium (Cat. No. 00CH37119)*. Vol. 2. IEEE, 2000.

[24] Lahitani, Alfirna Rizqi, Adhistya Erna Permanasari, and Noor Akhmad Setiawan. "Cosine similarity to determine similarity measure: Study case in online essay assessment." *2016 4th International Conference on Cyber and IT Service Management*. IEEE, 2016.