Bachelor of Science in Computer Science & Engineering

Image Steganography Using Wavelet Based Contourlet Transform and Quaternion QR Decomposition

by

Swarna Chakraborty

ID: 1504087

Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)

Chattogram-4349, Bangladesh.

April, 2021

Image Steganography Using Wavelet Based Contourlet Transform and Quaternion QR Decomposition

Submitted in partial fulfilment of the requirements for
Degree of Bachelor of Science
in Computer Science & Engineering

by

Swarna Chakraborty
ID: 1504087

Supervised by

Dr. Pranab Kumar Dhar
Professor
Department of Computer Science & Engineering

Chittagong University of Engineering & Technology (CUET)
Chattogram-4349, Bangladesh.

The thesis titled '**Image Steganography Using Wavelet Based Contourlet Transform and Quaternion QR Decomposition'** submitted by ID: 1504087, Session 2019-2020 has been accepted as satisfactory in fulfilment of the requirement for the degree of Bachelor of Science in Computer Science & Engineering to be awarded by the Chittagong University of Engineering & Technology (CUET).

Board of Examiners

Chairman

Dr. Pranab Kumar Dhar
Professor
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Member (Ex-Officio)

Dr. Asaduzzaman
Professor & Head
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Member (External)

Dr. Kaushik Deb
Professor
Department of Computer Science & Engineering
Chittagong University of Engineering & Technology (CUET)

Declaration of Originality

This is to certify that I am the sole author of this thesis and that neither any part of this thesis nor the whole of the thesis has been submitted for a degree to any other institution.

I certify that, to the best of my knowledge, my thesis does not infringe upon anyone's copyright nor violate any proprietary rights and that any ideas, techniques, quotations, or any other material from the work of other people included in my thesis, published or otherwise, are fully acknowledged in accordance with the standard referencing practices. I am also aware that if any infringement of anyone's copyright is found, whether intentional or otherwise, I may be subject to legal and disciplinary action determined by Dept. of CSE, CUET.

I hereby assign every rights in the copyright of this thesis work to Dept. of CSE, CUET, who shall be the owner of the copyright of this work and any reproduction or use in any form or by any means whatsoever is prohibited without the consent of Dept. of CSE, CUET.

swarna chakraborty

Signature of the candidate

Date: 19-04-2021

Acknowledgements

The success and final result of this thesis involved a great deal of support and assistance from many people, and I consider myself incredibly fortunate to have received it all the way through my thesis.It has been an enriching experience, professionally and personally. All that I have done is only due to such supervision and assistance.At first I would like to thank Almighty for providing me the strength to finish this work.I would like to express my deep gratitude to my honorable thesis supervisor Dr. Pranab Kumar Dhar, Professor, Department of Computer Science Engineering, Chittagong University of Engineering Technology (CUET) for his guidance, encouragement and continuous support during my thesis work.I also convey my gratitude to Professor Dr. Asaduzzaman, Head of the Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for his kind advice. I am also grateful to my external, Professor Dr. Kaushik Deb, Professor,Department of Computer Science and Engineering, Chittagong University of Engineering and Technology, for his guidance and review of my thesis work.I am also thankful for the constant encouragement, support, and guidance from all Teaching staffs of the department.Finally, I want to thank parents for their unconditional love, support, encouragement, and contribution all throughout my life and academic career in every aspect along the years.

Abstract

In recent years, data security has become a very significant concern as a result of the tremendous progress of information and communication technologies, as well as the massive rise in internet use by sending and receiving data. Researchers have therefore concentrated on developing data security systems, and experiments have been undertaken to refine old strategies and launch new ones to protect data from hackers. Digital image steganography is an effective solution in this regard. It can effectively hide secret data in an image to provide an efficient way of secret communication.This work proposes a new image steganography technique using Wavelet-based Contourlet Transform (WBCT) and Quaternion QR (QQR) Decomposition. By using WBCT this technique takes advantage of the significant texture information of the image to find the embedding position.After applying WBCT to the cover image, the coefficients are represented using quaternions and then Quaternion QR decomposition is applied. Embedding is performed on the R matrix of the decomposed image using the quantization index modulation method. Modification performed on the R component of QQR decomposition has less effect on the cover image.The simulated experimental result shows that this new steganography scheme produces good quality stego images with high PSNR, low MSE, attractive SSIM values indicating good imperceptibility. The scheme can hide 393,216 bits in the cover image indicating good capacity along with better robustness against several attacks.Security performance of proposed method is investigated using popular steganalysis schemes. Detection accuracy is found to be average that confirms the undetectability.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Recent development of information technology and easy sharing of data through communication mediums have imposed some challenges to data security. The methods that can be used to solve these challenges are classified into two types: cryptography and steganography. Cryptography provides security, but the existence of secret data in cipher can be suspected, while steganography provides security but does not reveal the existence of secret data in stego [1]. More specifically, cryptography encrypts plain text into a ciphertext based on an encryption algorithm as well as an automatic and randomized key, so only authorized persons can decipher and receive messages.On the other hand, Steganography completely hides the existence of the secret by embedding secret data concealed in a cover image in such a manner that it becomes almost impossible to intercept confidential data and hack it [2].So,steganography is more efficient way to pursue secret communication.Another data hiding technique is digital watermarking.It also hides data in cover medium but purpose of watermarking is different from steganography.Aim of steganography is secret communication while aim of watermarking is copyright protection,authentication etc.Figure 1.1 shows overview of security systems.

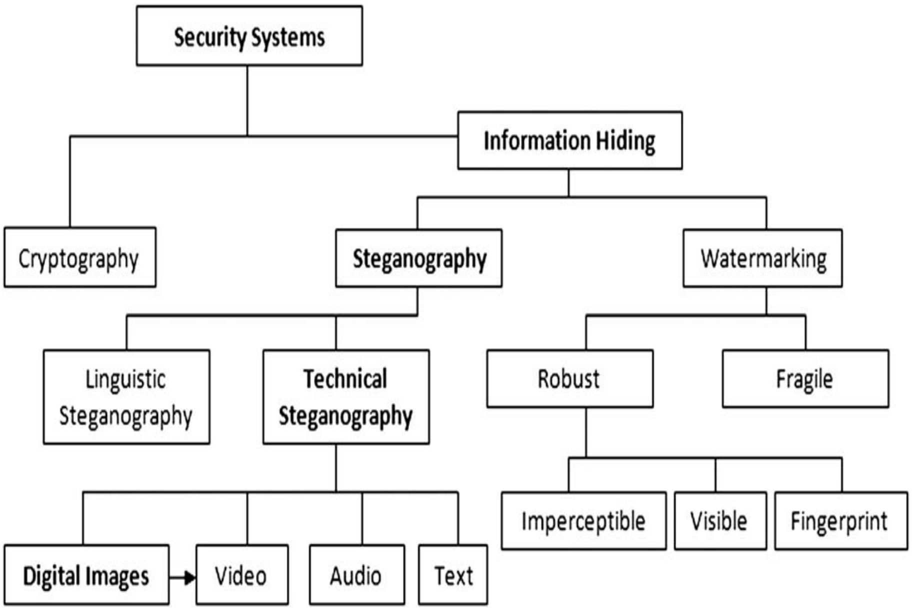


Figure 1.1: Taxonomy of security systems[3]

1.1.1 Image Steganography

Steganography is the art and science of writing secret data into the cover media in such a way that no one except the intended recipient knows the existence of the data[4].Image steganography uses image as its cover media.Data to be hidden can be either text or image.Currently,image is the most used multimedia.So it is more suitable medium for effective data hiding.Image steganography has two major parts.Embedding scheme and extraction scheme.The image where data is to be hidden is called cover image.After embedding the data stego image is generated.It is important to embed data such a way that stego image is visually similar to cover image.Again The hidden data should be extracted perfectly using the extraction scheme in the receiver end.

1.1.2 Properties of Steganography

There are some fundamental properties that should be maintained at an optimum level in a good steganographic system.

Imperceptibility: .A steganography system is called imperceptible when the cover image and the stego image are perceptually indistinguishable.Imperceptibility is determined using peak signal to noise ratio(PSNR) value,Structural Similarity

Index Matrix(SSIM) etc.The higher the PSNR or SSIMvalue,the higher the stego image quality is.

Capacity: Capacity refers to the number of bits can be embedded into a pixel of cover image.The aim of a good steganographic system is to send maximum information possible using minimum cover media.

Security: Security refers to the undetectability of hidden data.Security is the primary concern in order to avoid data access by unauthorized persons or computer while transmitting through an open channel.

Robustness: Robustness implies the amount of modification the stego medium can tolerate before an attack that can destroy hidden information[5].The attacks can be compression,format conversion,scaing,cropping,rotation etc.

1.1.3 Steganography Techniques

Over the years many steganographic algorithm has been developed.These methods use different types of techniques to embed and extract data.These techniques can be broadly divided into two domains,spatial domain and frequency domain.

1.1.3.1 Spatial Domain Techniques

In spatial domain methods, the processing is applied on the image pixel values directly. The advantage of these methods is simplicity.They provide good concealment while allowing for a large amount of embedded data and easy investigation.As a result , steganographic applications make extensive use of these techniques. The disadvantage is low ability to bear signal processing operations [6].They are often easy to detect.It includes :

- Least significant bit(LSB)
- Bit-Plane Complexity Segmentation(BPCS)
- Pixel value differencing (PVD)
- Histogram shifting method
- Edge based method

etc. methods

1.1.3.2 Transform Domain Techniques

In transform domain methods,the cover image is first transformed into different domain and then the transformed coefficients are used to hide data.The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Strong steganographic systems mostly operate within the transform domain.The advantage of transform domain methods is the high ability to face signal processing operations.However,methods of this type are computationally complex .They also offer less hiding capacity.Common transform domain techniques include:

- Discrete Fourier transformation technique (DFT).
- Discrete cosine transformation technique (DCT).
- Discrete Wavelet transformation technique (DWT).

etc.

1.2 Framework/Design Overview

The basic idea behind a digital image steganographic process is to conceal secret or private information inside an image in an undetectable manner.In image steganography the image where data is to be hidden is called cover image.The image generated after data hiding is called stego image. The secret data can be encrypted or scrambled using a key before embedding.After embedding visually undistorted stego image should be generated. In the receiver side,inverse approach is used to extract secret information from stego image.One or more key can be needed to extract the information depending on the embedding scheme.A block diagram is given in figure 1.2 to depict the representation of a generic steganographic system.

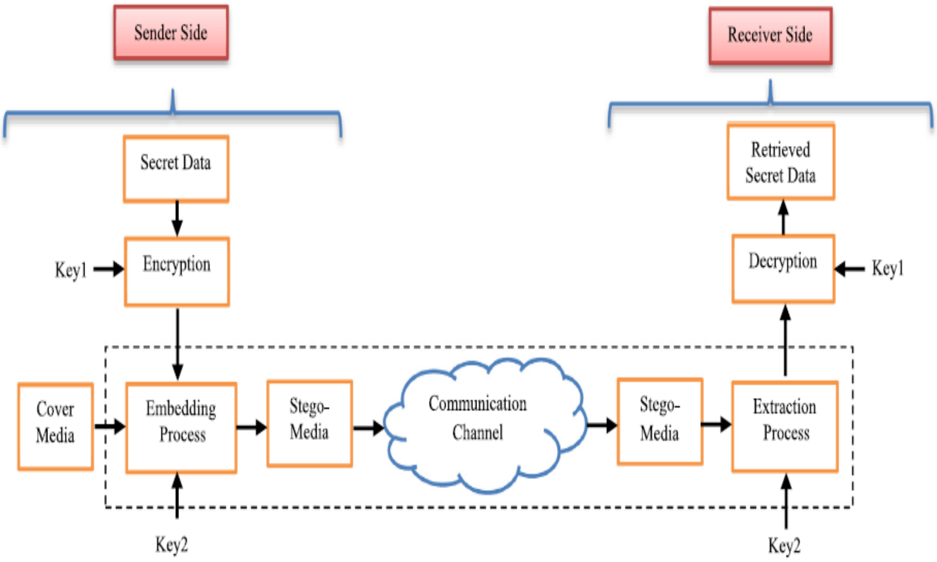


Figure 1.2: Block diagram of a Steganographic system[7]

1.3 Difficulties

The key issues in designing an image steganography scheme are capacity, imperceptibility,security.Also robustness is in some applications.Balancing these features in a scheme is a challenging task. There is a fundamental tradeoff between these properties in a steganography system.If one feature is focused more then another feature must be compromised.Maintaining optimum level for these properties is a difficult task.This trade of can be represented using a triangle shown in figure Maintaining optimum level for the properties is a difficult task.

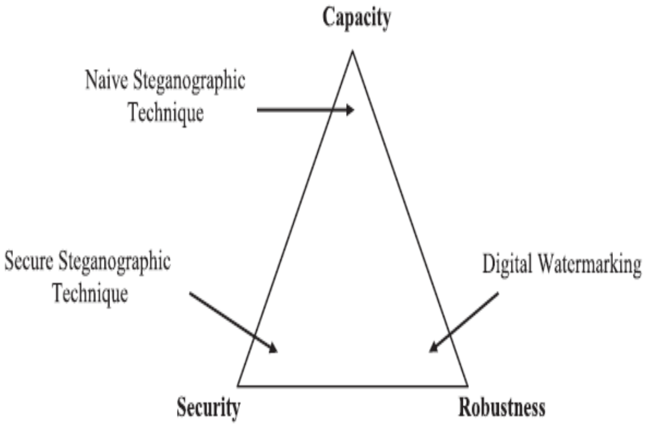

Capacity
Naive Steganographic Technique
Secure Steganographic Technique
Digital Watermarking
Security
Robustness

Figure 1.3: Trade-off between the properties of the steganography.[7]

Again,many of the steganography schemes are developed using grayscale images.But nowadays color image has more application and developing a scheme for color image is a challenging task.Most of the existing color image steganography schemes were designed to mark the image luminance component only,which ignores the correlation between coefficients.As a result,they are sensitive to color attacks.

With the advancement of machine learning and other technologies many universal steganalysis tools have been developed that can easily detect the existence of payload in an image.Developing a scheme to deceive those steganalyzers is quite difficult task.

1.4 Applications

Secure and stealth communication is widely used in almost all fields. Steganography is applicable to, but not limited to, the following areas.

- Medical field to hide crucial private information in the medical data itself.
- Military and defence system to ensure safe communication and prevent information leak.
- Investigation and intelligence agencies.
- Access control system for digital content distribution

1.5 Motivation

Advancement of internet,digitalization of information and increasing use of social media platforms have increased information sharing exponentially.Thus importance of information security has also increased.Nowadays hacking,data breaching , information stealth and leaking has become very common occurence.Steganography efficiently handles the problem of data security.Though there are many scheme developed in this regard.But there is still room for development towards making these techniques more secure and efficient in terms of performance measures.Again,image is the most used multimedia.This motivated us to design an efficient image steganography technique.

Many of the existing techniques use grayscale image as cover media.But in modern days color image is more common.The existing color image steganography techniques they embed information seperately in each color channel that makes them more vulnerable.Again,many of the schemes use spatial domain technique that provides less security and robustness and can be easily detected.To address these issues we developed a new color image steganography method using quaternion algebra and transform domain techniques.

1.6 Contribution of the thesis

The main goal of the thesis is to develop an efficient method for image steganography that can overcome the limitations of existing methods.The main contribution of this thesis are:

1. Development of an efficient image steganography scheme using Wavelet-Based Contourlet Transform(WBCT) and Quaternion QR(QQR) decomposition.
2. Development of a system that maintains a good trade off between inperceptibility and capacity.
3. Using a new method to embed secret data and evaluate its performance using different measures.

1.7 Thesis Organization

The rest of the thesis report is organized as follows:

- Chapter 2 gives a brief summary of the previous research works in the field of image steganography.
- Chapter 3 describes the proposed framework along with WBCT and QQR used in this method.It contains both the embedding and extraction scheme.
- Chapter 4 contains the simulation results,impact analysis and performance analysis using standard measures

- Finally chapter 5 contains conclusion and some future recommendations as well.

1.8 Conclusion

In this chapter overview of information hiding and image steganography has been provided.Along with the difficulties,the general framework of image steganography is described.Also,motivation and contribution of the work is also stated in this chapter.In the next chapter existing research work and their limitations will be described.

Chapter 2

Literature Review

2.1 Introduction

Color images are used widely in many social media platform like Facebook, WhatsApp,Instagram etc.These images are transferred from one computer or network or server to another using open networks such as the internet, wireless network etc., wherein they can undergo many manipulations and attacks . So a strong communication technique is required for secure transmission of color images over any open access medium.Image steganography is a successful tool to develop such a safe communication medium.

Researches have been done using different techniques,approaches,algorithms throughout the last two decades to overcome the existing limitations of steganographic systems.Some focus on imperceptibility while some focus on high capacity and so on.In this chapter these researches will be discussed along with their contribution and limitations.

2.2 Related Literature Review

Many methods have been proposed so far for image steganography on both spatial domain and transform domain. The most commonly used algorithm is the LSB Replacement algorithm in which the embedding of the secret message is done only to the least significant bits of the cover image in order to minimize distortion effect. In[8] an LSB based method has been proposed.The embedding of spread out secret data over the cover image was done based on random LSB substitution. It used some cryptography to ensure security but suffered from low payload capacity and pure robustness against compression and geometric attacks.Rajendran[9] proposed an LSB technique based steganography where logistic chaotic map is generated is used to generate a sequence and the secret data embedding is based on this generated sequence.The use of chaotic map increased security and simplicity but it also suffered from low payload capacity and robustness.

In[10] author proposed a new method for modifying the triway PVD by determining the best value of each pixel pair whose difference provides the most details without ignoring any.Though it provides high payload capacity but it suffers from poor visual quality and security. A bit plane slicing and histogram shifting based method has been proposed in[11] where the pixel intensity values are sliced into two based on the bit plane values and histogram shifting based embedding is applied over the histogram bins separately.It has high capacity with good imperceptibility.But it is vulnerable to intruder attacks.

Transform domain image steganography was evolved with embedding in Discrete Cosine Transform (DCT) domain; JPEG being the most popular file format on the Internet. A global adaptive region based embedding in the DCT domain was put forward by Rabie et al.[12].Imperceptibility results were obtained using a variety of block sizes and capacities.In[13], the author defines a universal distortion function called universal wavelet relative distortion (UNIWARD) for steganography in the frequency space. The distortion is considered as the form of a sum of relative changes between the cover and embedded images that is represented in the transform domain and, in [14], it is computed in the wavelet domain as a sum of relative changes of coefficients in a directional filter bank decomposition of the cover image. In [15] author proposed an approach using Integer Wavelet Transform(IWT) along with Singular Value Decomposition.This approach provides robustness against various attacks like addition of noise,gaussian filtering,cropping,rotating etc.In [16] a new cover selection technique is proposed to achieve secure stego image,high capacity by redundancy in RDWT.

The above mentioned wavelets provide a very sparse representation for piecewise smooth signals due to which wavelets are used in many signal processing applications. However, the separable wavelet transform does not work efficiently in higher dimensions. Wavelets are good at catching edge points but do not prove optimum for smoothness along contours. It demands the need for more powerful representation rich in directions.Wavelet transform suffers from the drawback of sub-band mixing. If we alter one coefficient in diagonal sub-band it will have an effect on the value of relevant coefficients in other directions too.To overcome this drawback, Contourlet Transform (CT) is the best solution as it allows for image decomposition in separate directions. The Contourlet transform is a directional multiresolution expansion which can represent the images that contain contours efficiently.In [17] a new image steganography method has been proposed that uses contourlet transform along with three common matrix decomposition techniques to compare their performance.The contourlet transform, on the other hand, has a redundancy factor of 4/3 due to the redundancy of the Laplacian pyramid, and hence several attempts have been made to implement non-redundant image transforms.Eslami et al. proposed a new non-redundant image transform [18], the Wavelet-Based Contourlet Transform (WBCT),with a construction similar to the contourlet transform. The proposed WBCT achieves both radial and angular decomposition to an arbitrary extent and obeys the anisotropy scaling law.

Though transform domain based techniques aim at achieving good robustness,color images are still vulnerable to attacks.As they embed data separately in each channel and ignore the correlation between color channels,they show poor performance against geometric attacks and become easily detectable.To overcome this problem quaternion representations have been used in a few cases,mostly in watermarking.In [19] author proposed a watermarking scheme using quaternion qr decomposition to process the image holisticaly and use the advantages of QR decomposition.Quaternion representation has also been used in steganography system[20] where both cover image and secret data is represented in quaternion form.But all of the methods provide low payload capacity.

To address the above mentioned limitations of the existing systems,we propose a new image steganography scheme using wavelet based contourlet transform and Quaternion QR decomposition.

2.3 Conclusion

In this chapter a detailed literature review of existing methods have been described.Both spatial domain and transform domain techniques are discussed here.WBCT and Quaternion based systems along with the justification of using these methods are also discussed.

2.3.1 Implementation Challenges

Maintaining a good capacity is a key property of a steganographic system.But as quaternion algebra represents image in a holistic manner it became difficult to ensure good capacity.But we overcome this problem by using a different type of quaternion representation of image as described in [21].

Chapter 3

Methodology

3.1 Introduction

In the previous chapter we have seen that many image steganography methods have been proposed.In many cases,they does not provide satisfactory result.In this thesis we propose a image steganography scheme using Wavelet-Based Contourlet Transform and Quaternion QR Decomposition.To understand the embedding and extraction process some background information like the transform,decomposition,chaotic map and other relevent information is necessary.

3.1.1 Gauss iterated Map

Gauss iterated map or Gauss map is one dimensional non chaotic map that can be used in image encryption. Chaotic maps are complex in nature, having properties of ergodicity, sensitivity to initial and control parameters[22].They can generate random sequence and this sequence can be used to generate key for encryption. Gauss iterative map is given by the following function:

$$x_{n+1} = exp(-\alpha x_n^2) + \beta \tag{3.1}$$

Here, α and β are real parameters. Gauss iterated map shows best result when the value of α has some positive value lies between +1 to +6 and β value lies between -1 to +1[23].

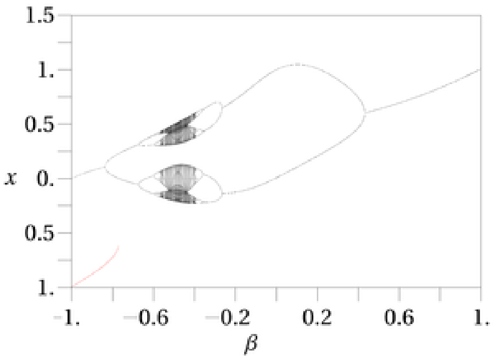


Figure 3.1: Gaussian map withα=4.90

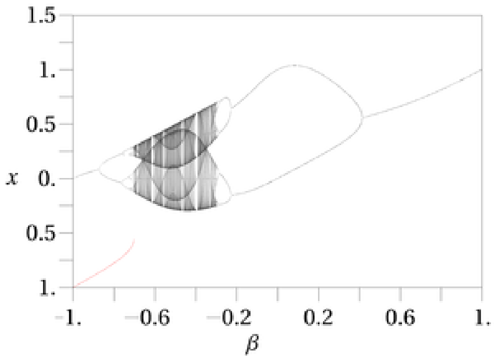


Figure 3.2: Gaussian map with α=6.20

Gauss iterated map is also called mouse map because its bifurcation diagram resembles a mouse.

3.1.2 Wavelet-Based Contourlet Transform

To fulfill the demand of more powerful representation rich in directions Do and Vetterli[24] proposed contourlet transform which can capture nearly arbitrarily directional information of the natural images.But,Because contourlet transform uses laplacian pyramid it is a redundant image transform.The Wavelet-Based Contourlet Transform(WBCT) developed by Eslami and Radha[18] , with a construction similar to the contourlet is a new non-redundant image transform.It also has two stages.But it uses wavelet transform in first stage instead of laplacian pyramid.The second stage is a directional fiter bank(DFB).At each level,the image is decomposed into one LF subband and three HF(LH,HL and HH) subband by wavelet transform of first stage.Then each HF subband is decomposed into number of diretional subband by the DFB of second stage.It begins at the finest level of the wavelet transform with the desired maximum number of directions, and decreases the number of directions at each subsequent dyadic scale as progress through the coarser stages.

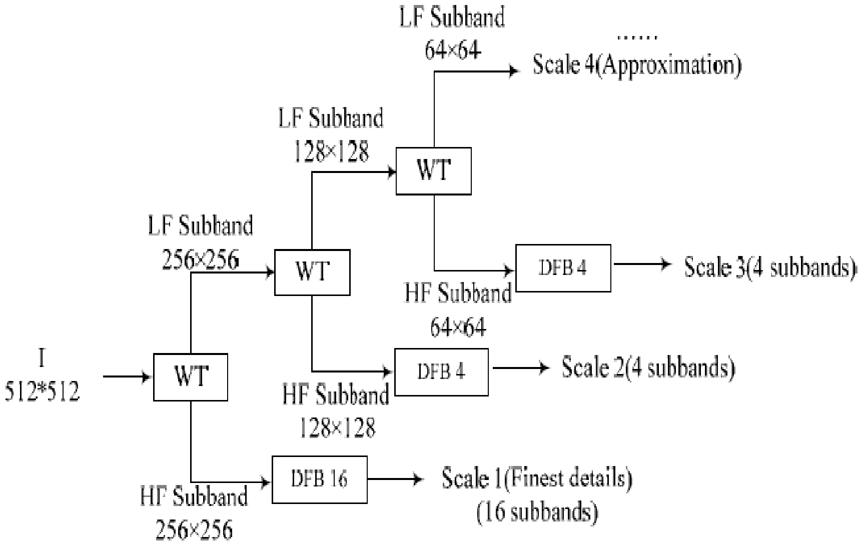


Figure 3.3: Flowchart of WBCT for a 512*512 image[25]

WBCT can capture image structure features more effectively than Discrete Wavelet Transform(DWT) and is better suited to identifying subbands in the cover image where payload can be effectively inserted. The secret image should be inserted into the low frequency subbands in our scheme to ensure the visual quality and robustness of the stego image.

3.1.3 Quaternion Representation of color images

Quaternion is a hypercomplex number first introduced by hamilton at 1843.It can be represented as a four dimensional complex number with one real part and three imaginary part as follows:

$$q = w + xi + yj + zk \tag{3.2}$$

its modulus is given by:

$|q| = sqrt(w^2 + x^2 + y^2 + z^2)$

Here,w,x,y,z are real numbers and x,y,z are imaginary operators that have the following properties:

$i^2 = j^2 = k^2 = ijk = -1$

$ij = k.jk = i.ki = j$

$ji = -k.kj = i.ik = -j$

To represent an image using quaternion we split the image in three color channels and represent each 1D image as a vector image,where each of the imaginary components of the quaternion contains l/sqrt(3) times the pixel value.We can use this representation to encode each channel separately in quaternion and increase capacity compared to other quaternion based methods.

3.1.4 Quaternion QR Decomposition

After performing WBCT on the host image we perform Quaternion QR decomposition on the obtained wbct coefficients.It was first developed by Bunse-Gerstner et al.[26].

Let $A \in H$ where H is a pure quaternion matrix.There is a factorization A= QR where Q is a unitary matrix and R is an upper triangular matrix.Here,$Q \in H$ and $R \in H$.

Let,

$$A_0 := A$$

$$Factor A_k = Q_k R_k$$

$$Set A_{k+1} := RkQk$$

$$A_{k+1} = Q_k^H A_k Qk \tag{3.3}$$

Now,let P be the permutation matrix.So, we can write:

$$PA_kP^H = (PQ_kP^H)(PR_kP^H)$$

$$PA_{k+1}P^H = (PR_kP^H)(PQ_kP^H) \tag{3.4}$$

Here,$PQ_kP^H and (PR_kP^H)$ are unitary matrix and triangular matrix, respectively.

To make the inverse matrix still pure quaternion,we embed data in the real part of the upper triangular matrix.

3.2 Diagram/Overview of Framework

The proposed steganography method consists of two major parts such as data embedding algorithm and data extraction algorithm.I also At first a color image is selected as cover image.It is then divided into three channels. Then a grayscale encrypted image is embedded into the cover image after performing Wavelet-Based Contourlet Transform and Quaternion QR decomposition.

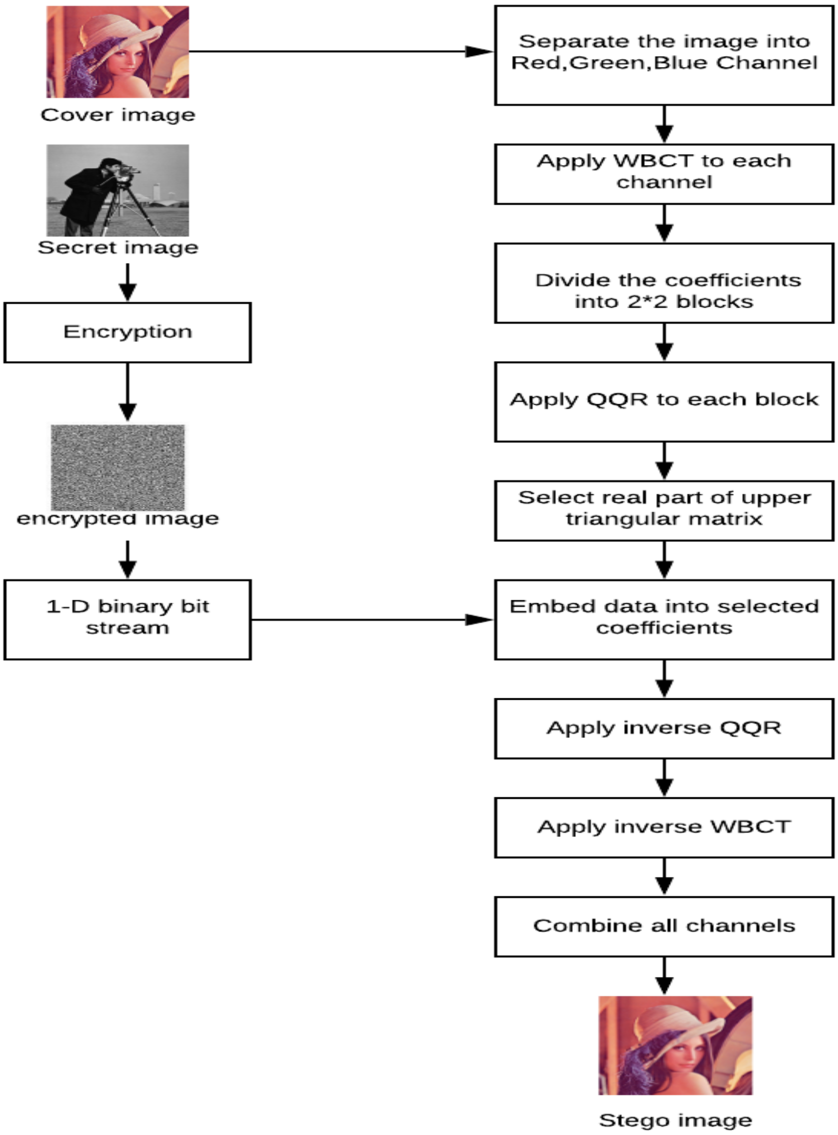

Cover image
Secret image
Encryption
encrypted image
1-D binary bit stream
Separate the image into Red,Green,Blue Channel
Apply WBCT to each channel
Divide the coefficients into 2*2 blocks
Apply QQR to each block
Select real part of upper triangular matrix
Embed data into selected coefficients
Apply inverse QQR
Apply inverse WBCT
Combine all channels
Stego image

Figure 3.4: Embedding process of the proposed method

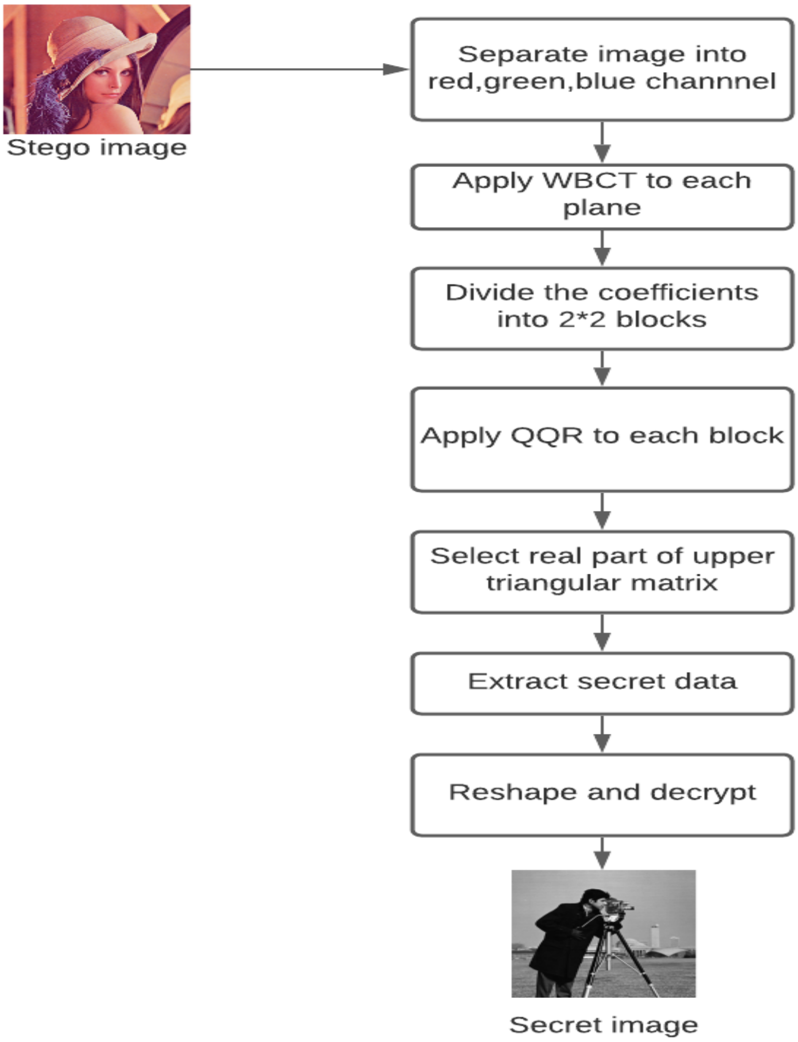

Stego image
Separate image into red,green,blue channnel
Apply WBCT to each plane
Divide the coefficients into 2*2 blocks
Apply QQR to each block
Select real part of upper triangular matrix
Extract secret data
Reshape and decrypt
Secret image

Figure 3.5: Extraction process of the proposed method

In the extraction process,reverse process is applied to extract the secret image. The stego image is divided into three color planes and WBCT,QQR is applied to each channel.Secret image is extracted from real part of upper triangular matrix.

3.3 Detailed Explanation

In this section detailed explanation of the encryption,embedding and extraction is provided.

3.3.1 Encryption and Decryption Process

The secret image is encrypted using gauss iterated map for enhanced security.The encryption and decryption process is given below:

3.3.1.1 Encryption Process

1. First take a M*M image and generate a random sequence X of size M*M using the equation 3.1.
2. Now we use the following quantization formula to generate another sequence.

   $$S_i = 0; if 0 < X(n) <= T$$

   $$S_i = 1; if T < X(n) <= 1$$

   Here,Value of T can vary with the value of the parameters α and $beta$
3. Now,XOR S(i) with each bit of the M*M image.This will give us the encrypted image.

3.3.1.2 Decryption Process

1. .Take the encrypted image of size M*M and generate the random sequence X of size M*M using Gauss iterated map.
2. .Generate sequence S using the method mentioned in encryption process.
3. Apply XOR operation to the encrypted image bit and S.

3.3.2 Embedding Process

The embedding process shown in figure 3.2 can be described as follows.

1. Read the rgb cover image and grayscale secret image.
2. encrypt the image using gauss iterative map as described in the encryption process.
3. Convert the encrypted image into binary bit stream.

4. Divide the cover image into Red,Green and Blue planes.
5. Apply Wavelet based Contourlet transform to each plane.
6. Divide the coefficients of each plane into 2*2 blocks.
7. Represent each coefficient with a quaternion.
8. Apply Quaternion QR decomposition to each block.
9. Real part of the first row of R matrix is used to embed the secret binary bit stream using the following equation:

   Let q be a positive integer. w is the coefficient where we will embed a binary bit of secret data and d is the binary bit that we want to embed.
   Now, $r = wmodq$

   when d=1:

   if $r <= q/2$:

   $s = q/2 - r$

   $w = w + s + 0.3q$

   when **d=0:**

   if $r > q/2$:

   $s = q/2 - r$

   $w = w - s - 0.3q$

10. Apply inverse quaternion qr decomposition to each block.
11. After combining the blocks apply inverse Wavelet Based Contourlet Transform to get the stego image.

3.3.3 Extraction Process

1. Divide the stego image into Red,Green,Blue planes.
2. Apply Wavelet based Contourlet Transform to each plane.

3. Divide the coefficients of each plane into 2*2 blocks.

4. Represent each coefficients with quaternion in the above mentioned manner.

5. Apply Quaternion QR decomposition to each blocks.

6. Real part of the first row of R matrix is used to extract the secret binary bit stream using the following equation: Let q be a positive integer.w' is the coefficient from which we want to extract secret data and d' is the binary bit that we want to extract.
   Now, $r' = w' mod q$

   if $r' < q/2$

   $d' = 0$

   else

   $d' = 1$

7. Reshape the binary data stream and decrypt it as described in the decryption process to obtain the secret image.

3.4 Conclusion

In this chapter,At first the related background information like Gauss iterated map, WBCT and QQR is discussed.Their description and why we used them in our project is also discussed.Then we have discussed the whole embedding and extracting process in detail.In the next chapter we will discuss the results and evaluate the framework using some common performance measures.

Chapter 4

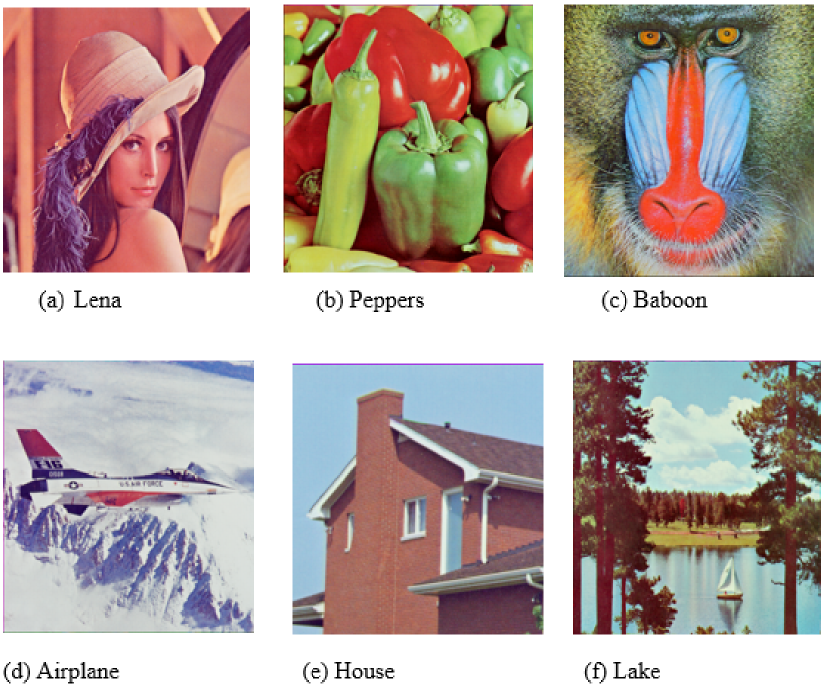
Results and Discussions

4.1 Introduction

In the previous chapter, a detailed explanation of the proposed framework for image steganography was given.A good steganography scheme should have a good embedding capacity, better imperceptibility, and high security. Increased embedding capability can result in visible distortions and a reduction in visual quality. While preserving security, a balance must be maintained between embedding capacity and imperceptibility.

4.2 Dataset Description

For performance evaluation we used several well known 24 bit color images of 512*512 size as cover image and one popular grayscale image as secret image from the popular USC-SIPI databse.



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

(d) Airplane (e) House (f) Lake

Figure 4.1: Cover Images

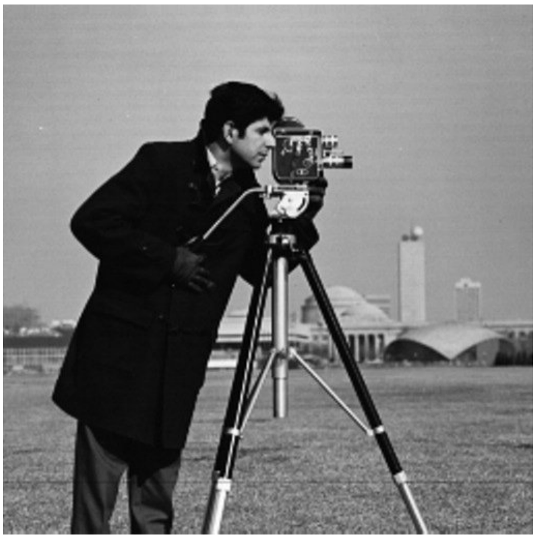


Figure 4.2: Secret Image

4.3 Impact Analysis

The impact of image steganography is huge.It can be used in both positive and negative way.Its impacts are discussed below

4.3.1 Social and Environmental Impact

Data digitalization has greatly increased the capacity for regenerating and disseminating information, due to the growth of wireless networks, interconnected multimedia systems, and electronic digital cameras. Steganography has emerged as a reliable data transmission technique in the digital world, and it is attracting a wide range of industrial applications.Image being the most used data has become most popular cover media to transfer controversial information through an insecure channel.Not only common people but defence system and investigation agencies can also use this type of steganographic system for secure communication.

4.3.2 Ethical Impact

In steganography ethical impact is a huge issue.It is designed to be used in ethical purpose but sadly,it can also be used in unethical purpose.While defence systems,investigation agencies can use it for transmitting controversial or secret information for the sake of tracking criminals or terrorists ,hackers can use it for hacking and terrorists or criminals can use it for planning terrorist attacks and criminal activities .

4.4 Performance metrics

This framework was implemented in MATLAB R2017a environment with Intel Core i5 processor and 8GB RAM. In the evaluation of performance,it is important to outline the definitions of metrics so that other can verify it.

4.4.1 Peak Signal to Noise Ratio(PSNR)

Changes in the cover image pixel values can occur as the cover image is altered to embed the hidden data. The adjustments must be investigated because they have a direct impact on the output stego image quality. image's PSNR is a well-known and highly regarded metric for evaluating the quality of a stego-image by comparing the mean squared error value between the cover and the stego image.PSNR can be represented as-

$$PSNR = 10\log 10(\frac{255^2}{MSE})$$

Where,

$$MSE = \frac{1}{M}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(A - A')$$

4.4.2 Structural Similarity Index Matrix(SSIM)

SSIM is a comparison metric to check the similarity between to images.Here,one of the image is compared as perfect quality and the other is compared with the former.It is calculated as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2}{(\mu_x^2\mu_y^2 + c1)(\sigma_x^2\sigma_y^2 + c2)}$$

here,μ is the mean intensity and σ is the standard deviation.

4.4.3 Capacity

Capacity of a scheme is the amount of payload concealed in the cover image.It is generally represented as Bits per pixel(BPP),where

$$BPP = \frac{Number\ \ of\ \ secret\ \ bits\ \ embedded}{Total\ \ pixels\ \ in\ \ the\ \ cover\ \ image}$$

4.4.4 Normalized Coefficients(NC)

NC compares the original secret image to the extracted secret image to see how close they are. If the NC value is equal to 1, any steganography technique is considered to perform well.It is given by the following equation:

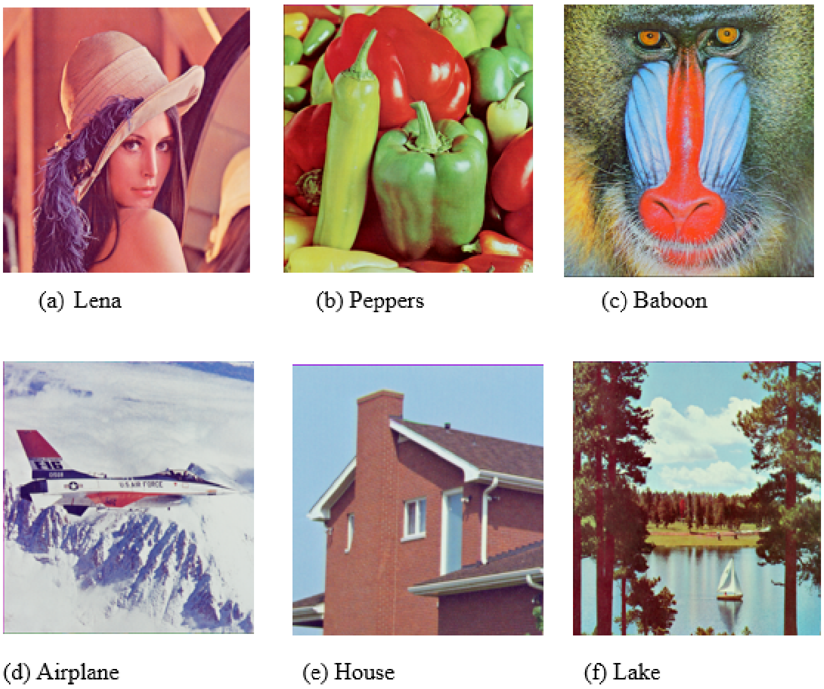
$$NC = \frac{\sum_{i=1}^{N}(S_i' - \mu_{s'})(S_i - \mu_s)}{\sqrt{(\sum_{i=1}^{N}(S_i' - \mu_{s'})^2)(\sum_{i=1}^{N}(S_i - \mu_s)^2)}}$$

Here,S’ is the ith pixel intensity of extracted image and S is ith pixel intensity of secret image.$\mu_{s'}$ and μ_s are the mean pixel values of extracted image and secret image respectively.N is image pixel count.

4.5 Evaluation of Performance

4.5.1 Imperceptibility Analysis

Imperceptibility refers to the measurement of visual quality distortion of stego images after embedding data.It can be done subjectively and statistically.Stego images after embedding secret data are shown in figure 4.3 .It is evident form the figures that all stego images are of good visual quality and it is difficult to suspect about the presence of hidden information in them.So,we can conclude that it is subjectively imperceptible.To statistically Measure the visual quality of stego image PSNR and SSIM values are calculated.Table 4.1 shows the PSNR values and table 4.2 shows the SSIM values of the proposed scheme with respect to different capacities.



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

(d) Airplane (e) House (f) Lake

Figure 4.3: Stego images generated after embedding data

Capacity	PSNR(Lena)	PSNR(Peppers)	PSNR(Baboon)	PSNR(Airplane)	PSNR(House)	PSNR(Lake)
0.03125	61.8989	62.0110	62.0635	61.9144	61.8747	61.8303
0.125	55.8507	55.9227	55.8564	55.9464	55.8831	55.8989
0.3125	51.8801	51.8476	51.9246	51.9008	51.8893	51.9310
0.5	50.7930	50.7092	50.7444	50.7789	49.7017	49.7716
0.75	48.0072	47.9485	47.9910	47.9881	47.7782	48.0008
1	46.7042	46.6559	46.6458	46.6650	46.3817	46.6656
1.25	45.7301	45.6818	45.6777	45.6937	45.1423	43.1217
1.5	44.9739	44.9375	44.9372	44.9409	43.1217	42.9524

Table 4.1: PSNR values of the stego images using proposed method

Capacity	SSIM(Lena)	SSIM(Peppers)	SSIM(Baboon)	SSIM(Airplane)	SSIM(House)	SSIM(Lake)
0.03125	1	1	1	0.9999	1	0.9999
0.125	1	0.9999	0.9999	0.9995	0.9998	0.9998
0.3125	0.9998	0.9998	0.9998	0.9992	0.9995	0.9994
0.5	0.9997	0.9996	0.9995	0.9987	0.9991	0.9992
0.75	0.9995	0.9995	0.9993	0.9926	0.9986	0.9988
1	0.9994	0.9993	0.9990	0.9876	0.9982	0.9985
1.25	0.9992	0.9992	0.9988	0.9812	0.9974	0.9983
1.5	0.9991	0.9991	0.9986	0.9775	0.9968	0.9980

Table 4.2: SSIM values of the stego images using proposed method

If a stego image has a PSNR value greater than 40db then it is considered as good quality. We can see from table 4.1 and table 4.2 that our method has high PSNR and SSIM value even when capacity increases.PSNR value of our method ranges from 62.0110 db to 42.9634 db.SSIM values ranges from 1 to 0.9775 db.It benefits from the use of WBCT that gives more accurate representation of image edges and contours.Morever,we use QQR decomposition and use first row values of the upper triangular matrix that have larger absolute coefficients.So,modifying these coefficients results in less distortion of visual image quality.

In table 4.3 we can see comparison of imperceptibility with several other recent methods.We can see that our method has higher capacity than the listed method with higher psnr value.[27]uses discrete cosine transform and coupled chaotic map(ccm) as embedding approach.First,It generates random embedding locations using ccm.Then it replaces the dct coefficients of cover image with ccm values.Due to large difference between dct coefficients and ccm values the method results in relatively low imperceptibility.[28] uses dct and fuzzy inference system and the best target host blocks are intelligently determined using the degree defined in the fuzzy system.But it has comparatively low capacity as stated in the table. Ghosh also developed a blind color image steganography technique using dct.All of the mentioned dct based techniques has comparatively low imperceptibility as they embedding in low frequency dct coefficients results in high distortion in stego images.

Methods	Lena		Pepper		Baboon		Airplane	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
Kaur[27]	212890	32.9906	212890	33.0408	212890	31.1982	212890	32.7383
Nazari[28]	63752	49.6482	74672	45.3788	50856	41.6475	179124	41.5883
Ghosh[29]	98304	39.6061	98304	39.3342	98304	37.7455	98304	39.6757
Miri[30]	393216	36.7379	393216	39.9843	393216	41.2946	393216	36.9905
Proposed	393216	44.9086	393216	44.8866	393216	44.8665	393216	44.8601

Table 4.3: Comparison of proposed scheme with other schemes in terms of payload and PSNR

In table 4.4 and 4.5 we can see the comparison of how psnr and ssim values changes with respect to capacity.To calculate these values,we have used a random binary sequence as secret data.By comparison we can see that [30] performs well when capacity is low.But as the capacity increases its PSNR values fall abruptly.Thats beacuse it uses Integer Wavelet Transform (IWT) and performs embedding using LSB approach.First,It embeds data in the HH coefficients.In HH subband it performs well.But as capacity increases it embeds in LH,HL and LL subbands respectively.Embedding in other subbands does not perform well as compared to HH.In LL sub band it results very poorly.[27] replaces the dct coefficients with chaotic values which also results in comparatively less PSNR values and poor SSIM values.On the other hand our method uses wbct and embeds first in low frequency coefficients and then gradually embeds in higher frequency sub-bands.Though in wbct also higher frequency sub-bands result in greater imperceptibility but it low frequency sub-bands does not result in very low imperceptibility like dct and iwt.

Image	Capacity(bits)	PSNR[proposed]	PSNR[[27]]	PSNR[[30]]
Lena	23654	57.3512	42.9263	64.1844
	47309	55.8504	39.6778	60.4665
	70963	52.4845	37.8528	57.8766
	118272	50.2484	35.4703	49.9075
	141926	49.4215	34.6759	46.7656
	165581	48.7285	33.8777	41.7771
	212890	47.6221	32.9906	41.6222
Peppers	23654	57.3602	44.6924	63.9680
	47309	55.8675	41.6404	61.0120
	70963	52.4459	39.1768	59.1898
	118272	50.1871	36.6601	56.0206
	141926	49.3665	35.7984	53.4311
	165581	48.6844	34.9728	51.8272
	212890	47.5878	33.0408	45.8348
Baboon	23654	57.3166	39.1188	62.4237
	47309	55.8845	36.2419	60.8201
	70963	52.5381	34.4821	58.9590
	118272	50.2436	32.8325	55.7682
	141926	49.4022	32.2774	53.2382
	165581	48.6886	31.8182	51.6712
	212890	47.5851	31.1982	45.6388
Airplane	23654	57.2560	42.5824	64.3221
	47309	55.8710	39.3660	60.1216
	70963	52.4735	37.4682	56.4500
	118272	50.2495	35.2308	47.4186
	141926	49.4240	34.3921	41.8435
	165581	48.7266	33.6544	41.6955
	212890	47.5958	32.7383	40.5512

Table 4.4: Comparison of Capacity vs PSNR with other methods

Image	Capacity(bits)	SSIM[proposed]	SSIM[[27]]	SSIM[[30]]
Lena	23654	1	0.9686	1
	47309	0.9999	0.9368	1
	70963	0.9999	0.9091	1
	118272	0.9997	0.8574	0.9997
	141926	0.9997	0.8343	0.9991
	165581	0.9997	0.8078	0.9980
	212890	0.9995	0.7687	0.9979
Peppers	23654	0.9999	0.9760	1
	47309	0.9999	0.9549	1
	70963	0.9998	0.9287	1
	118272	0.9997	0.8865	0.9999
	141926	0.9996	0.8686	0.9998
	165581	0.9996	0.8486	0.9998
	212890	0.9995	0.7647	0.9992
Baboon	23654	0.9999	0.9623	1
	47309	0.9999	0.9303	1
	70963	0.9998	0.8974	0.9999
	118272	0.9996	0.8469	0.9999
	141926	0.9995	0.8236	0.9998
	165581	0.9994	0.8006	0.9996
	212890	0.9992	0.7574	0.9985
Airplane	23654	0.9995	0.9760	0.9994
	47309	0.9994	0.9549	0.9982
	70963	0.9992	0.9287	0.9952
	118272	0.9988	0.8865	0.9669
	141926	0.9952	0.8686	0.9107
	165581	0.9938	0.8486	0.9081
	212890	0.9880	0.7647	0.9060

Table 4.5: Comparison of Capacity vs SSIM with other methods

Figure 4.4 shows the graph between embedding capacity and PSNR of proposed method,[27] and [30] for lena image.It is evident from the graph that our method outperforms the other two methods in terms of handling the trade off between imperceptibility and capacity.Though,[30] performs well when capacity is low,it performs poorly when capacity increases.So,it can not maintain the balance between capacity and psnr efficiently.On the other hand,[27] performs low from the beginning and hence does not maintain the trade-off efficiently either.So,our mmethod outperforms these two methods in terms of maintaining trade-off between psnr and capacity which is a key feature of an efficient steganography system.

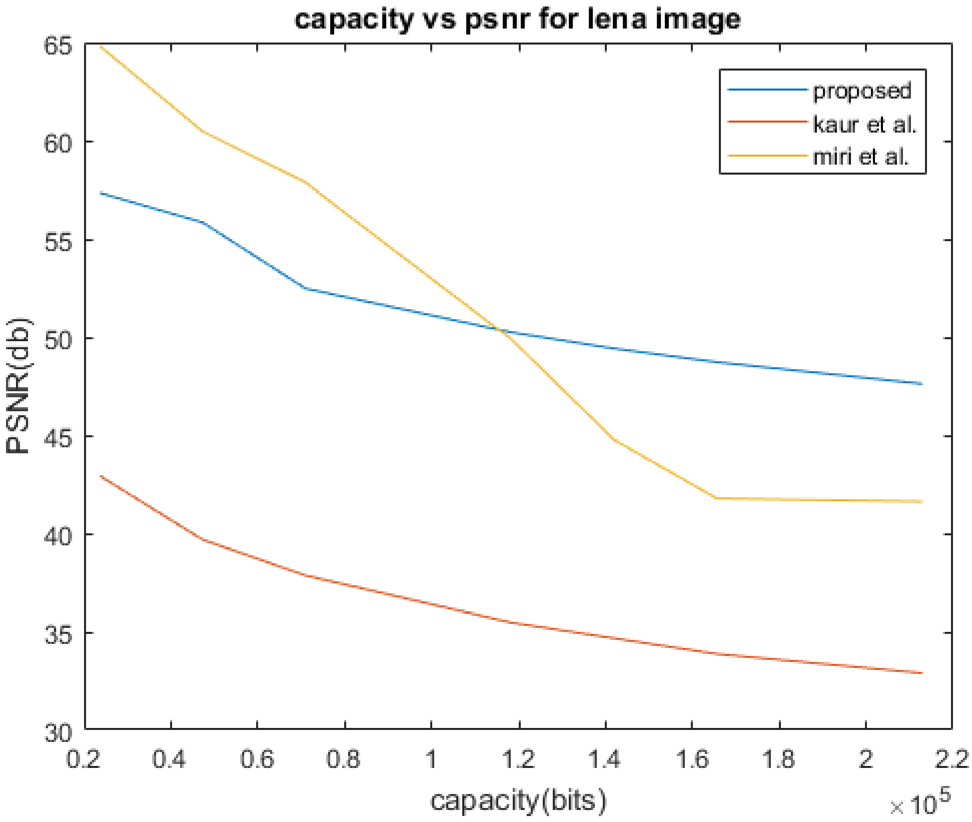


Figure 4.4: comparison of capacity vs PSNR for lena image with other techniques

4.5.2 Robustness Analysis

Similarity between original secret image and extracted image is measured by calculating the Normalized Cofficient(NC).Without any attack the secret image extracts perfectly. The robustness of the proposed scheme was evaluated by conducting some possible attacks on the stego image such as JPEG compression, filtering, noise addition,scaling etc. which are given as follows:

- **JPEG compression:** JPEG compression is a standard lossy compression technique in which an image is compressed to reduce its memory space and bandwidth requirements for transmission over the Internet. In our simulation, JPEG compression with quality factor 90 , 75 and JPEG 2000 with compression ration 5,10 was applied.

- **Gaussian noise:** Gaussian noise with variance 0.01 was applied to the stego images.
- **Salt and pepper noise:** Salt and pepper noise with variance 0.01 was applied.
- **Median filtering:** 3 ×3 median filter was applied to the stego images.
- **Wiener filtering:** 3 × 3 wiener filter was applied to the stego images.
- **Scaling:** The stego image was resized to 256× 256 to provide a scaling factor of 0.5.

Table 4.6 shows the NC values of different attacks performed on the stego images.We can see that the NC values ranges from 0.9905 to 0.8041 which are on accepted level.It is most robust against JPEG compression and least robust against gaussian noise. In table 4.6 we can see that NC values for JPEG compression with quality factor 90 ranges from 0.9708 to 0.9845.With quality factor 0.75 it ranges from 0.9505 to 9733.For JPEG 2000 with compression ratio 5 and 10 NC values ranges from 0.9587 to 9905 and 0.9311 to 0.9827 respectively.For gaussian and salt and pepper noise it ranges from 0.8041 to 0.8505 and 0.9325 to 0.9478.For median filtering,average filtering and scaling it ranges from 0.8132 to 0.9712,0.8100 to 0.9386,0.8500 to 0.9731.From these results we can say that our method has good robustness against several attacks.

Attack	NC(Lena)	NC(Airplane)	NC(Baboon)	NC(Peppers)	NC (Lake)	NC (House)
JPEG 90	0.9769	0.9845	0.9708	0.9687	0.9749	0.9738
JPEG 75	0.9640	0.9733	0.9505	0.9548	0.9553	0.9629
JPEG 2000 (5:1)	0.9872	0.9905	0.9587	0.9809	0.9821	0.9889
JPEG 2000(10:1)	0.9770	0.9827	0.9311	0.9742	0.9588	0.9750
Gaussian noise (0.01)	0.8323	0.8206	0.8041	0.8184	0.8169	0.8505
Salt and Pepper noise(0.01)	0.9478	0.9432	0.9325	0.9456	0.9342	0.9393
Median filtering(3*3)	0.9712	0.9688	0.8132	0.9454	0.9184	0.9703
Blurring(Average filtering 3*3)	0.9310	0.9386	0.8100	0.9129	0.8892	0.9232
Scaling(1/2)	0.9700	0.9731	0.8500	0.9609	0.9422	0.9582

Table 4.6: NC values after performing different attacks

In 4.7 we can see the comparison of robustness using NC value with the above mentioned method.It is evident from the table that our method performs good in terms of robustness.[31] shows better robustness for some attacks like JPEG 2000 and scaling but shows poor robustness for some other methods like gaussian noise,salt and pepper noise.They use non blind approach and spread spectrum method for data embedding which makes it robust to several attacks.However,Our method is blind which is more preferable in steganography.[29] shows comparatively less robustness for every attack shown in the table.They use dct and while extracting dct results in some round off error which makes it difficult to resist attacks.Our scheme uses quantization index modulation for data embedding.QIM based method generally perform well against robustness.Morever,We have done our work in quaternion domain which provides us extra benefits from several attacks.In quaternion based methods, data energy propagates through all the color channels rather than only one color channel which provides extra benefits in terms of robustness without affecting imperceptibility.

Attack	[31]	[29]	Proposed
jpg 90	0.9457	0.8614	0.9769
jpg 75	0.9442	0.6017	0.9640
j2k 1:5	0.9479	0.9868	0.9872
j2k 1:10	0.9474	0.9522	0.9770
Gaussian noise	0.9117	0.7276	0.8323
Salt and pepper noise	0.9384	0.8973	0.9478
Scaling	0.9480	0.0476	0.9700

Table 4.7: Comparison of robustness with other methods

4.5.3 Security Analysis

Security is one of the most important part of an image steganographic algorithm.It can be analyzed using various techniques.One of the technique is analyzing key-space and key sensitivity.In our method we used gauss iterated map for better security.We have performed key space analysis,key sensitivity analysis, histogram analysis,blind steganalysis.We have also performed differential analysis of gauss map to evaluate security.Key space and key sensitivity of this map is discussed below.

Keyspace: Key space refers to the number of unique keys that can be generated using the map.In our method the key length is equal to the secret sequence size N.Again it consists of binary bits 0 and 1.So,the key space can be calculated as 2^N which is sufficiently large.

keysensitivity: It refers to the value of bit error rate occured in extracted image after giving a wrong key.Table 4.8 reflects the key sensitivity of our method.

Key type	key	BER
Right Key	$\alpha = 5.67, \beta = 0.567, x = 0.231$	0.0000
Wrong key	$\alpha = 5.28, \beta = 0.567, x = 0.231$	0.5000

Table 4.8: Key sensitivity analysis

4.5.3.1 Differential Analysis

Differential analysis of an encryption method can be done by calculating The number of changing pixel rate (NPCR) and the unified averaged changed intensity (UACI).NPCR is defined as the number of pixels that change in the encrypted image when one pixel change occurs in the original image.It can be calculated as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{I \times J} \times 100\% \tag{4.1}$$

Where,

$$D(i,j) = \begin{cases} 0 & \text{if } d(i,j) = d\prime(i,j) \\ 1 & \text{if } d(i,j) \neq d\prime(i,j) \end{cases} \tag{4.2}$$

Where,d(i,j) and d′(i,j) are pixel values of two ciphertext images whose plaintext images are slightly different.The more the NPCR value the better the encryption algorithm but it should be above 90 percent.

UACI refers to the average intensity differences between two paired cipher images.Lower value of UACI is appreciated for a good encryption scheme.It can be calculated as:

$$UACI = \frac{1}{I \times J} \sum_{i,j} \frac{d(i,j) - d\prime(i,j)}{255} \times 100\% \tag{4.3}$$

From table 4.9 we can see that gauss map has an acceptable NPCR and UACI value for large images that clarifies its ability to resist differential attacks.

Image Size	NPCR	UACI
32 × 32	0.78563995 83798	0.24798514 61900
64 × 64	0.93652343 75145	0.27936102 17510

Table 4.9: NPCR and UACI values

4.5.3.2 Histogram Analysis

Another common technique is to analyze histograms of stego image and cover image.If they both look similar then we can say that existence of payload is not detectable and the method is secure.From the histograms we can see that the histograms of cover image and corresponding stego image look similar hence passes histogram analysis test.

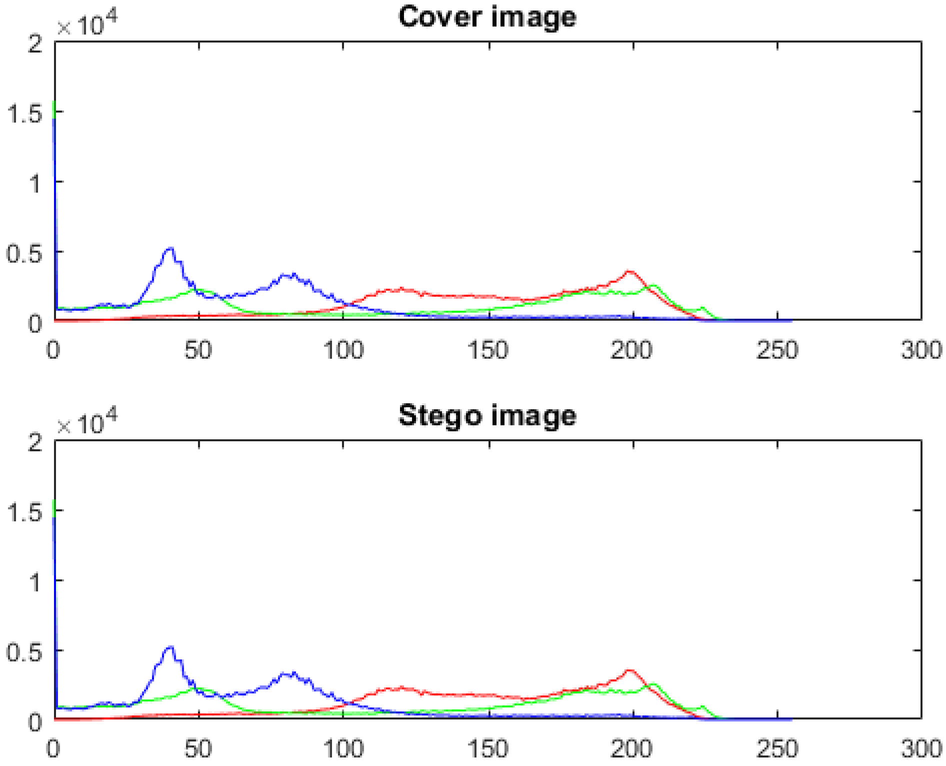


Figure 4.5: Histogram of ’Peppers’ cover image and stego image

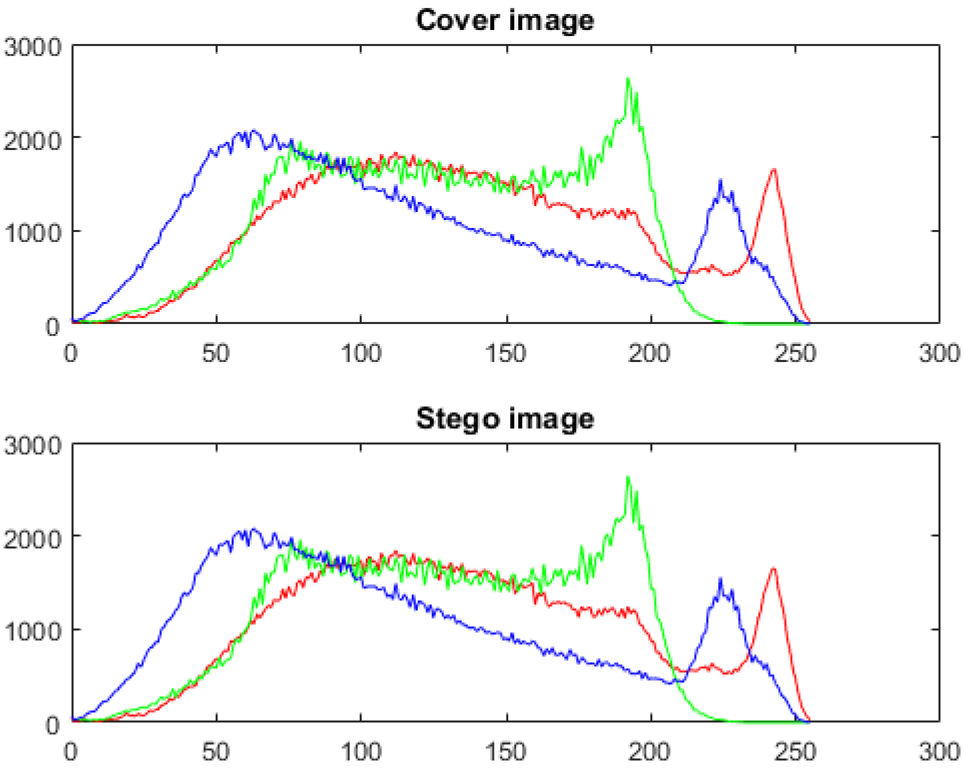


Figure 4.6: Histogram of ’Baboon’ cover image and stego image

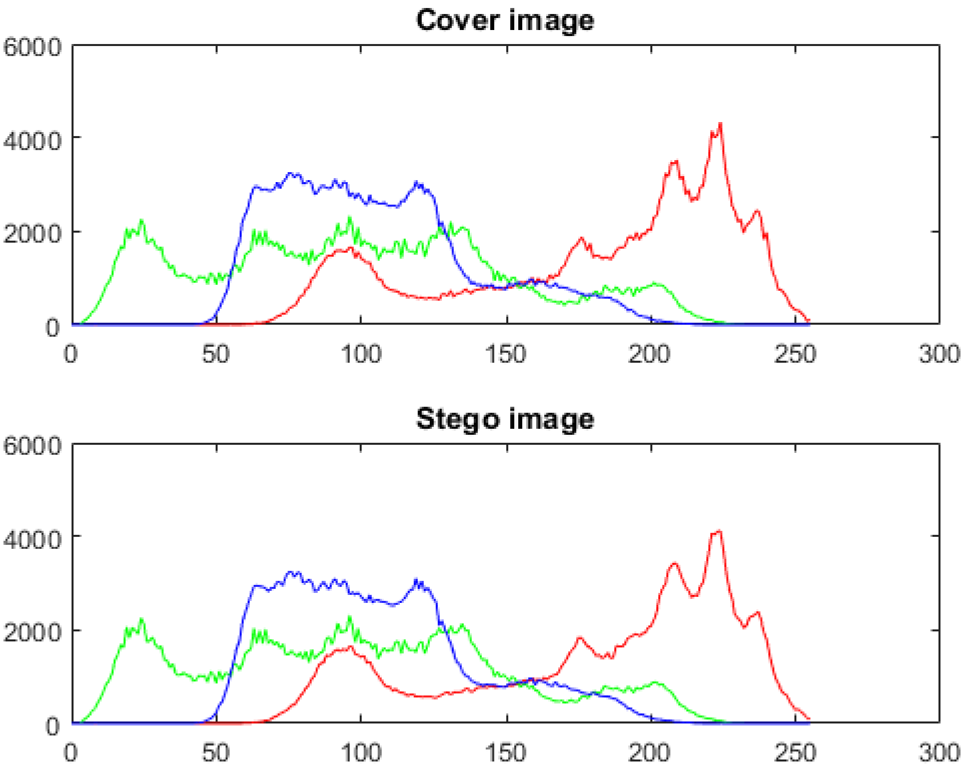


Figure 4.7: Histogram of ’Lena’ cover image and stego image

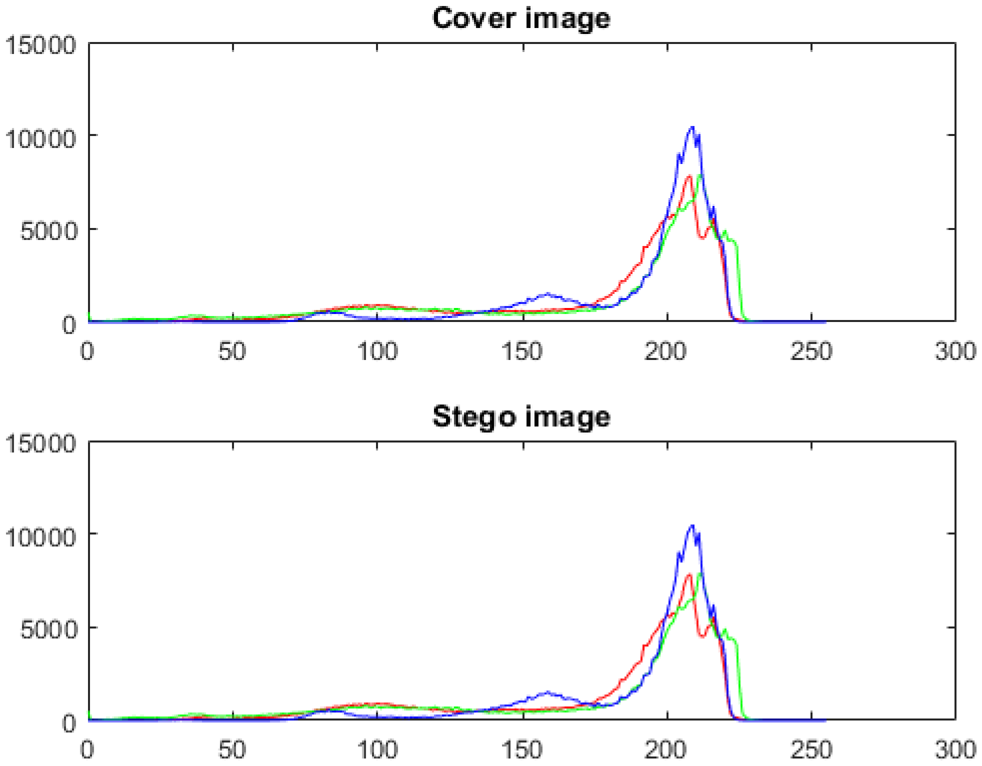


Figure 4.8: Histogram of 'Airplane' cover image and stego image

4.5.3.3 Steganalysis performance

Steganalysis is process of detecting existence of hidden data in a cover media.It is an important part of security analysis of a steganographic system.Steganalysis is a two class classification problem that classifies input image as either cover or stego.Here ,we have used StegExpose tool[32] and carried blind steganalysis to analyze security performance.

Steganalysis using StegExpose tool:

StegExpose is a tool that performs combination of several well known steganalysis methods including primary sets,RS analysis,Chi-square attacks„simple pair analysis.It takes a given threshold,performs the experiments and gives result of whether a given image is above threshold or not.Primary sets is a technique of recognizing lsb steganography that forms subset of pixels whose cardinality differs to detect existence of payload.Lossless capacity in lsb and shifted lsb plane is inspected to determine message length.Sample pair analysis is a fast and simple steganalytic technique that is based on a finite state machine whose states are formed from selected multisets of sample pairs.Statistical measures of these pairs are used to detect steganography.RS analysis divides stego image pixels into three groups.Regular group(R_m or R_{-m}),Singular group(S_m or S_{-m}) and unusable group.If $R_m \cong R_{-m} > S_m \cong S{-}m$ then secret message is not detected.Chi square attack is another famous method to test the security of an information hiding system.It compares the probability analysis of the image before and after embedding.If the difference is near zero that means the image is clean.If the difference is near one then it is stego.

Image	Capacity(bpp)	Above stego threshold?	Primary Sets	Chi Square	Sample Pairs	RS analysis	Fusion (mean)
Lena	0.1	False	0.056935823	0.008812059	0.107577776	0.012222711	0.046387092
	0.3	False	0.012297875	0.004498658	0.065062898	0.0168353	0.024673683
	0.5	False	0.009518265	0.004908711	0.025324322	0.01690084	0.014163035
Peppers	0.1	False	0.057750725	0.001281419	0.024504799	0.075572913	0.039777464
	0.3	False	0.008758748	0.009887209	0.06290166	0.074431762	0.038994845
	0.5	False	0.008261542	0.004454271	0.038978467	0.064385042	0.02901983
Baboon	0.1	False	0.067577646	0.234222474	0.357689896	0.061563648	0.180263416
	0.3	False	0.012635019	0.504718218	0.064824729	0.027608654	0.152446655
	0.5	False	0.059298857	0.506963958	0.040945045	0.010781442	0.154497325
Airplane	0.1	False	0.033468702	0.069284334	0.024025586	0.012724305	0.034875732
	0.3	False	0.002159886	0.076936729	0.013751809	0.005574291	0.024605679
	0.5	False	0.03969522	0.073493765	0.002040235	0.011090121	0.031579835
House	0.1	False	0.009432752	0.000653	0.00723403	0.003713184	0.005258252
	0.3	False	0.002574475	0.00171	0.002282724	0.007991213	0.003254801
	0.5	False	0.007619128	0.0000505	0.002920422	0.009736307	0.0050816
Lake	0.1	False	0.012777079	0.001151288	0.109135993	0.008017093	0.032770364
	0.3	False	NaN	0.007204706	0.034182242	0.021254022	0.020880323
	0.5	False	0.037095264	0.005539327	0.019741618	0.029955571	0.023082945

Table 4.10: Security analysis using different types of attacks

Table 4.10 shows the result of security analysis using StegExpose tool.From the table we can see that all our test images with different capacities are below the threshold and can resist the steganalytic attacks. **Blind Steganalysis:**

We have performed two blind steganlysis experiment.We performed these analysis using images from Washington image database .The experiments are described below.

1. DCT and Markov Feature Based Steganalysis: In the first experiment for

security is steganalysis method which consists of two parts: “feature extraction” and “classification.” The extracted features include 274 merged extended DCT and Markov features which are calibrated by the Cartesian product as introduced in [33] yielding 548 features in total. For classification, we applied the ensemble classifiers[34] using the extracted features.

2. The second algorithm we used to verify detection accuracy is Gabor filter based steganalysis [35]. Features were extracted for the same set of cover and stego images. Here, feature dimension was 17000 for each image. The same ensemble classifier was used to classify the test images.

Detection Errors for above experiments are given below:

Capacity(bpp)	Experiment 1	Experiment 2
0.1	51.57%	48.06%
0.3	48.80%	40.78%
0.5	41.57%	37.75%

Table 4.11: Result of Blind Steganalysis

From the above result we can see that detection accuracy of the classifier for our method is random.It can not effectively identify cover and stego images.Hence,we can say that our proposed method is secure.

4.6 Conclusion

From the above tables we can see that the method generates stego image of very good quality even when capacity is high.It also uses a chaotic encryption algorithm and without the knowledge of the key,it is not possible to decrypt the secret image.It also shows,robustness to an acceptable level compared to the other steganographic techniques shown here.

Chapter 5

Conclusion

5.1 Conclusion

In this thesis,we have developed a new image steganography scheme that uses Wavelet Based Contourlet Transform and Quaternion QR decomposition.Both WBCT and QQR are relatively new in the field of data hiding.The method maintains a good balance between imperceptibility and capacity which is feature of an efficient steganographic system.Morever,In this method secret image is encrypted using relatively new and secure chaotic map encryption method that ensures its security.This method also provides robustness to an accepted level.So,we can say that our method is an unique and good one.

5.2 Future Work

In image steganography both WBCT and QQR has not been used before.So,many other techniques can be used to design and enhance the embedding and extraction scheme.It can be made more secure by using more sophisticated encryption algorithm.

References

[1] S. Katzenbeisser and F. A. Petitcolas, *Information Hiding Techniques for Steganography and Digital Watermarking*, 1st. USA: Artech House, Inc., 2000, ISBN: 1580530354 (cit. on p. 1).

[2] N. Tiwari and M. Shandilya, 'Evaluation of various lsb based methods of image steganography on gif file format,' *International Journal of Computer Applications*, vol. 6, pp. 1–4, 2010 (cit. on p. 1).

[3] A. Cheddad, J. Condell, K. Curran and P. Mc Kevitt, 'Digital image steganography: Survey and analysis of current methods,' *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010, ISSN: 0165-1684. DOI: `https://doi.org/10.1016/j.sigpro.2009.08.010`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0165168409003648` (cit. on p. 2).

[4] L. Marvel, C. Boncelet and C. Retter, 'Spread spectrum image steganography,' *IEEE transactions on image processing : a publication of the IEEE Signal Processing Society*, vol. 8, pp. 1075–83, Feb. 1999. DOI: `10.1109/83.777088` (cit. on p. 2).

[5] B. Datta, S. Roy, S. Roy and S. Bandyopadhyay, 'Multi-bit robust image steganography based on modular arithmetic,' *Multimedia Tools and Applications*, vol. 78, Jan. 2019. DOI: `10.1007/s11042-018-6195-y` (cit. on p. 3).

[6] H. Shivaram, D. Acharya, R. Adige and P. Kamath, 'A secure image steganography technique to hide multiple secret images,' vol. 131, pp. 613–620, Jan. 2013. DOI: `10.1007/978-1-4614-6154-8_60` (cit. on p. 3).

[7] I. J. Kadhim, P. Premaratne, P. J. Vial and B. Halloran, 'Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,' *Neurocomputing*, vol. 335, pp. 299–326, 2019, ISSN: 0925-2312. DOI: `https://doi.org/10.1016/j.neucom.2018.06.075`. [Online]. Available: `https://www.sciencedirect.com/science/article/pii/S0925231218312591` (cit. on p. 5).

[8] M. Sutaone and M. Khandare, 'Image based steganography using lsb insertion,' 2008 (cit. on p. 9).

[9] S. Rajendran and M. Doraipandian, 'Chaotic map based random image steganography using lsb technique.,' *IJ Network Security*, vol. 19, no. 4, pp. 593–598, 2017 (cit. on p. 9).

[10] I. R. Grajeda-Marın, H. A. Montes-Venegas, J. R. Marcial-Romero, J. Hernández-Servın, V. Muñoz-Jiménez and G. D. I. Luna, 'A new optimization strategy for solving the fall-off boundary value problem in pixel-value

differencing steganography,' *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 32, no. 01, p. 1 860 010, 2018 (cit. on p. 10).

[11] H. Nyeem, 'Reversible data hiding with image bit-plane slicing,' in *2017 20th International Conference of Computer and Information Technology (ICCIT)*, 2017, pp. 1–6. DOI: 10.1109/ICCITECHN.2017.8281763 (cit. on p. 10).

[12] T. Rabie and I. Kamel, 'High-capacity steganography: A global-adaptive-region discrete cosine transform approach,' *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6473–6493, 2017 (cit. on p. 10).

[13] V. Holub, J. Fridrich and T. Denemark, 'Universal distortion function for steganography in an arbitrary domain,' *EURASIP Journal on Information Security*, vol. 2014, no. 1, pp. 1–13, 2014 (cit. on p. 10).

[14] V. Holub and J. Fridrich, 'Designing steganographic distortion using directional filters,' in *2012 IEEE International workshop on information forensics and security (WIFS)*, IEEE, 2012, pp. 234–239 (cit. on p. 10).

[15] S. Singh, R. Singh and T. J. Siddiqui, 'Singular value decomposition based image steganography using integer wavelet transform,' in *Advances in signal processing and intelligent recognition systems*, Springer, 2016, pp. 593–601 (cit. on p. 10).

[16] M. S. Subhedar and V. H. Mankar, 'Image steganography using redundant discrete wavelet transform and qr factorization,' *Computers & Electrical Engineering*, vol. 54, pp. 406–422, 2016 (cit. on p. 10).

[17] ——, 'Image steganography using contourlet transform and matrix decomposition techniques,' *Multimedia Tools and Applications*, vol. 78, no. 15, pp. 22 155–22 181, 2019 (cit. on p. 11).

[18] R. Eslami and H. Radha, 'Wavelet-based contourlet transform and its application to image coding,' in *2004 International Conference on Image Processing, 2004. ICIP'04.*, IEEE, vol. 5, 2004, pp. 3189–3192 (cit. on pp. 11, 14).

[19] M. Li, X. Yuan, H. Chen and J. Li, 'Quaternion discrete fourier transform-based color image watermarking method using quaternion qr decomposition,' *IEEE Access*, vol. 8, pp. 72 308–72 315, 2020 (cit. on p. 11).

[20] M. Khalil, 'Using quaternion fourier transform in steganography systems,' *International Journal of Communication Networks and Information Security*, vol. 10, no. 2, pp. 425–431, 2018 (cit. on p. 11).

[21] C. E. Moxey, S. J. Sangwine and T. A. Ell, 'Color-grayscale image registration using hypercomplex phase correlation,' in *Proceedings. International Conference on Image Processing*, IEEE, vol. 2, 2002, pp. II–Ii (cit. on p. 12).

[22] M. Khan, T. Shah and S. I. Batool, ‘Texture analysis of chaotic coupled map lattices based image encryption algorithm,’ *3D Research*, vol. 5, no. 3, pp. 1–5, 2014 (cit. on p. 13).

[23] K. S. Sankaran, G. Ammu and V. Nagarajan, ‘Non local image restoration using iterative method,’ in *2014 International Conference on Communication and Signal Processing*, IEEE, 2014, pp. 1740–1744 (cit. on p. 13).

[24] M. N. Do and M. Vetterli, ‘The contourlet transform: An efficient directional multiresolution image representation,’ *IEEE Transactions on image processing*, vol. 14, no. 12, pp. 2091–2106, 2005 (cit. on p. 14).

[25] J. Liu, G. Liu, W. He and Y. Li, ‘A new digital watermarking algorithm based on wbct,’ *Procedia Engineering*, vol. 29, pp. 1559–1564, 2012 (cit. on p. 15).

[26] A. Bunse-Gerstner, R. Byers and V. Mehrmann, ‘A quaternion qr algorithm,’ *Numerische Mathematik*, vol. 55, no. 1, pp. 83–95, 1989 (cit. on p. 16).

[27] R. Kaur and B. Singh, ‘A hybrid algorithm for robust image steganography,’ *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 1–23, 2021 (cit. on pp. 27–31).

[28] M. Nazari and I. D. Ahmadi, ‘A novel chaotic steganography method with three approaches for color and grayscale images based on fis and dct with flexible capacity,’ *Multimedia Tools and Applications*, vol. 79, no. 19, pp. 13 693–13 724, 2020 (cit. on p. 28).

[29] E. Ghosh, D. Debnath and B. G. Banik, ‘Blind rgb image steganography using discrete cosine transformation,’ in *Emerging Technologies in Data Mining and Information Security*, Springer, 2019, pp. 189–201 (cit. on pp. 28, 33).

[30] A. Miri and K. Faez, ‘An image steganography method based on integer wavelet transform,’ *Multimedia Tools and Applications*, vol. 77, no. 11, pp. 13 133–13 144, 2018 (cit. on pp. 28–30).

[31] G. V. K. Murugan and R. U. Subramaniyam, ‘Performance analysis of image steganography using wavelet transform for safe and secured transaction,’ *Multimedia Tools and Applications*, pp. 1–15, 2019 (cit. on p. 33).

[32] B. Boehm, ‘Stegexpose - a tool for detecting lsb steganography,’ Oct. 2014 (cit. on p. 37).

[33] J. Kodovsk and J. Fridrich, ‘Calibration revisited,’ in *Proceedings of the 11th ACM workshop on Multimedia and security*, 2009, pp. 63–74 (cit. on p. 39).

[34] J. Kodovsky, J. Fridrich and V. Holub, ‘Ensemble classifiers for steganalysis of digital media,’ *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, pp. 432–444, 2011 (cit. on p. 39).

[35] X. Song, F. Liu, C. Yang, X. Luo and Y. Zhang, ‘Steganalysis of adaptive jpeg steganography using 2d gabor filters,’ in *Proceedings of the 3rd ACM workshop on information hiding and multimedia security*, 2015, pp. 15–23 (cit. on p. 39).