Histogram and Vector Quantization based Multilevel Reversible Data Hiding Schemes

Thesis Submitted in partial fulfillment of the requirements for the award of degree of

Master of Technology

in

Computer Science and Applications

Submitted By

Sonal Kukreja
Roll No. 601303026

Under the Supervision of
Dr. Singara Singh Kasana
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR UNIVERSITY

PATIALA - 147004

JULY 2015

CERTIFICATE

Certified that this Thesis Report entitled "**Histogram and Vector Quantizaion Based Multilevel Reversible Data Hiding Schemes** " submitted by **Ms. Sonal Kukreja,** in the partial fulfillment of the requirement, for the award of **Master of Technology (Computer Science & Applications)** of **Thapar University, Patiala** is a record of student's own study carried under my supervision. This report is of desired standard and has not been submitted in any other University or Institute for the award of the degree.

Dated: 6.7.2015

Place: Patiala

Sonal.

(Sonal Kukreja)

This is to certify that above declaration made by the student concerned is correct to the best of my knowledge and belief.

6/7/15

Dr. Singara Singh Kasana
Assistant Professor
Computer Science and Engineering Department

Countersigned By:

Dr. Deepak Garg
Head
Computer Science and Engineering Department
Thapar University
Patiala

Dr. S.S. Bhatia
Dean (Academic Affairs)
Thapar University
Patiala

ACKNOWLEDGEMENT

I am highly grateful to the authorities of Thapar University, Patiala for providing this opportunity to carry out the thesis work. I would like to express a deep sense of gratitude and thanks profusely to my thesis guide Dr. Singara Singh, Assistant Professor, Department of Computer Science and Engineering, T.U, Patiala, for his sincere and invaluable guidance, suggestion and sympathetic attitude which inspired me to submit this seminar report in the present form. This thesis work was enabled and sustained by his vision and ideas. I have been amazingly fortunate to have an advisor like him, whose patience and support always helped me to overcome many crisis situations and successfully complete this dissertation. I am also thankful to other faculty members of CSED, T.U. Patiala for their intellectual support. Lastly, I would like to thank my parents, other family members and friends who constantly encouraged me to complete this study.

Sonal.

Sonal Kukreja

(601303026)

Abstract

Data hiding techniques in digital images has been a topic of research for so many years. The role of data hiding is to embed secret data in the cover media at the sender side and retrieve the embedded secret data as well as the cover media at the receiver side. Reversible data hiding techniques are used to recover the cover media from marked media by extracting secret media without any distortion. The main purpose of this dissertation is to improve the hiding capacity of the images while maintaining the PSNR upto a level.

In this dissertation, we have proposed three reversible data hiding techniques. The first technique is based on histogram shifting. In this technique, histogram shifting is used to create space for hiding the secret data, where the shifting is done between the peak and minimum points of the histogram of the cover image, hiding the data into the pixels corresponding to the maximum point. This technique is applied first to the cover image and then to the obtained stego images upto a desired number of levels, thus increasing the hiding capacity of the cover image. This technique embeds large amount of secret data while maintaining the visual quality of the stego images. Proposed technique is completely reversible as embedded data is extracted without any loss.

Second technique is multilevel reversible data hiding technique based on the blocks of difference image. In this technique, a cover image is divided into non overlapping blocks of equal size and then simple and absolute differences of each block are evaluated. After it, histogram of each absolute difference block is generated and peak negative points of simple difference are replaced into absolute difference blocks at respective positions. Then peak positive and peak negative points of each difference block are used to hide the secret data. Numbers of bits hidden into each positive peak points is one bit only but in negative peak points, more than a bit are hidden which increase the hiding capacity of a cover image. Proposed technique achieves high hiding capacity than existing reversible data hiding techniques while keeping distortion in the marked image low.

Another reversible data hiding technique based on a *VQ* index table as well as histogram shifting is proposed in which first, the codebook is rearranged referring to the index occurrence frequency in the *VQ* index table. After that, the code words in the newly generated codebook are clustered into a number of groups for the usage of hiding secret digits in the proposed technique. After applying *VQ* to the image, histogram shifting is applied to this vector quantized image thereby hiding data in the compressed image. Proposed techniques have been tested on different gray scale images at different hiding capacities and qualitative measures of these images are performed.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Introduction

In this Chapter, basic concepts and techniques of data hiding are discussed. It also covers the principle of data hiding, need of data hiding, various types of data hiding, properties of data hiding, applications of data hiding and its quality parameters which have been used throughout the dissertation. It also briefs the contribution of the dissertation and the organization of the dissertation.

With the rapid development of Information and multimedia technologies, almost all types of applications like medical, law enforcement, military, fine art work protection and many more, immensely use digital media to share and transmit data. Hence while transferring confidential data on the network, security of the data being transmitted is the main concern. The digital data, being transferred, consists of various types of data like text, images, audio, video *etc*., so there is a need to protect all these types of data from unauthorized users. From past few years, various methods have been proposed to enforce security of digital data in various applications. Most commonly used methods to secure the data are: cryptography and data hiding. In cryptography, the secret data is secured by scrambling it into unreadable form with the help of some key or program, and the same key is used to unscramble it at the receiver side. Various properties of data security like data integrity, data confidentiality, authentication, non repudiation of data *etc.* are fulfilled by cryptography. While in data hiding, the secret data is hidden in the cover media without any perceptual distortion or scrambling. Data hiding uses a variety of multimedia as the cover media and hides the secret information into it thereby generating marked media. Data hiding techniques must fulfill two main properties: good imperceptibility and sufficient capacity. Good imperceptibility guarantees the embedded data to be undetectable and sufficient capacity maximizes the hiding capacity.

1.2 Principle of Data Hiding

Data hiding involves both data embedding as well as data extraction. During embedding process secret data is hidden into digital data. The original digital data will be altered after the secret data gets hideded into it. This modified digital data is known as marked data which contain secret data. The original digital data is recovered when secret data is extracted from the marked data.

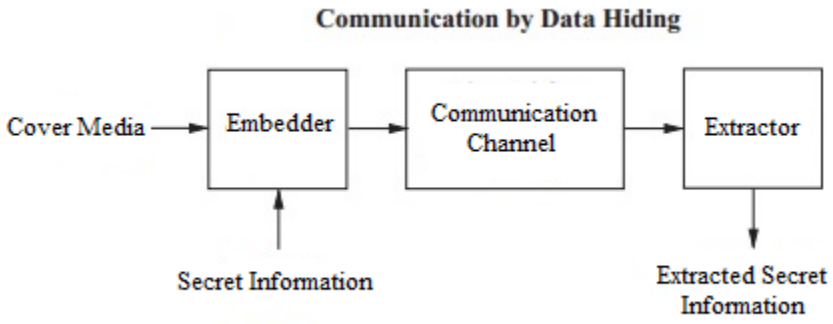


Figure 1.1 Traditional Data Hiding System

Figure 1.1 shows the traditional data hiding system which includes embedder and extractor. The multimedia data and secret data which is to be hidden are provided as input to the embedder. Various techniques and algorithms are applied in the embedder to hide secret data in the cover media ensuring maximum capacity and minimum distortion in the marked image. The output of embedder is marked data. Then the marked image is transferred through the communication channel. At the receiver side, reverse of the embedding algorithms is applied to retrieve the secret data as well as the cover media exactly without any distortion. The input to the extractor is the marked data and the output of the extractor is the secret data and cover media.

1.3 Need of Data Hiding

- Covert communication using the images (secret data is hidden in the cover media)
- Ownership of digital images, copyright and authentication
- Data integrity, self-correcting images and fraud detection
- Traitor-tracing (fingerprinting video-tapes)
- Adding captions to images, additional information, such as subtitles, to video, embedding subtitles or audio tracks to video (video-in-video)

- Intelligent browsers, viewing a movie in a given rated version, automatic copyright information,
- Copy control
- Device control

1.4 Types of Data hiding

There are multiple kinds of data hiding techniques, which are differentiated and briefed in the explanation below. Data techniques have been broadly classified into four types and further divided:

1.4.1 On the basis of recovery of cover media

On the basis of recovery of media, data hiding techniques are divided into two categories.

1.4.1.1 Reversible data hiding technique

In the reversible data hiding techniques, secret data is hidden in the cover media at the sender side and at the receiver side, secret data is extracted from the cover media and both are recovered. Reversible techniques are used to recover the cover media from marked media by extracting secret media without any distortion. Cover media and secret data both are equally important in many areas such as medical, military *etc.*

1.4.1.2 Irreversible data hiding technique

In the irreversible data hiding techniques, when secret information is hidden in cover media and transferred to the receiver side, then at the time of extraction, only secret information is recovered but cover media gets lost or distorted *i.e.* cover media cannot be recovered from the marked media in the extraction process.

1.4.2 On the basis of extraction

On the basis of the extra information needed at the time of extraction, data hiding techniques are divided into three categories:

1.4.2.1 Blind data hiding technique

In the blind data hiding technique the cover media is not required to extract the secret data during the time of extraction at the receiver side.

1.4.2.2 Semi blind data hiding technique

In the semi blind data hiding technique, like the blind data hiding technique it also does not require cover media to extract the secret media, but it extracts the secret media with the help of some extra information.

1.4.2.3 Non blind data hiding technique

In the non blind data hiding technique, the cover media is required to extract the secret media from it at the receiver side.

1.4.3 On the basis of domain

On the basis of domain of data embedding, data hiding techniques are divided into three categories.

1.4.3.1 Spatial domain data hiding technique

In the spatial data hiding technique, secret data is hidden directly into the pixels of cover image. This technique is easy to implement. A remarkable example of spatial domain data hiding technique is Least significant bit (*LSB*) method, in which secret data is hidden in the *LSB* of the pixel values of the cover image.

1.4.3.2 Transform domain data hiding technique

In the transform domain data hiding techniques, various transformations like Discrete Wavelet Transform *(DWT)*, Discrete Fourier Transform *(DFT)* etc. are applied to the cover media, and then secret data is embedded into these transform domain instead of directly embedding into the cover media.

1.4.3.3 Compressed domain Information hiding

In this type of data hiding technique, compressed codes of the cover media are used to hide the secret information.

1.4.4 On the basis of application

On the basis of recovery of application, data hiding techniques are divided into two categories.

1.4.4.1 Steganography

The term Steganography has been derived from Greek words steganos that means covered whereas graphein refers to writing. In steganography, the message which has been hidden into the image does not have any relationship with the cover image. The recipient does not have any interest in the original cover image, as it is only an extra source and is basically of not much importance to the reciever. Therefore, there is no need to retrieve the original cover image at the reciever side after extracting the hidden secret message.

1.4.4.2 Watermarking

In digital watermarking, the hidden secret data has a close relationship with the cover media. The hidden message provides additional information about the cover image, like an authentication code, signature of the author, and many more. Unavoidably, hiding the data modifies the cover image although the distortion which occurs by hiding the data is undetectable to the human visual system. But, for some sensitive images, like medical images, military images, artwork preservation , even the least alteration in the values of the pixels prove to be intolerable. Reversible data hiding or lossless data hiding has been proposed to ensure that a sensitive image gets completely recovered after the hidden data is extracted completely.

1.5 Properties of Data Hiding

There are some properties that must be included by data hiding technique.

1.5.1 Imperceptibility

Imperceptibility is the fundamental property of information hiding in which marked image looks similar as the original image. The secret data should not be visible to human eyes. Peak Signal to Noise Ratio (*PSNR*) is usually used to define imperceptibility. This property is based on the human visual system. The embedded secret data in the cover media should not develop any visual distortion, which an average human subject is able to differentiate between cover media containing hidden data and those without any hidden data. In the embedding technique, the solution to this problem is human perceptual modeling. The concept of imperceptibility comes when the visibility of distortion is tested by presenting both cover media with or without embedded data.

1.5.2 Robustness

Robustness describes the behavior of the algorithm for distortions in the data which are introduced due to standard and malicious data processing. If the presence of embedded data can be detected reliably even after tempering an image but not have any distortion beyond reorganization then this embedded information said to be robust. Lossy compression, linear and nonlinear filters (blurring, sharpening, median filtering), gamma correction, cropping, contrast adjustment, resampling, recoloring, rotation, scaling, small nonlinear deformations, noise adding, pixel permutation in small neighborhood, are some of the examples of tempering. Attacks on the

embedding techniques which are based on the concept of the embedding algorithm or on the availability of the detector function, are not included in the robustness. A good data hiding technique should be robust against noise addition, filter processing, geometrical transformations such as scaling, translation and rotating and.lossy compression.

1.5.3 Security

Based on the concept of the embedding technique and the detector , and the information about least one carrier with secret data, if the embedded data cannot be retrieved or tampered by targeted attacks then, the embedding algorithm is said to be secure. Attacks attempt to remove, modify or embed unrequired data into marked image. Attacks are basically of two types, active attack and passive attack. Active attacks attempt to modify the secret data while passive attacks only detect only secret data.

1.5.4 Complexity

Complexity of the data hiding techniques is described by the time and effort needed to embed and retrieve the secret data. The computation cost of the technique increases with the increase in complexity, as more hardware and software resources are required to implement it. To decrease the computational cost of the system, the complexity should be reduced. Like in telemedicine domain, during the transmission of medical data, data hiding techniques with minimum complexity are implemented to reduce the cost of bandwidth consumption data capacity.

1.5.5 Capacity

Capacity of the data hiding system describes how much maximum amount of secret data can be embedded. Higher capacity of embedded information in data can be obtained by comprising either the robustness or imperceptibility of technique. Figure 1.2 below shows the trade off between the various properties of data hiding.

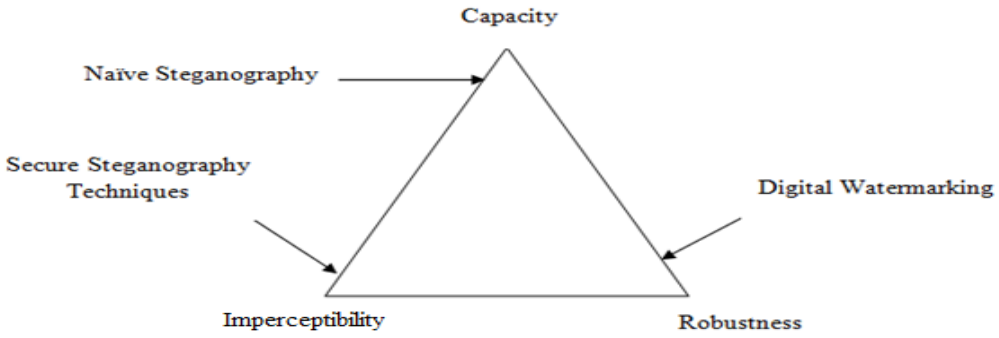


Figure 1.2 Trade off between embedding capacity, imperceptibility and robustness in data hiding.

1.6 Applications of data hiding

1.6.1 Broadcast Monitoring

In the broadcast monitoring, the human observers watch and observe the broadcasts and keep on recording what is visible and audible to them. The technique being used is too costly and is usually prone to errors. Hence the method should be preferably replaced with any form of automated monitoring. There are two types of techniques which can be used to do this: Passive monitoring and active monitoring. In Passive monitoring, the content being broadcasted is directly recognized by the systems, and hence human observers are simulated at much lower cost and is more reliable. In the case of Active monitoring, the systems are dependent on the related information that is broadcasted together with the content.

In the case of passive system, the system system monitors broadcasting and also compares the signals being received with the database of the existing works. There is no requirement of introducing any associated information into the broadcast, and hence there is no requirement of changes in the workflow of advertisers. No cooperation is required with any of the broadcasters or advertisers. However, there are still many problems existing which may cause hindrance enduring the implementation of the passive monitoring systems. Firstly, comparison of the received signals against the database is not a trivial solution. Moreover, broadcasting usually degrades the signals, and this degradation varies with time, resulting in multiple receptions of the same work at different durations may lead to various different signatures. This shows that the exact match cannot be searched in the database by the monitoring system. As an alternative, a substantially more complex nearest-neighbor search must be performed. As it it too complex to derive valid signatures and to searc nearest neighbors from the database, it is quite difficult to design a completely reliable passive monitoring system. Even if this issue of searching the database is solved, managing and storing the database proves to be still quite costly due to the large size of the database. Moreover, the system must also keep monitoring several geographic locations simultaneously. Still there has been a recent remarkable progress in passive broadcast monitoring.

An active monitoring system is required to ensure the accuracy of the verification services, hence the identification information which can be recognized by the computers easily has to be transmitted

along with the content. Passive monitoring is technically complex to implement as compared to active monitoring. It is straightforward to decode the identification information , and also no database is needed to interpret its meaning.

By placing the identical information in a separate area of the broadcast signal active system can be implemented. Watermarking is the alternative technique of coding the identification information in active monitoring systems. It can exist within the content itself, instead of exploiting a particular section of the broadcast signal, and hence is completely compatible with the base of broadcast equipments, which includes both digital and analog transmission.

1.6.2 Owner Identification

Owner identification is another very important application. To identify the owner of a specific digital work of art, a video or an image can be a quite complex task. But, it is a very important task, especially in the cases related to copyright infringement. So, instead of sending copyright notices with every image or song, watermarks can be used to embed the copyright in the image or the song itself.

As a technology for identifying owner of the work, textual copyright notices have various limitations. Firstly, they can be easily removed from the document when it is being copied, even when there is no intention of wrong doing. Therefore, a citizen who might want to use a work may sometimes find it complex to determine whether the work has been protected by the copyright. Even if the work is assumed to be protected, it may be difficult to detect the identity of the creator or the person whose permission must be obtained.

Another issue with the textual copyright notices is that they are sometimes quite ugly in presentation and might cover some part of the image. Some practices like making them unobtrusive, makes them even more susceptible for getting cropped, by placing them in an unimportant corner of the picture. The situation in audios is worse, where this copyright notice has to be usually placed on the physical medium or on the packaging. None of these notices are normally copied along with the audio content. In fact, some audio content may exist only in electronic form like on a website, where there is no physical medium or packaging .

As watermarks are made unnoticeable and inseparable from the work in which they are contained, they are most probably superior to the text to identify the owner. The users of the work are provided

with watermark detectors, hence they can identify the owner of a work which has been watermarked, even after the work is modified in ways which can remove the copyright notice.

1.6.3 Proof of Ownership

Watermarks are used not only to identify the ownership of copyright ownership but also to prove it. It cannot be performed by a textual notice, as it can be forged very easily. For example, let some individual creates some image and publishes it on the web site, together with the notice of copyright "c 2001 Alice." And let there be an adversary (say Bob) who then steals the image, uses some image processing technique to replace the copyright notice by its own "c 2001 Bob," and then claims to own the copyright himself. The first way of solving such an issue is by utilizing the central repository. Alice who initially posted the image on the website must register the image with the Copyright Office by submitting there one copy, before posting the image on the website. The image is archived, along with the information about it's rightful owner. After that, when some argument arises between Alice and Bob, Alice should contact the Copyright Office and can prove that she is the only rightful owner of that image. However, Alice may also refuse to register the image due to high expenses. As many images have to be registered, it can prove to be quite expensive for a struggling artist. There may be the case when Alice cannot afford the expenses, then she might prosecute Bob without any benefit of the Copyright Office on her side. In such cases, Alice can prove that she created the image by showing the evidences. For example, if that image was originally a photograph, the film negative or some previous drafts may also exist. Now the problem is, such evidences can also be fabricated themselves if Bob is highly determined to win the case. A new negative can be made from the image, or own drafts can be manufactured. On a worse case, if an image is created digitally, at the first case there may be the case when no negative or early draft might be present.

In the case of watermark of Digimarc, the rights cannot be protected and the registration cost can also be not avoided by transmitting a watermark along with the image. The adversaries always have the detectors along with them, hence anyone who can detect a watermark can also probably remove it. Thus, with the help of a detector, Bob can also remove the watermark of Alice and replace it with his own.

It is often required to restrict the availability of detector, so that the level of security to prove ownership can be achieved. When a detector is not available to the adversary, it can be extremely difficult to remove the watermark. Hence, when Alice and Bob are made to appear before the judge,

Alice can produce the original copy of her image. Both the original and the disputed copy are entered into the watermark detector, and the detector will detect the Alice's watermark.

However, even if her watermark cannot be removed, Bob can also undermine her. Bob, can make it appear as if his own watermark was present in the original copy of the Alice's image by using his own watermarking system. Hence, a third party might fail to judge who had the original copy. This issue can be solved a slight change is made in the problem statement. Instead of trying to directly prove ownership by embedding watermark message into it, it can instead be proved that one image is derived from another.

Thus this application area protects the rights of intellectual property and enables the proof of ownership. Data hiding techniques can embed data about the original author directly into the multimedia content. Thus, when some arguments considering the ownership of the multimedia arise, the legitimate author can claim its ownership.

1.6.4 Transaction Tracking

Transaction tracking is an interesting application of data hiding and watermarking. In this application of data hiding, the watermark records the transactions of the copy of some works in which embedding has been done, that have taken place in the history. In the terms of transaction tracking, the individual responsible for the misuse of the work is usually referred to as a traitor and the person who receives the work from the traitor is known as a pirate.

Transaction tracking is also known as fingerprinting, as every copy of the work is unique and can be excusively identified by the watermark, that is similar to the human fingerprint which uniquely identifies a person. There exist some technologies for transaction tracking which do not come under the definition of watermarking. Using visible watermarks is an alternative to the watermarking.

For example, watermark can be embedded in every legal copy of the movie to record the recipient of every copy. If then by any chance, movie is leaked to the Internet, the watermark can help the movie producers to identify which recipient of the movie was the source of the leak.

1.6.5 Content Authentication

Image content authentication was proposed to verify the integrity of the images, i.e. to provide a check if the images have undergone any tampering since the time it was created. Digital watermarking is becoming a sure technique which can provide image content authentication with the help of its outstanding performance and the capability to detect tampering of the media. But still,

many challenges still remain unsolved by which the watermarking techniques can provide authentication to the images, or it can be said that they need to be improved, like accuracy in tamper localization, quality of image, synthetic image protection, security and many more. Different solutions have been proposed to provide content authentication of natural images and synthetic images both, and also improving the accuracy of tamper localization and the quality of the image which has been watermarked. Additionally, new watermarking schemes have been developed with area of interest focusing on how to tackle the problems of high image fidelity requirements in specialized applications. Firstly, a watermarking technique was proposed for natural images authentication. The watermarking techniques significantly improve the resolution of tampered detection along with low watermark payload, by introducing the random permutation strategy in the wavelet domain,. As less watermarks get embedded, the quality of image is hence improved. Hence, thanks to those random wavelet coefficient groupings, that the scheme is proved to be intrinsically secure to the local attacks happening. Also, scalable sensitivity of tampered detection is set to enabled mode in the authentication processes by presetting the size of the noise filters. The proposed watermarking algorithm was completely compatible with the existing characteristics of the synthetic images. As comparatively less pixels are modified, the authentication system can still aim to achieve tamper localization resolution pixel wise. Moreover, a new embedding strategy was proposed, that enables the recovering of the the altered image content of the authentication system. Hence, the authenticator can localize the tampered media area and it can also recover the extracted content and identify the forged parts.

1.6.6 Copy Control

The use of watermarking technology to protect *DVD* from copy protection was first proposed in *IBM's* Tokyo Research Laboratory in 1996. It was shown that the embedded watermarks can be detected even in the *MPEG2*-compressed domain. This development enabled *DVD* recording devices to prevent playback of the copies and recordings which are unauthorized by using copy control information detected in the digital content. The digital information is transmitted between the transmitter side apparatus and receiver side apparatus passing through the interfaces which control that the access should be between the authorized parties only. An extra information i.e. the copy control information is added along with the main data that was recorded in the digital medium in such a way that now the recorded information consists of two parts: first part consists of the image or

the voice information and the second portion consists of the copy control information. Now the digital watermark is embedded into the second portion of the recorded information.

1.6.7 Device Control

These device control watermarks are embedded in the media to control access to the resources which are using a verifying device. The watermarking system is present to embed an authorization code in the signals and transmit it to the verifying device, for example television and radio programs. At the site of the verifying device, the authorization code is extracted from the signals which were watermarked and the operations which are to be performed on the resources are authorized separately on the authorization code which has been extracted, which might also contain permission to execute a program or copy a multimedia object.

The watermarks can also be embedded in the audio signals to remotely access the devices like toys, computer systems or various other appliances. An appropriate detector is embedded in the device so that the hidden signals can be detected and identified, triggering an action or changing the state of the machine or device. The watermarks are also used with time gate devices, where the watermark is held in the detector for a particular time interval, within which the user has permission to perform actions like typing or pushing buttons.

1.7 Quality Parameters

The visual quality of marked image versus the original image is the most important property of data hiding as it is difficult to detect by detectors. In the current work, *PSNR* has been taken as the quality parameter that is calculated using the cover original image and the marked image. The statistical difference between the cover image and the marked image is calculated using the given equation:

$$PSNR = 10log_{10}\frac{(2^b-1)^2}{MSE} \tag{1.1}$$

where b is the bit depth of cover image and *MSE* is the mean square error and is defined as

$$MSE = \sum_{m=1}^{h}\sum_{n=1}^{w}\frac{\delta(im,n)}{h\times w} \tag{1.2}$$

Where $\delta(m,n) = (X(m,n) - Y(m,n))^2$ in which $Y(m,n)$ describes the pixel of marked image and $X(m,n)$ describes the pixel of cover image, h and w is the height and width of the image respectively.

Similarity Index Modulation (*SIM*) is defined as

$$SIM = \frac{\sum_{m=1}^{h}\sum_{n=1}^{w} S(m,n)\times S'(m,n)}{\sum_{m=1}^{h}\sum_{n=1}^{w}[S(m,n)]^2} \quad (1.3)$$

SIM is used to evaluate the quality of extracted secret data image by the measurement of the similarity of the original secret image S and the extracted secret data image S'.

PSNR HVS is defined by taking into account Contrast Sensitivity Function (*CSF*). Images are divided into 8×8 pixels non-overlapping blocks and *DCT* of each block is computed. Then the $\delta(i,j)$ difference between the original and the distorted *DCT* blocks is weighted for every 8×8 block by the coefficients of the *CSF*. So equation (1.3) can be rewritten as follows,

$$\delta_{PSNR\ HVS}(i,j) = \delta(i,j)\ CSF(i,j) \quad (1.4)$$

For *PSNR HVS*, $\delta(i,j)$ is replaced by $\delta_{PSNR\ HVS}(i,j)$ in (1.2) to calculate *MSE* and (1.1) is then used to find *PSNR HVS* between original image and its marked image.

1.8 Contribution of the Dissertation

In this dissertation, the focus lies on the data hiding in cover media image with high hiding capacity as well as with high *PSNR*. For this criteria to put into practice, we used histogram shifting proposed by Ni *et al.* (2006), and the difference images proposed by Lin *et al.* (2009) to enhance the hiding capacity. In this dissertation, reversible data hiding algorithms with high hiding capacity has been proposed. Reversible data hiding is mainly used in areas such as medical, military *etc.* The main focus is to enhance the hiding capacity maintaining high *PSNR* between marked image and cover media. The contributions of the dissertation, in summary are:

- First, a multilevel data hiding technique is proposed in which histogram shifting is used upto certain number of levels. The number of levels has been used to increase the number of peak points in the histogram thereby increasing the hiding capacity. Histogram shifting is applied to the input cover image. Peak points are evaluated which are used to embed the secret data and the received marked image is again used as the cover image to embed the data. Thus, a method has been proposed for reversible data hiding which has high hiding capacity as well as *PSNR* value. Both the secret data as well as the cover media can be extracted and retrieved at the receiver side.
- Further multi level data hiding technique based on the histogram shifting in the difference images has been proposed in which both positive as well as negative differences between

the adjacent pixels are used to embed the data. This multi level data hiding technique provides large hiding capacity as compared to the previous ones. In this technique multi level concept has also been used to embed the secret data. The *PSNR* has also been maintained upto the desired values.

- A technique has been proposed to hide the secret data in the cover media by applying histogram shifting on the index images obtained after vector quantization, thereby efficiently using the transmission bandwidth by transmitting the compressed images and also hiding the data maintain the *PSNR* above 21 dB.

1.9 Organization of the Dissertation

Several techniques for data hiding using the histogram shifting along with multilevel embedding, difference images and vector quantization are proposed in this dissertation. The dissertation is organized as follows.

In Chapter 2, current literature on reversible data hiding has been described which elaborates the techniques used in reversible data hiding using histogram shifting and techniques which used difference images and vector quantization to embed the secret information.

Multilevel Reversible data hiding based histogram shifting has been discussed in Chapter 3. In this chapter, the data hiding using histogram shifting technique is applied first to the cover image and then to the obtained stego images upto desired number of levels, thus increasing the hiding capacity of the cover image.

In Chapter 4, Histogram based multilevel reversible data hiding scheme using simple and absolute difference images has been discussed which exploits the simple and absolute differences to increase the hiding capacity and reduce image distortion.

Chapter 5 covers the data hiding scheme using histogram shifting technique on vector quantized images, which shows the results of hiding capacity being increased as compared to the existing techniques.

The dissertation concludes in Chapter 6 where we summarize our work and also discuss some issues for further research in the area of data hiding.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

This Chapter briefs the various research papers studied covering various techniques of data hiding. Section 2.2 covers the histogram based techniques which will describe the various algorithms of hiding data in the images with the help of histogram shifting and then retrieving data as well as the cover media exactly at the receiver side with the minimum distortion possible. Section 2.3 of the chapter covers pixel value difference based techniques which will describe various algorithms which use difference of the adjacent pixels to hide the secret data. Then the hybrid and interpolation based techniques have been covered in section 2.4 and 2.5. The vector quantization based techniques in which data is hidden in the images compressed by the vector quantization techniques are covered in Section 2.6..

2.2 Histogram Based Techniques

Ni *et al.* (2006) proposed a reversible data hiding technique based on the histogram. The histogram of the image is generated by recording the occurrences of all the pixel values of the image. Hence with the help of this histogram, peak and zero points are calculated. Peak point corresponds to the pixel value with the maximum number of occurrences while zero point corresponds to the pixel value with minimum number of occurrences. All the pixels are shifted toward right or left based on the fact whether zero point is greater or less than the peak point respectively, thereby generating space to embed the secret data. *PSNR* of the marked image versus the original image is always maintained greater or equal to 48 dB with this technique.

Hwang *et al.* (2006) also proposed a modified histogram based reversible data hiding technique, in which the pixel values that are located adjacent to the peak point on both the sides are

modified to generate space to embed secret information. In this paper hiding capacity was enhanced, as there is no requirement to send the peak points and the zero points as side information to the receiver side. The secret information is embedded in the cover media with the help of location map.

Lee *et al.* (2006) proposed a reversible data hiding technique which is also based on the histogram shifting and uses the characteristic of difference image. The difference image consists of the differences between the adjacent pixels of the original image. In this paper, MD5 algorithm is used to securely transfer the cover media. The histogram shifting is applied on the difference image and the secret data is embedded into the modified difference image. Lower bound of *PSNR* of marked image with this technique is 51.14 dB. Execution time of this technique is better than previous technique.

Fallahpour *et al.* (2007) proposed a reversible data hiding technique which used block division and histogram shifting. This technique utilizes the peak point and the zero point of every block of the cover image to embed the secret data. Firstly it decomposed the whole cover image into blocks of same size and then histogram shifting is used to create the embedding space. Secret data is embedded in the space generated.

Kuo *et al.* (2008) proposed another histogram based reversible data hiding technique. In Hwang *et al.* (2006) technique, it is not compulsory that minimum point in cover image should be zero. To overcome this shortcoming, block division method in which cover image is decomposed into sub blocks has been proposed in this technique. This block division method increases the hiding capacity and recovers the cover image exactly at the receiver side.

Chung *et al.* (2012) proposed a reversible data hiding algorithm based on the histogram modification that uses block based complement method thereby reducing distortion taking place in Ni *et al.* (2006) data hiding technique.

Wang *et al.* (2012) proposed another reversible data hiding technique which was also based on the multilevel histogram shifting and embedding. Iterative multi histogram strategy has been applied to decrease the overhead information at the time of hiding data. This technique does not suffer underflow and overflow problems and maintain *PSNR* around 48.13 dB with hiding capacity 1 bit per pixel (bpp).

Wang *et al.* (2013) proposed a histogram shifting based reversible data hiding technique. The secret data is embedded into cover media by modifying the peak point pixel value into another

pixel value within the same segment instead of peak point of the histogram of the complete cover image. To extract secret data exactly, a location map is also used. Multilevel data embedding technique has been used to enhance the hiding capacity.

Li *et al.* (2013) proposed a general framework for histogram shifting based reversible data hiding technique. Many reversible data hiding techniques are the special case of this technique. In this technique by defining sifting and embedding function, a reversible data hiding technique is obtained. Adaptive embedding and location map free methods are limitation of this technique.

2.3 Pixel value Difference (PVD) Based Techniques

Tian (2003) used Difference Expansion *(DE)* to embed the secret information into cover image. In this technique, redundancy in an image is produced using integer Haar wavelet transform. Single pixel pair is used at a time and average and difference is computed for these pixels Secret information is embedded by expanding the difference of a pair of pixels so that it is called as difference expansion. In this technique pixel of a cover image divided into two type; expendable pixels and changeable pixel. This technique used a location map to prevent overflow/underflow.

Kamstra *et al.* (2005) proposed two technique of reversible data hiding; one is based on the *LSB* prediction and second one is an enhancement of Tian (2003) technique. In this technique Swelden's Lifting scheme is used for *LSB* prediction and *LSB* prediction is used for anticipate *LSB* plane with the help of information reside in the Most Significant Bit (*MSB*). This technique sorts the predicted *LSB* which enhance the performance of technique.

Thodi *et al.* (2007) proposed a technique which is an improvement of Tian (2003) technique. In this technique, prediction error is used for hiding data instead of taking difference between adjacent pixels. Several predictors are used for prediction in this technique like median edge detector, gradient adjust predictor etc. It not only uses prediction error expansion but also use histogram shifting for hiding secret information. This technique provides nearly double hiding capacity as compared to *DE* techniques.

Alter (2010) proposed a technique based on the *DE*. In this technique, difference expansion of vector is used instead of pixel pair to increase the hiding capacity. A general reversible integer transform is proposed which avoid the overflow and underflow problem which are derived for

any vector of inconsistent length. This technique is recursively applied to color component to enhance the hiding capacity.

2.4 Hybrid Techniques

Lin *et al.* (2008) proposed a difference image histogram modification based multilevel reversible data hiding technique. In this technique, difference image histogram is generated and peak of histogram is used to embed the secret information and multilevel hiding concept is used to enhance the hiding capacity. After 9^{th} level of this technique it provides average *PSNR* value greater than 30dB and average hiding capacity is 1.3 (bpp).

Tseng *et al*. (2008) proposed technique based on the histogram shifting and difference expansion and a extension of Tian (2003) technique. In this technique pixel is divide into type: shiftable and expandable pixel pair. With the help of shifting the difference of pixel pair hiding capacity is enhanced. This technique provides better visual quality and hiding capacity than Tian (2003) technique.

Tsai *et al.* (2009) proposed a histogram shifting based reversible data hiding technique. In this technique, linear prediction is used o explore the neighboring pixel in the cover image and residual histogram of predicted errors of the cover image is generated and used to embed the secret information. Hiding capacity enhances by using the overlapping of peak and zero points of the generated histogram. Visual quality of marked image is enhanced by 1.5 db as compared to other histogram based technique when equal amount of secret information is embedded into the cover image.

Luo *et al.* (2010) proposed a histogram based reversible data hiding technique using median. This technique uses the median to produce a difference histogram. Cover image is decomposed into blocks and blocks are divided into four different types to corresponding four hiding technique. In this technique histogram is generated block difference which is computed with the help of integer median. This technique uses multilevel strategy to enhance the hiding capacity.

Zhao *et al*. (2011) proposed a reversible data hiding method based on the pixel value difference and histogram. Similarity of neighboring pixel is used in this technique because differences between neighborhood pixels are close to zero or equal to zero. In basis of these differences, a histogram is generated. To embed the secret information a multilevel histogram modification is

used which enhance the hiding capacity as compared to traditional method based on one or two level histogram modification.

Chang *et al.* (2012) proposed a prediction and sorting based reversible data hiding technique. To compute the prediction for histogram based data hiding a rhombus prediction is used. To enhance correlation of neighbor pixels, prediction and sorting is used which enhance the hiding capacity. Overhead information is embedded by two state strategies and to prevent overflow and underflow, histogram shifting technique is used.

Huang *et al.* (2013) proposed a reversible data hiding technique based by using the hierarchal relationships of cover image. Histogram shifting is used to modify the difference values between pixels to embed the secret information using the inherent characteristics of cover image. This technique produces high visual quality with high hiding capacity.

2.5 Interpolation Based Techniques

Yang *et al.* (2008) proposed a data hiding technique which used interpolation and LSB substitution techniques. Here, the cover image is divided into non overlapping blocks of size 5×5. 5×5 size blocks are shrinked into blocks of size 3×3 and again blocks of size 5×5 are obtained by the interpolation of blocks of size 3×3. The difference is calculated between the interpolated block pixel value and original pixel value, if that difference is less than the threshold value or equal to zero, then the secret data is embedded using the pseudo random number generator. More security is ensured in this technique due to scrambling.

Based on the scaling-up neighbor mean interpolation method , Jung *et al.* (2009) proposed a data hiding technique which used the values of neighborhood pixels to compute the mean value. This technique was proved to be better than the nearest neighbor and bilinear interpolation techniques. The technique ensured *PSNR* value of marked image versus original image to be always higher than 35 db as well as high hiding capacity of the existing algorithms.

Abadi *et al.* (2010) proposed another reversible data hiding technique which was based on the interpolation technique and histogram shifting. In this technique, interpolation error is computed to generate the histogram to embed the secret information. In this technique, due to prevent overflow and underflow only smaller location map which carry the information about preprocessing and postprocessing. This technique provides better visual quality with high hiding capacity.

Hong *et al.* (2010) proposed a reversible data hiding technique based on interpolation and detection of smooth and complex region in the cover image. According the local image activity, a binary image is generated that represent the locations of reference pixels. In complex region, only few pixels are used for hiding secret information. Prediction technique is used to reduce the reference pixel in smooth region which enhance the hiding capacity.

Luo *et al.* (2010) proposed an interpolation based reversible data hiding technique. In this technique, interpolation is used to compute the interpolation error. Using additive expansion of interpolation error i.e. embed '1' or '0' additively enhance the hiding capacity. This technique provides better visual quality with low computational cost.

Wang *et al.* (2013) proposed a reversible data hiding technique based on interpolation. In this technique, pixel of cover image divide into groups named as wall pixel and non wall pixel. The interpolation error is used for wall pixel to embed the secret information. While difference between non wall pixel and its parents pixel is used for hiding the secret information. Histogram shifting of difference is used to embed the secret information in the cover Image. This technique provides better image quality with high hiding capacity.

2.6 Vector Quantized Based Techniques

Lu *et al.* (2009) proposed a technique of reversible data hiding that used *VQ*-index (Vector Quantization) residual value coding. The proposed technique was divided into two steps : first, the process of *VQ* encoding to generate the *VQ*-index table and then second process is to hide the data to hide the secret message into the code stream. The core idea of the technique is to encode the cover image by using the index table, and after that, the secret data is hidden by using the relationship that exists between the mean values and the neighboring four indices of the current index. Lastly, the bit rate is reduced by encoding the difference of the indices by the proper bit stream.

Wang *et al.* (2009) proposed a lossless data hiding technique which uses the joint neighboring coding (*JNC*) of the *VQ* index table. This scheme first generates a *VQ* index table using the cover image. Then, with the help of the initial key and the secret data bits, various adjacent indices are chosen to present *JNC* for every index value and then the secret data is hidden there. Finally, on the basis of the minimal length principle a suitable output code stream is generated.

The data hiding techniques of multimedia enable the message senders to disguise the secret data by embedding the secret data into the cover media. Hence, transmitting the secret data is as simple as transmitting the cover media. In the past few years, many studies have been performed on reversible data hiding techniques on images. The existing techniques are able to retrieve the original cover image after the embedded secret data bits have been extracted from the stego image. A novel reversible steganographic technique had been proposed which uses the concept of side match and hide the secret data into the *VQ* compressed image by applying the concept of side match. Yang *et al.* (2011) proposed this method which uses extra information which is known as the hit pattern, to achieve the reversibility. In most of the cases the hiding of the entire bit pattern along with the secret data is enabled by using the small hit patterns. To improve the visual quality of the stego-image which has to be transmitted to the receiver side, the concept of partitioned codebooks (state codebooks) has been used in this technique. The embedding and extraction times are minimized with the help of the partition operation on the codebook by using a look-up table.

By utilizing the concept of the modified fast correlation *VQ (MFCVQ),* Yang *et al.* (2011) proposed another reversible data hiding technique which used *VQ*-index tables. A modified *MFCVQ*-based scheme had also been proposed, by this technique the hiding capacities have been improved as more than one bit is hidden into the *VQ* index, reducing the compressed bit rates after the concept of Huffman-code had been applied to it.

Qin *et al.* (2013) proposed a reversible data-hiding technique in which the index tables of the *VQ* compressed images were based on the mechanism of index mapping. At the sender's side, the *VQ* indices having zero occurrences along with those who have largest occurrence in the image index table are used to construct a series of index mappings. The indices in all the mappings have the length of the mapping bit number and they correspond to the binary representations. During the data embedding process the indices are substituted by the current subset of the secret bits to hide them. The same index mappings are retrieved and reconstructed at the receiver side to ensure the correctness of the extraction of the secret data and the index table is recovered losslessly.

Another novel lossless data hiding technique was proposed by Lee *et al.* (2013) which hides the secret data into the *VQ* compressed image to achieve data compression and secret communication simultaneously. The correlation among the neighboring blocks of a *VQ*-

compressed image is explored. It has been shown that the neighboring blocks of a *VQ*-compressed image usually have high mutual correlation. Hence, this scheme utilizes the neighboring indices which have been processed and compressed thereby producing specific sub-codebooks which are then used to encode and hide the data simultaneously. The encoded size of every index can be significantly reduced as the sizes of sub-codebooks are smaller than the original *VQ* codebook,. Hence, a large extra free space can be created and also the original *VQ*-compressed images can be perfectly recovered after data extraction.

Chang et al (2013) proposed a new index compression and reversible data hiding scheme based on the combination of the *SMVQ* (Kim, 1992) and *SOC* (Hsieh and Tsai, 1996) approaches to further improve the compression rate of the image.

In 2007, Chang *et al*. proposed another reversible data hiding technique to achieve secret communication. The secret data is hidden in the compressed codes of the cover image, but the technique has low hiding capacity and extra m bits are introduced so that original *VQ* can be reversed after the secret data are extracted. Instead of introducing m bits and utilising only one-third of the *VQ* indices of the cover image to hide the secret data, Tu *et al.* (2015) proposed a technique that used only one bit to distinguish between the indices of the two clusters. The indices of the cluster 1, 2 and 3, all can hide the secret data bits. The proposed scheme reduced the number of extra information bits thereby increasing the hiding capacity.

CHAPTER 3
MULTILEVEL REVERSIBLE DATA HIDING FOR DIGITAL IMAGES USING HISTOGRAM SHIFTING

3.1 Introduction

In this Chapter, a data hiding technique using histogram shifting is proposed. Histogram shifting creates space so that the secret data can be hidden. The shifting is done between the peak point and the zero points of the histogram that has been constructed of the image, hiding the data into the pixels corresponding to the maximum point. This technique is applied first to the cover image and then to the obtained stego images upto desired number of levels, thus increasing the hiding capacity of a cover image. This technique embeds high quantity of secret data and also maintains the visual quality of the stego images. Proposed technique is completely reversible as embedded data is extracted without any loss. It has been shown experimentally that the *PSNR* of the marked image versus the original image is maintained to be above 33 *d*B.

3.2 Multilevel Data Embedding Algorithm

The following technique has been proposed to enhance the hiding capacity of these reversible data hiding techniques which are based on histogram shifting. The data is embedded using the maximum and the minimum peak points [35] and is embedded in various levels.

For any given grayscale image, firstly its histogram is generated as shown in the figure.

Step 1: In the histogram constructed, a zero or minimum point and a maximum point are recorded. Zero or minimum point refers to the grayscale pixel value which are held by the minimum number of pixels in the cover image. Whereas the maximum point refers to the

grayscale pixel value which occurs maximum number of times in the image. The peak point determines the number of bits that can be embedded into the cover image.

Step 2: The complete cover image is scanned row by row and column by column and the values of the pixels between the maximum and minimum point are incremented or decremented by 1 depending whether the minimum point lies to the right or left of the maximum point respectively, leaving the grayscale value corresponding to the maximum number of pixels empty.

Step 3: The complete marked image is scanned again maintaining the same order. Whenever the pixf maximum point is encountered, the to-be embedded bit is verified. If the to-be embedded bit is '1' the pixel value is incremented by 1. Otherwise the pixel value remains the same.

Step 4: In this way when the data is hidden in the image, a stego image is obtained. The above algorithm can be repeated again on this obtained stego image about 4-5 times, thus enabling multilevel data hiding. In this way data hiding capacity of the image can be increased significantly maintain the *PSNR* above 36 *d*B.

DATA EMBEDDING PROPOSED PROCEDURE :

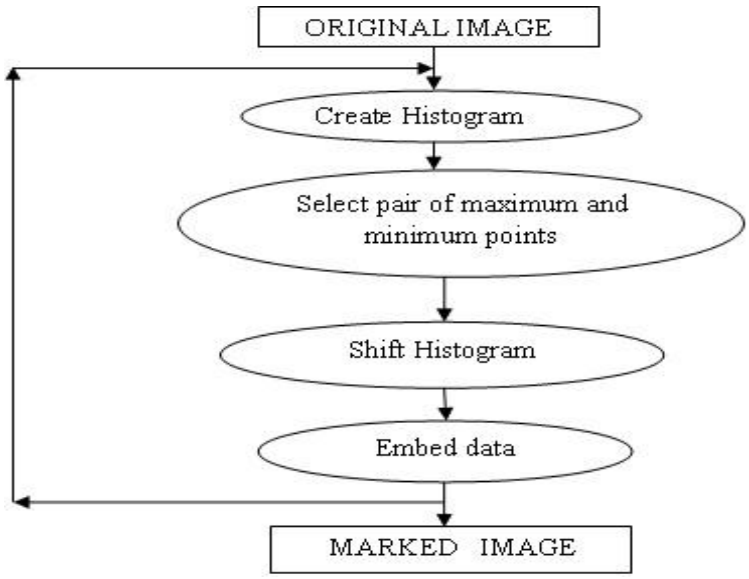


Figure 3.1. Flowchart of embedding procedure

3.3 Multilevel Data extraction algorithm

The marked image is received at the receiver side in which data has been embedded at the sender's side with the help of the histogram shifting. The extraction algorithm should extract data as well as the cover media without any distortion. Let us assume the grayscale value of the maximum points zero points of the last level are m and n respectively. The marked image is of size M × N, each pixel grayscale value x Є [0,255].

Step 1: Scan the marked image in the same sequential order which was used at the time of embedding. If the pixel with a grayscale value m+1 is encountered, bit "1" is extracted and if the pixel with grayscale value m is encountered, a bit "0" is extracted.

Step 2: Scan the image in the sequential order, if any pixel whose grayscale value belongs to (a,b] , subtract it by 1.

Step 3: If there is some overhead information extracted along with the secret data, set the value of the pixel grayscale to n.

Step 4: This algorithm is repeated for all the number of levels till all the data is extracted and the cover media is obtained.

The original image is recovered from the marked image without any distortion.

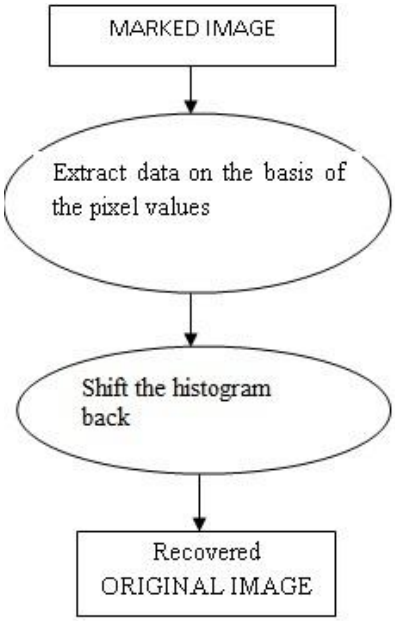


Figure 3.2 Flowchart of extraction procedure

3.4 Experimental Results

Proposed data hiding technique is implemented in MATLAB. For this, several different images has been taken. Secret data of different capacity is embedded into these images. *PSNR* of the marked image v/s the cover image is calculated to evaluate the performance of the proposed technique using the expression explained before.

PSNR and hiding capacity of various images are shown in Table 3.1 and Table 3.2, respectively.

Table 3.1: *PSNR* of different images at various levels

IMAGE	(LEVEL1)	(LEVEL2)	(LEVEL3)	(LEVEL4)	(LEVEL5)
Lena	47.4067	41.5302	38.1102	35.6409	33.7944
Boat	45.6564	40.1416	35.2072	31.8357	29.3836
Pepper	40.4472	34.5451	31.1356	28.7462	26.9155
Truck	41.4148	35.6399	32.1601	29.6300	27.6690
Baboon	43.6560	37.7649	33.0225	30.0337	27.8483
Barbara	41.4692	35.5625	32.1488	29.7587	27.9279
Jet	42.0055	36.1227	32.7323	29.8767	27.7742

Table 3.2: Hiding Capacity of different images at various levels

IMAGE	(LEVEL1)	(LEVEL2)	(LEVEL3)	(LEVEL4)	(LEVEL5)
Lena	5421	10377	15281	19594	24764
Boat	10575	21957	23042	27518	30974
Pepper	3078	6062	8194	10206	12208
Truck	14949	28263	40386	51560	61656
Baboon	2769	5515	8237	10956	13659
Barbara	5522	10605	17362	22726	29094
Jet	13329	24428	33222	33275	33310

From these tables, one can infer that by increasing the number of levels, data hiding capacity has been increased by a remarkable amount. From table 3.2 it can be observed that the *PSNR* decreases as the number of hiding levels increase. But the visual distortion is still quite small thereby maintaining the visual quality of the marked image as shown in the Fig. 3.3. Fig. 3.3 (e) and (f) are the histograms of the marked lena and pepper image respectively. From the histogram it can be seen that the data has been hidden in the maximum points of the image.

Fig. 3.3 (a)

Fig. 3.3 (b)

Fig. 3.3 (c)

Fig. 3.3 (d)

Fig.3.3 (a) Lena Image (b) Marked Lena Image (c) Pepper Image (d) Marked Pepper Image

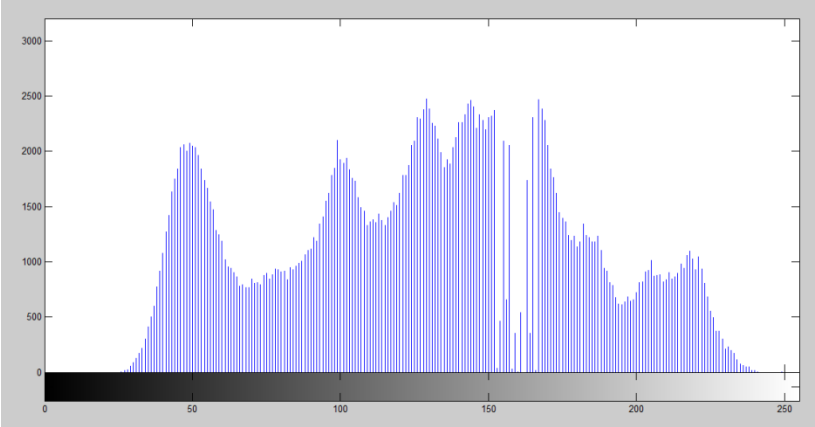


Fig. 3.3 (e) Histogram of Marked Lena image

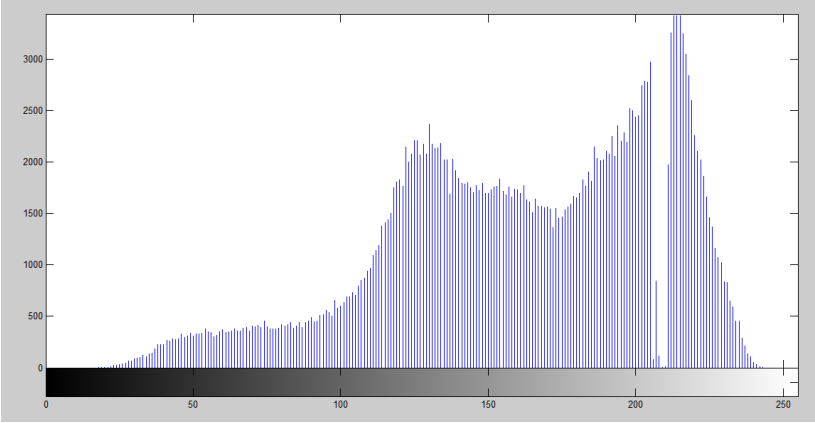


Fig. 3.3 (f) Histogram of Marked Pepper image

3.5 Conclusion

The proposed multilevel reversible data hiding technique can embed data equal to the number of pixels corresponding to the maximum point of the cover image and also guarantees the *PSNR* of the marked image versus the original image to be above 36 dB. The algorithm has been applied to various images.

CHAPTER 4
HISTOGRAM BASED MULTILEVEL REVERSIBLE DATA HIDING TECHNIQUE USING SIMPLE AND ABSOLUTE DIFFERENCE IMAGES

4.1 Introduction

In this Chapter, a multilevel reversible data hiding technique based on the blocks of difference image is proposed. In this technique, the cover image is divided into non overlapping blocks of equal size and then simple and absolute differences of each block are evaluated. After it, histogram of each absolute difference block is generated and peak negative points of simple difference are replaced into absolute difference blocks at respective positions. Then peak positive and peak negative points of each difference block are used to hide the secret data. Numbers of bits hidden into each positive peak points is one bit only but in negative peak points, more than a bits are hidden that increases the hiding capacity of a cover image. Proposed technique achieves high hiding capacity than existing reversible data hiding techniques while keeping distortion in the marked image low. To prove its validity, the proposed technique is compared with the other existing reversible hiding techniques.

4.2 Data Embedding Algorithm

Firstly, a simple difference image *SD* and absolute difference *D* of the given cover image are generated. This difference image *SD* contains both positive and negative values. Then the histogram of the difference image *SD* is generated and set of peak points P_b are recorded for every block *b* of the difference image. This set P_b consists of both positive and negative peak values. Except negative peak points, rest all the grayscale values are taken as absolute values in

the image. All pixels of the block having values greater than P_b are shifted by 2 to create space for hiding secret data. Position P_b+1 will be occupied by positive peak points to embed secret data and P_b+2 values will be used by negative peak points to embed secret data.

Data Embedding Algorithm

Input: Original Cover Image *H*.

Output: Marked image *S*.

Step 1: Divide the original cover image into blocks of size*A*×*B*.

Generate a simple difference image SD_b(i,j) of size *A*×(*B*-1) of every block *b* with the help of the the formula:

$$SD_b(i,j) = H_b(i,j) - H_b(i,j+1) \quad (4.1)$$

for 0 ≤ i≤ P− 1, 0 ≤ j ≤ Q− 2,

Generate absolute difference image $D_b(i,j)$ of size *A*×(*B*-1) of every block *b* with the help of the the formula:

$$D_b(i,j) = |SD_b(i,j)| \quad (4.2)$$

for 0 ≤ i≤ P− 1, 0 ≤ j ≤ Q− 2,

Step 2: Generate the histogram of the difference image D_b and record the peak point P_b for each block. Copy all the peak pixel values from SD_b to D_b so that now D_b consists of all absolute values except those peak values which have negative difference values in SD_b image.

Step 3: If the pixel value $D_b(i, j)$ of block *b* is larger than the peak point P_b of block *b*, modify the pixel value $D_b(i, j)$ of block *b* to $D_b(i, j)$+2. Else, the pixel value $D_b(i, j)$ remains unchanged. The modification is done on the basis of the principle which is as follows:

$$D'_b(i,j) = \begin{cases} D_b(i,j) + 2 & if\ D_b(i,j) < 0 \\ D_b & otherwise \end{cases} \quad (4.3)$$

for 0 ≤ *i*≤ *A* − 1, 0 ≤ *j* ≤ *B* − 2, and 0 ≤ *b* ≤ ((*M* × *N*) / (*A*×*B*)) - *1*

Step 4: In the modified difference image D_b, the secret data bit m is hidden in the the pixels which have grayscale values equal to the peak point P_b . The modification is done as follows:

$$D''_b(i,j) = \begin{cases} D'_b(i,j) + m, & if\ D'_b(i,j) = P_b \\ |D'_b(i,j)| + 2 & if\ D'_b(i,j) = -P_b \\ D'_b(i,j) & otherwise \end{cases} \quad (4.4)$$

SI(k) = m if $D'_b(i, j) = -P_b$

for $0 \le i \le A-1$, $0 \le j \le B-2$, and $0 \le b \le ((M \times N) / (A \times B)) - 1$

and $m \in \{0, 1\}$.

Step 5: The marked image is constructed by performing the following inverse transformation T^{-1}, using the original cover image and its modified difference image. For the first two pixels of every row, the inverse operation is expressed as

$$S_b(i,0) = \begin{cases} H_b(i,0) & if\ H_b(i,0) < H_b(i,1) \\ H_b(i,1) + D''_b(i,0) & otherwise \end{cases} \quad (4.5)$$

$$S_b(i,1) = \begin{cases} H_b(i,0) + D''_b(i,0) & if\ H_b(i,0) > H_b(i,1) \\ H_b(i,1) & otherwise \end{cases} \quad (4.6)$$

for $0 \le i \le A-1$, $0 \le b \le ((M \times N) / (A \times B)) - 1$

For other remaining pixels, the inverse operation is defined as

$$S_b(i,j) = \begin{cases} S_b(i,j) + D''_b(i,j-1) & if\ H_b(i,j-1) \le H_b(i,j) \\ S_b(i,j-1) - D''_b(i,j-1) & otherwise \end{cases} \quad (4.7)$$

for $0 \leq i \leq A-1$, $2 \leq j \leq B-2$, and $0 \leq b \leq ((M \times N) / (A \times B)) - 1$

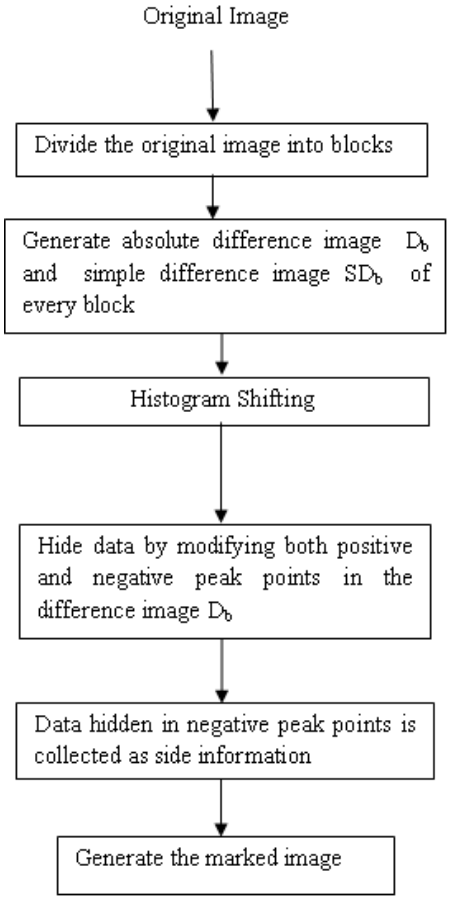


Figure 4.1: Flow chart of data embedding procedure used in proposed technique

4.3 Data Extraction Algorithm

In the data extraction process, the hidden message is extracted and the marked image is restored to its original image. The basic steps for this procedure are given in Figure 3 and are depicted in the following algorithm.

Input: Marked Image S.

Output: Original image H and secret data.

Step 1: Divide the received marked image into blocks $A \times B$ in size.

Generate the difference image $RD_b(i,j)$ of each block from the received marked image by using the formula:

$$RD_b(i,j) = |S_b(i,j) - S_b(i,j+1)| \quad (4.8)$$

for $0 \leq i \leq A - 1$, $0 \leq j \leq B - 2$,

Step 2: Traverse the pixel values of the difference image generated in Step 1 and extract the hidden data from the the difference image $RD_b(i,j)$ of block b by using the following formula:

$$m = \begin{cases} 0, & if\ RD_b(i,j) = P_b \\ 1, & if\ RD_b(i,j) = P_b + 1 \\ SD(k), & if\ RD_b(i,j) = P_b + 1 \end{cases} \quad (4.9)$$

for $0 \le i \le A-1$, $0 \le j \le B-2$,

where P_b is the received peak point of block b. We first scan the entire difference image of block b. For block b, if the pixel value P_b is encountered, bit 0 is retrieved. If the pixel with (P_b+1) is encountered, bit 1 is retrieved. If the pixel with (P_b+2) is encountered, the 8 bits of the next byte is retrieved from the side information.

Step 3: The hidden message is extracted from the difference image $RD_b(i, j)$ for block b by using the following formula :

$$RD'_b = \begin{cases} RD_b(i,j) - 1, & if\ RD_b(i,j) = P_b + 1 \\ RD_b(i,j), & if\ RD_b(i,j) = P_b \\ -(|RD_b(i,j) - 2|), & if\ RD_b(i,j) = P_b + 2 \end{cases} \quad (4.10)$$

for $0 \le i \le A-1$, $0 \le j \le B-2$, and $0 \le b \le ((M \times N) / (A \times B)) - 1$

where P_b is the peak point of block b.

Step 4: Some pixel values of the difference image $RD'_b(i, j)$ are shifted to obtain the reconstructed original difference image $RD''_b(i, j)$ on the basis of :

$$RD''_b(i,j) = \begin{cases} RD'_b(i,j) - 2, & if\ RD_b(i,j) > P_b + 1 \\ RD'_b(i,j), & otherwise \end{cases} \quad (4.11)$$

for $0 \le i \le A-1$, $0 \le j \le B-2$, and $0 \le b \le ((M \times N) / (A \times B)) - 1$

where P_b is the peak point of block b.

Step 5: Finally obtain the recovered original image $RH_b(i, j)$ by performing the inverse transformation T^{-1}. Similar to step 5 in the hiding phase, for the first two pixels of every row the inverse operation is expressed as

$$RH_b(i,0) = \begin{cases} S_b(i,0) & if\ S_b(i,0) < S_b(i,1) \\ S_b(i,1) + RD"_b(i,0) & otherwise \end{cases} \quad (4.12)$$

$$RH_b(i,1) = \begin{cases} S_b(i,0) + RD"_b(i,0), & if\ S_b(i,0) \le S_b(i,1) \\ S_b(i,1), & otherwise \end{cases} \quad (4.13)$$

for $0 \le i \le A - 1$, $0 \le b \le ((M \times N) / (A \times B)) - 1$

For any residual pixels, the corresponding inverse operation is defined as

$$RH_b(i,j) = \begin{cases} RH_b(i,j-1) + RD"_b(i,j-1), & if\ S_b(i,j-1) \le S_b(i,j) \\ RH_b(i,j-1) - RD"_b(i,j-1), & otherwise \end{cases} \quad (4.14)$$

for $0 \le i \le A - 1$, $2 \le j \le B - 2$, and $0 \le b \le ((M \times N) / (A \times B)) - 1$

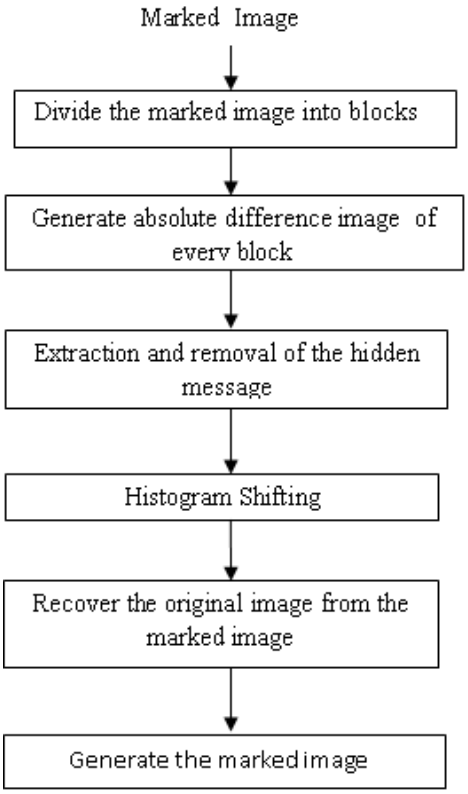


Figure 4.2: Flowchart of data extraction procedure used in proposed technique

Proposed technique is elaborated using an example of a 4×4 block of Lena image, shown in following fig.:

162	156	163	160
161	159	158	159
160	161	159	155
158	158	156	157

(a) Original Cover Data

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

(b) Secret Data

6	-7	3
2	1	-1
-1	2	4
0	2	-1

(c) Simple difference Image

6	7	3
2	1	1
1	2	4
0	2	1

(d) Absolute Difference Image

6	7	3
2	1	-1
-1	2	4
0	2	-1

(e) Simple difference image copied to difference image

8	9	5
4	1	-1
-1	4	6
0	4	-1

(f) Difference Image after Shifting

8	9	5
4	1	3
3	4	6
0	4	3

(g) Data embedded in the difference Image

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

(h) Data embedded in negative targets as Side Information

164	156	165	158
163	159	158	161
160	164	160	154
158	158	154	157

(i) Marked Image

Figure 4.3 **:** Example showing embedding of the secret data in 4 × 4 block of Lena image

164	156	165	158
163	159	158	161
160	164	160	154
158	158	154	157

(a) Marked image

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

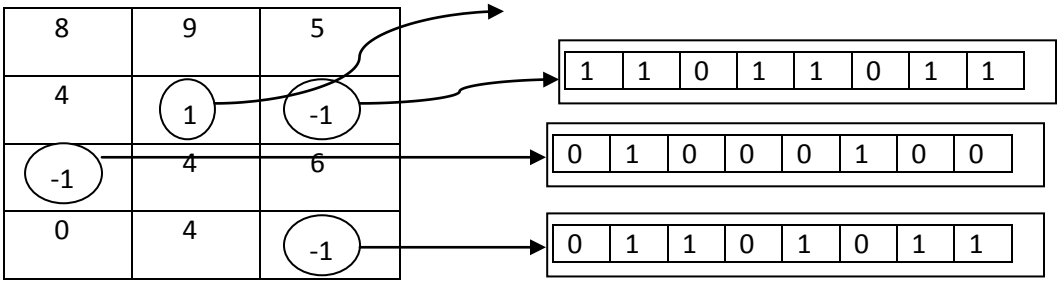
(b) Side Information

8	9	5
4	1	3
3	4	6
0	4	3

(c) Difference image of the marked image

8	9	5
4	1	-1
-1	4	6
0	4	-1

(d) Replace all (peak value + 2) values by (- peak value)



(e) Data extracted from every target value (both +ve and –ve)

8	9	5
4	1	1
1	4	6
0	4	1

(f) all –ve peak values are replaced by their absolute values

6	7	3
2	1	1
1	2	4
0	2	1

(g) Shifting back the values greater than peak value

162	156	163	160
161	159	158	159
160	161	159	155
158	158	156	157

(h) Recovered Original Image

Figure 4.4: Example showing the extraction process used in proposed technique

4. 4 Results and Discussion

This section discusses the experimental results of embedding and extracting of secret image in different cover images considered in this work.

Experimental Results

Proposed technique is implemented using *MATLAB*. Five standard grayscale images, from complex to smooth, were selected as the testing images in the resolution of 512×512 pixels as shown in the fig. In this experiment, a random binary image is taken as secret data.

In Figure 4.6, it has been shown that *PSNR* values for an image are better for 4×4 block size as compared to higher block size. For this, different amount of secret data is embedded into each of

the image and then *PSNR* is calculated between cover image and its marked version. A graph is then plot for each of these images at different capacity and different block size.

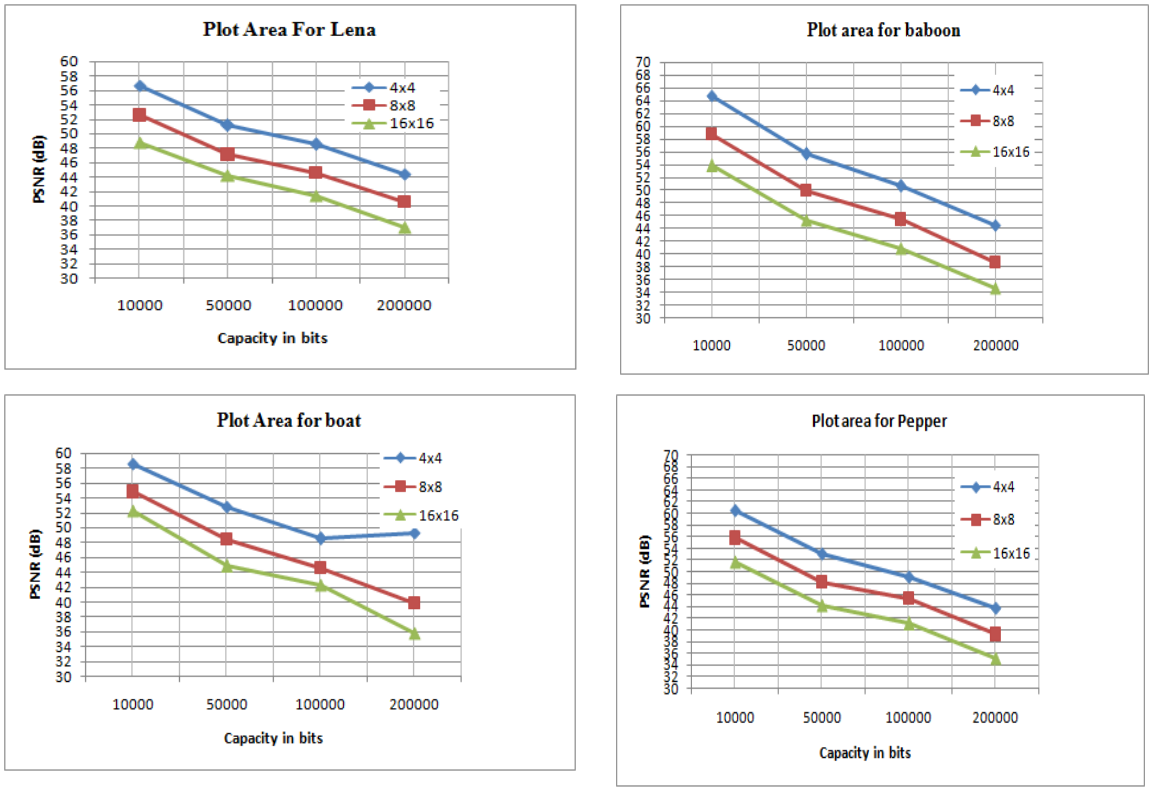


Figure 4.5: *PSNR* vs capacity comparison for different images at different block size.

Table 4.1 contains *PSNR*, *PSNR HVS*, hiding capacity and side information for different images considered in this proposed work. Different levels of embedding are performed on each image to show the effectiveness of the proposed technique. This data is for block size of 4×4.

Figure 4.6: (a)-(e) Original cover images; (f)-(j) Marked images after hiding 1,00,000 bits; (k) – (o): Marked image after hiding 5,00,000 bits (p)-(t): Marked image after hiding 10,00,000 bits.

Table 4.1: *PSNR* (in dB),*PSNR HVS* (in dB),Hiding Capacities (bits) and side information at various levels for different images

Levels	1	2	3	4	5	6	9	12	18
Lena									
PSNR	45.7	41.19	38.08	35.88	34.23	32.92	29.98	27.98	25.35
PSNR HVS	47.5	42.74	38.79	36.13	33.89	32.15	28.11	25.31	21.39
Data Embedded	126930	269690	409383	562149	713237	872790	1349830	1839126	2819354
Side Information	12960	27973	42697	59136	75482	93021	145947	201348	314729
Baboon									
PSNR	45.79	40.68	37.5	35.4	33.82	32.55	29.8	27.93	25.48

PSNR HVS	54.32	47.68	43.09	39.87	37.26	35.2	30.66	27.56	23.36
Data Embedded	65835	146148	232586	324947	421084	521438	836677	1169615	1859948
Side Information	6024	13978	22676	32139	42076	52576	86070	122310	198994
Boat									
PSNR	46.82	42.12	39.11	36.98	35.35	34.07	31.22	29.25	26.53
PSNR HVS	50.83	45.33	41.26	38.53	36.25	34.47	30.32	27.4	23.3
Data Embedded	87417	190155	294515	406467	520166	639446	100188	1376904	2140151
Side Information	8228	18477	28957	40445	52194	64649	103208	144108	229724
Jet									
PSNR	44.97	41.12	38.02	36.03	34.27	32.99	29.96	27.97	25.29
PSNR HVS	46.06	43.10	38.86	36.52	34.06	32.47	28.25	25.45	21.44
Data Embedded	149867	311953	453321	618627	774487	949302	1456467	1989956	3053175
Side Information	15323	32327	46978	64856	81768	101325	158770	220750	346594
Pepper									
PSNR	46.12	41.5	38.66	36.69	35.16	33.93	31.23	29.34	26.79
PSNR HVS	50.76	44.46	40.49	37.81	35.73	34.06	30.29	27.57	23.69
Data Embedded	85143	186624	293991	408745	526398	647864	1020511	1403219	2179261
Side Information	8059	18334	29393	41437	53889	66919	107428	150142	238839
Aerial									
PSNR	46.03	41.64	38.52	36.44	34.70	33.38	30.26	28.27	26.77
PSNR HVS	49.65	45.60	40.85	37.99	35.30	33.40	28.89	25.91	23.59
Data Embedded	109393	236821	353130	486450	614483	756298	1169855	1607692	2037508
Side Information	10893	24046	35881	49915	63373	78646	123600	172480	221164
Airfield									
PSNR	45.92	41.95	38.72	36.91	35.19	34.04	31.14	29.26	26.63
PSNR HVS	49.07	46.01	40.69	38.59	35.87	34.40	30.02	27.25	23.13
Data Embedded	63344	167545	255603	368599	463655	582118	907362	1263177	1971652
Side Information	5800	16840	25907	38118	48090	61016	96342	135931	216029
Barbara									
PSNR	44.74	41.22	37.62	35.78	33.83	32.68	29.63	27.75	25.15
PSNR HVS	44.05	42.50	37.56	35.77	33.01	31.68	27.42	24.82	20.95
Data Embedded	127197	303431	440326	622411	767809	957419	1451617	1997331	3056070
Side Information	12905	31908	46101	66130	81634	102809	157586	219811	342332
Bridge									
PSNR	43.57	40.52	37.79	36.16	34.39	33.29	30.27	28.39	25.69
PSNR HVS	44.11	42.29	38.16	36.54	33.64	32.31	27.79	25.12	21.02
Data Embedded	122631	299216	404963	587637	681648	866850	1229466	1683369	2478565
Side Information	122403	32592	44049	65415	75584	97295	138776	192181	286166
Clown									

PSNR	41.65	40.64	36.30	35.46	33.00	32.42	29.01	27.54	24.93
PSNR HVS	39.25	40.01	34.05	33.81	30.45	30.08	25.64	23.58	19.80
Data Embedded	77946	355997	446399	724577	818718	1096867	1567200	2222385	3352260
Side Information	7782	40982	50904	84333	94827	128373	183654	262321	398112
Couple									
PSNR	45.95	41.50	38.52	36.47	34.80	33.48	30.49	28.48	25.81
PSNR HVS	49.43	44.49	40.44	37.60	35.15	33.28	28.93	26.00	21.93
Data Embedded	93744	214830	324042	451183	569224	703125	1091868	1502795	2326932
Side Information	9119	21737	32979	46505	58950	73467	115973	162073	256910
Crowd									
PSNR	43.42	41.15	37.34	35.83	33.73	32.72	29.49	27.63	24.94
PSNR HVS	41.96	41.85	36.07	34.80	31.70	30.66	26.21	23.73	19.82
Data Embedded	92309	310629	418425	632710	746433	965577	1422760	1987875	3019137
Side Information	9098	33603	44571	68863	80664	1056714	156172	220899	339728
Girlface									
PSNR	43.29	40.01	36.68	34.88	32.98	31.80	28.77	26.85	24.25
PSNR HVS	44.35	42.24	37.64	35.64	33.10	31.66	27.47	24.79	20.85
Data Embedded	137813	304083	434838	601436	745230	918206	1390136	1893004	2879363
Side Information	13570	30821	43931	61758	76982	96056	148364	205799	321444
Sailboat									
PSNR	46.10	41.42	38.53	36.56	35.00	33.76	31.01	29.13	26.58
PSNR HVS	51.44	45.42	41.24	38.58	36.25	34.49	30.47	27.66	23.65
Data Embedded	83906	183097	287212	399194	513425	631729	995676	1372079	2135456
Side Information	7929	17911	28570	40279	52320	64899	104168	145603	231571
Tank									
PSNR	43.79	40.07	36.87	34.72	32.79	31.31	28.13	26.21	23.68
PSNR HVS	46.66	42.98	38.47	35.93	33.48	31.78	27.60	24.80	20.84
Data Embedded	100106	227415	336678	459992	571772	698023	1053105	1424559	2157712
Side Information	9936	23744	35475	48998	61155	75213	114996	157441	242844

In this table, levels means the number of round, the proposed hiding technique undergoes. From this table, one can infer that the hiding capacity of the proposed technique is very large. As it can be seen from this table, the proposed hiding technique is able to hide more than 8 bits per pixel (bpp) with allowable distortion after performing 18 levels. Also, as the number of hiding levels increase, hiding capacity of each images increase, but *PSNR* and *PSNR HVS* decreases. The main reason is that hiding a large amount of secret data produces larger distortion in the pixels of the marked images. That is, higher embedding yields higher *MSE* and hence lower *PSNR* values. So there is a tradeoff between imperceptibility and hiding capacity of a data hiding technique.

Proposed technique is also compared with state of art reversible data hiding technique. For this comparison, maximum possible embeddable amount of data is hidden into cover images using proposed technique and existing techniques to generate marked images. Then *PSNR* between cover image and its marked version is calculated using proposed technique and existing techniques. This comparison is summarized in Table 4.2. In Table 4.2 $PSNR^1$ refers to the *PSNR* of the corresponding technique and $PSNR^2$ refers to the *PSNR* of the proposed technique with tha same capacity.

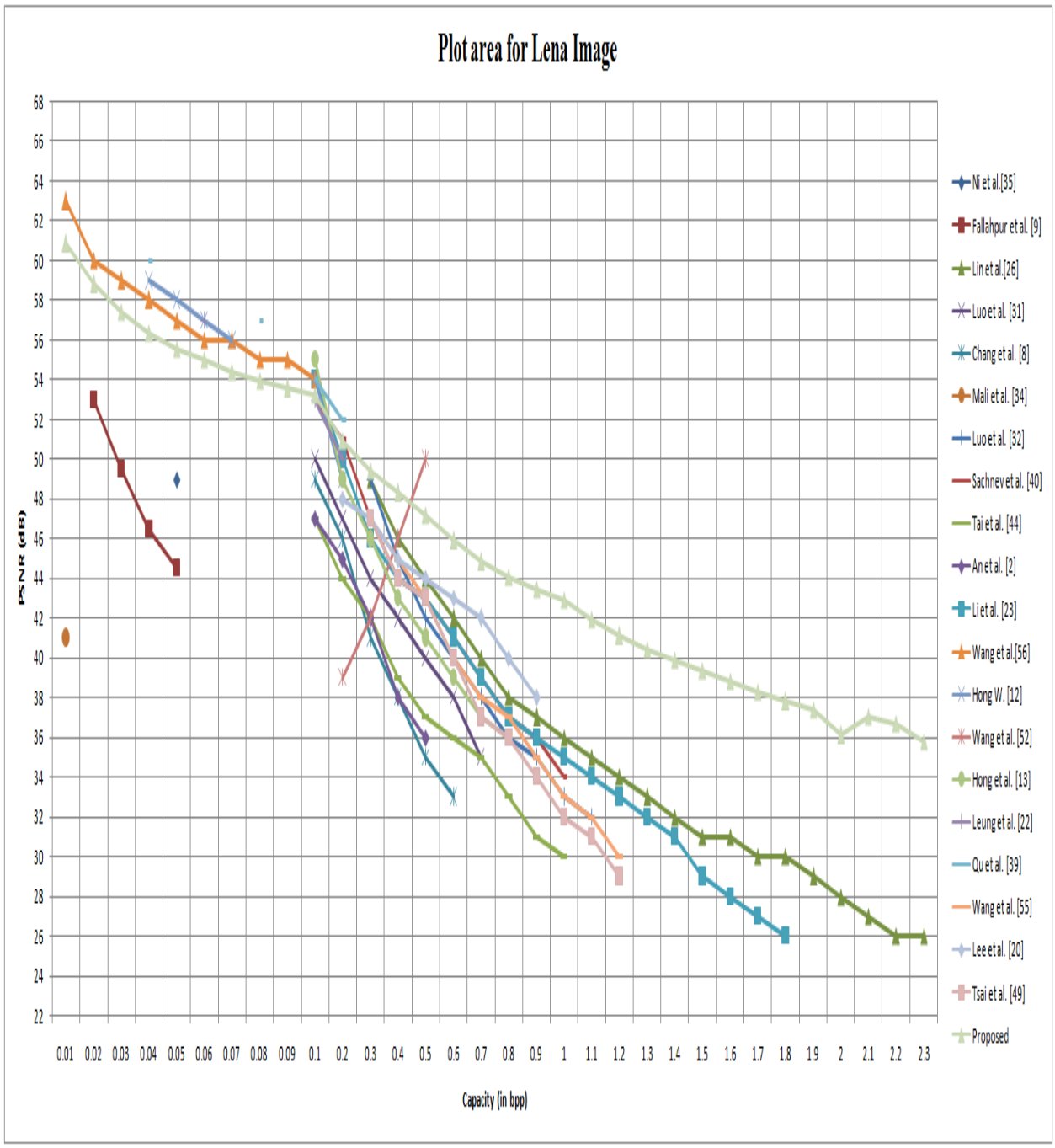
Table 4.2: Capacity (in bits) and *PSNR(d*B*)* comparison of proposed technique with existing techniques

Image ⟶	**Lena**		**Airplane**		**Boat**		**Baboon**	
Technique	**Capacity**	***PSNR*^{1}/ *PSNR*^{2}**	**Capacity**	***PSNR*^{1}/ *PSNR*^{2}**	**Capacity**	***PSNR*^{1}/ *PSNR*^{2}**	**Capacity**	***PSNR*^{1}/ *PSNR*^{2}**
Ni*et al* [43]	5460	48.2/ 59.95	16171	48.30/ 54.90	7301	48.2/ 58.42	5421	48.2/ 55.54
Fallahpour *et al.* [9]	13868	47.29/ 56.01	29250	48.56/ 52.51	15579	46.73/ 54.81	7874	47.12/ 54.02
Kuo*et al.*[31]	33931	48.73/ 51.72	50920	49.15/ 50.31	40379	48.81/ 50.11	12909	48.46/ 51.91
Lin *et al.*[52]	65394	48.67/ 58.68	69941	48.67/ 50.31	56713	48.67/ 48.59	38465	48.67/ 47.96
Tsai *et al.* [48]	47912	49.06/ 50.13	64996	49.24/ 49.34	-	-	15820	48.73/ 51.22
Luo *et al.*[31]	29813	48.68/ 52.35	44786	48.83/ 50.83	-	-	9522	48.50/ 53.07
Chang *et al.* [18]	45038	48.98/ 50.40	65698	49.54/ 49.30	46425	49.01/ 49.42	14361	48.38/ 51.55
Mali *et al*. [34]	14357	41.72/ 55.89	-	-	21063	41.08/ 53.41	40075	39.67/ 47.81
Luo *et al*. [55]	71674	48.82/ 48.28	84050	48.94/ 48.00	38734	48.50/ 50.32	22696	48.36/ 49.91
Sachnev*et al*. [40]	20000	55.06/ 54.33	20000	57.33/ 53.97	20000	52.68/ 53.65	20000	49.42/ 50.37
Tai *et al*. [49]	22377	48.32/ 53.68	45472	48.53/ 50.75	25412	48.35/ 52.48	-	-
Kim *et al.*	52428	47.05/	52428	51.00/	-	-	-	-

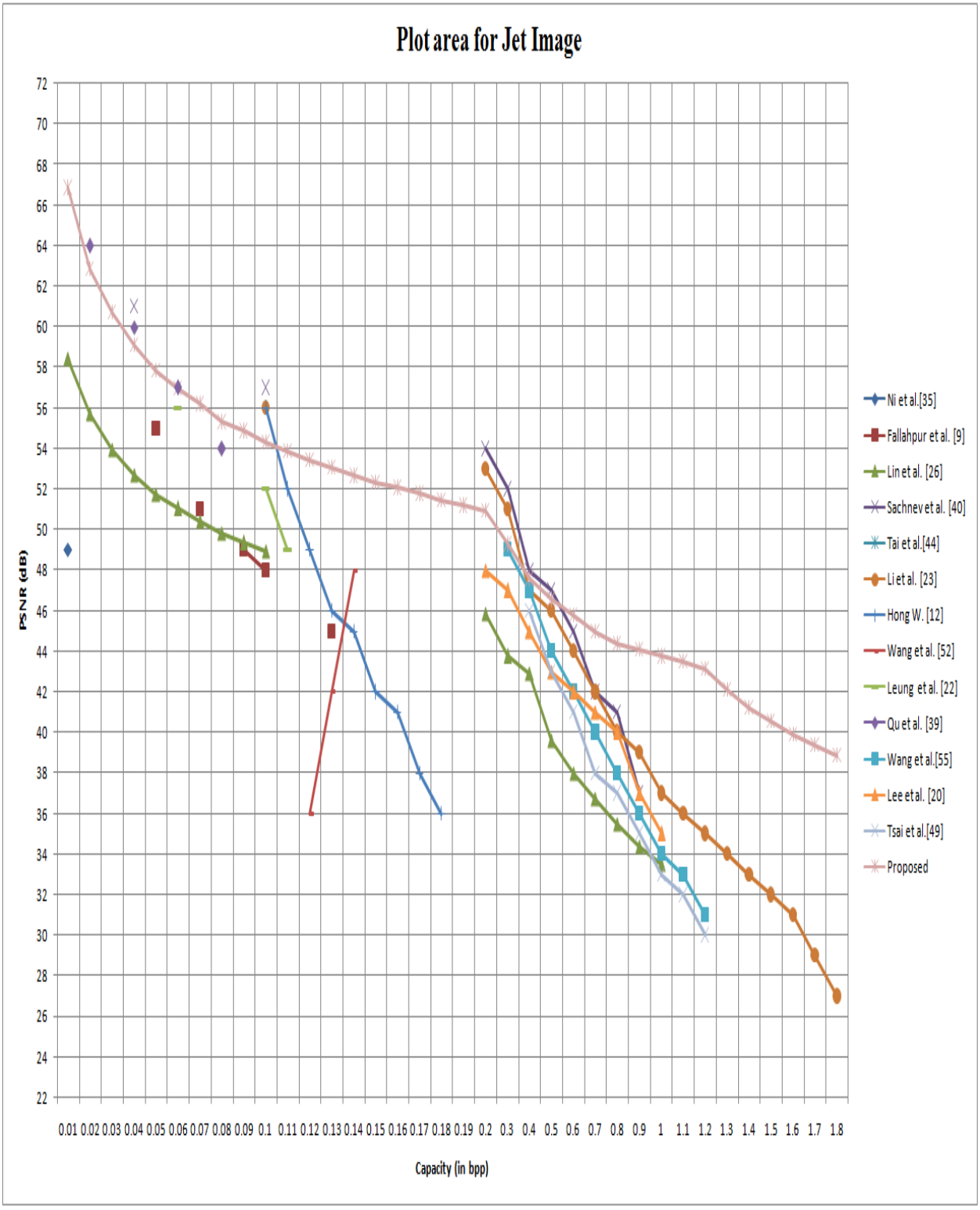
[52]		49.74		50.20				
An *et al.* [57]	3900	34.72/ 61.38	-	-	-	-	-	-
Li *et al.* [23]	60000	46.00/ 49.10	60000	49.00/ 49.67	-	-	40000	31.50/ 47.81
Wien Hong [18]	53112	48.54/ 49.66	79061	48.54/ 48.31	32622	48.54/ 51.19	17224	48.54/ 50.91
Liao *et al.* [52]	26214	47.81/ 52.94	-	-	-	-	-	-
Wien *et al.*[43]	53112	48.62/ 49.66	79061	48.87/ 48.31	32622	48.43/ 51.19	17224	48.30/ 50.19
Leung *et al.*[49]	56129	48.72/ 49.40	57314	48.74/ 49.86	-	-	-	-
Qu *et al.* [55]	10000	60.3/ 57.47	-	-	10000	58.4/ 57.95	10000	54.2/ 53.87
Peng *et al* [41]	10000	60.40/ 57.47	10000	62.96/ 56.85	-	-	10000	53.55/ 52.87
Tsai *et al.* [49]	73555	47.00/ 48.16	83690	47.54/ 47.98	67773	47.11/ 47.94	22191	47.08/ 49.98
Lee *et al.* [55]	155240	42.87/ 44.57	156993	41.98/ 44.65	144747	40.64/ 43.5	100345	39.34/ 42.67
Wang *et al al* [55]	63491	48.8/ 48.8	80634	49.03/ 48.21	-	-	23503	48.66/ 49.79

From this comparison, one can infer that at maximum hiding capacity,proposed technique provides better *PSNR* than existing reversible techniques except Qu *et al.* [39] technique. But hiding capacity of proposed technique is significantly larger than existing techniques.

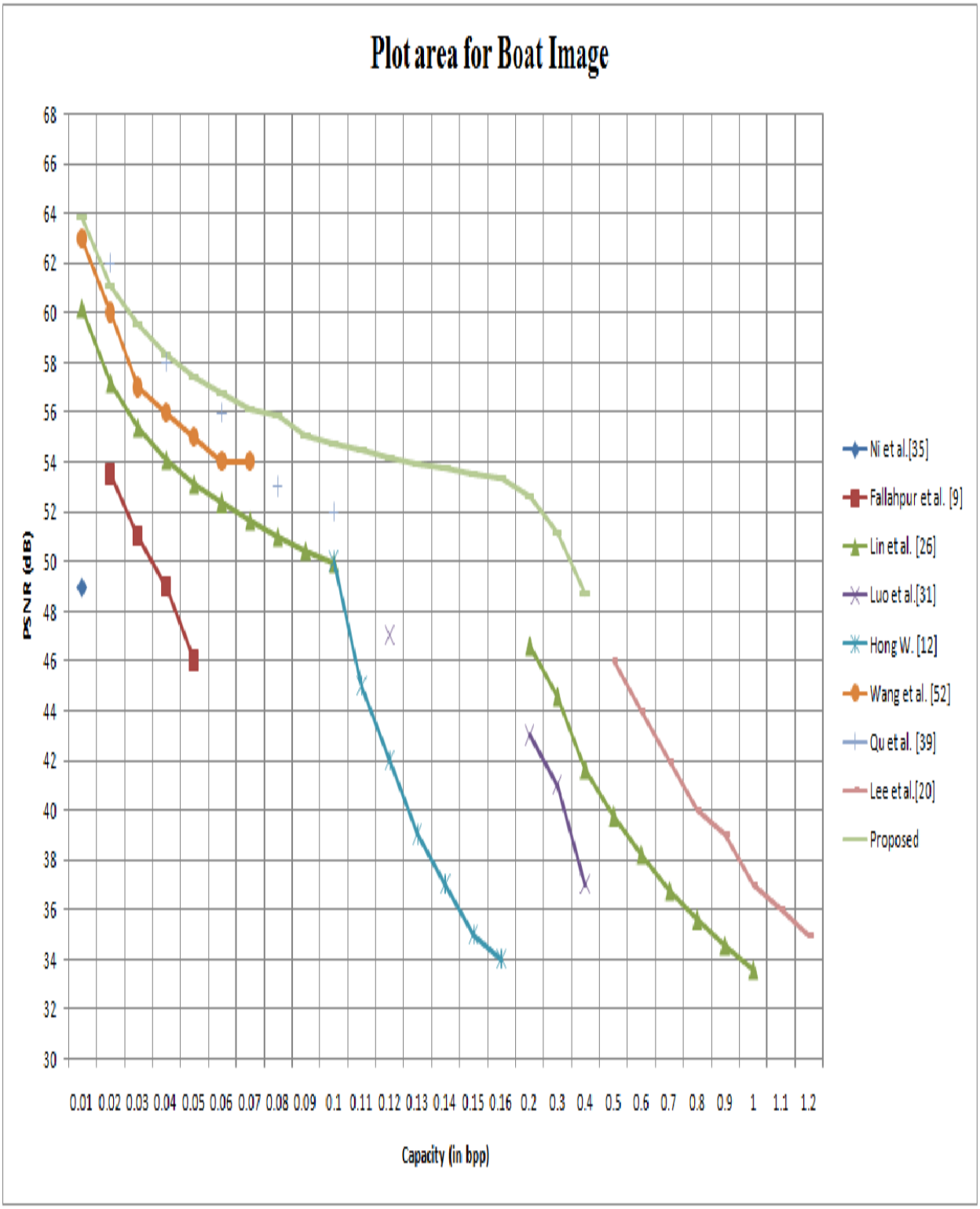
Proposed technique is also compared with existing techniques at different hiding capacity. This comparison is shown in Figure 4.7.


Plot area for Lena Image
PSNR (dB)
Capacity (in bpp)
Ni et al.[35]
Fallahpur et al. [9]
Lin et al.[26]
Luo et al. [31]
Chang et al. [8]
Mali et al. [34]
Luo et al. [32]
Sachnev et al. [40]
Tai et al. [44]
An et al. [2]
Li et al. [23]
Wang et al.[56]
Hong W. [12]
Wang et al. [52]
Hong et al. [13]
Leung et al. [22]
Qu et al. [39]
Wang et al. [55]
Lee et al. [20]
Tsai et al. [49]
Proposed

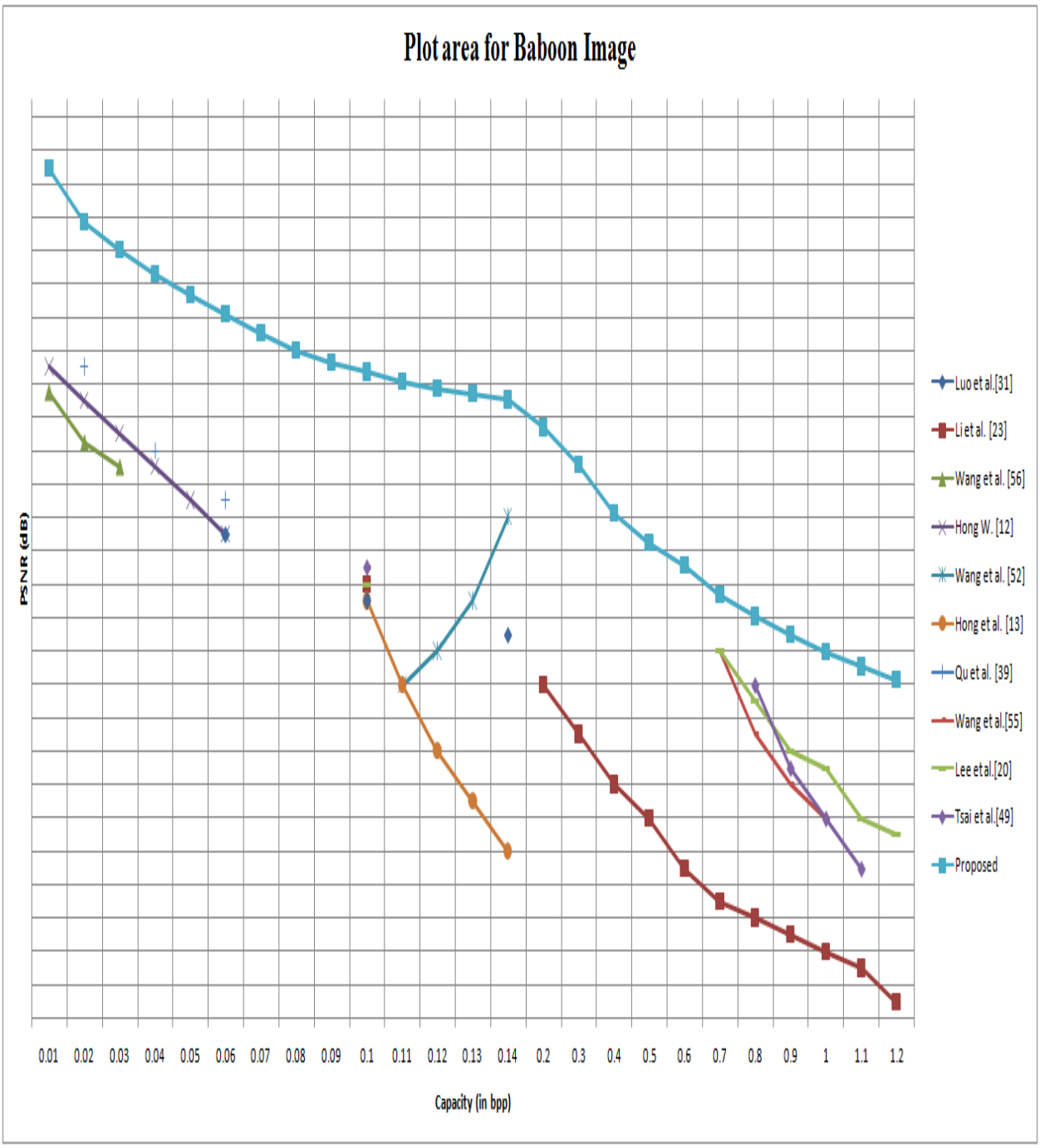
(a)


Plot area for Jet Image
PSNR (dB)
Capacity (in bpp)
Ni et al.[35]
Fallahpur et al. [9]
Lin et al. [26]
Sachnev et al. [40]
Tai et al.[44]
Li et al. [23]
Hong W. [12]
Wang et al. [52]
Leung et al. [22]
Qu et al. [39]
Wang et al.[55]
Lee et al. [20]
Tsai et al.[49]
Proposed

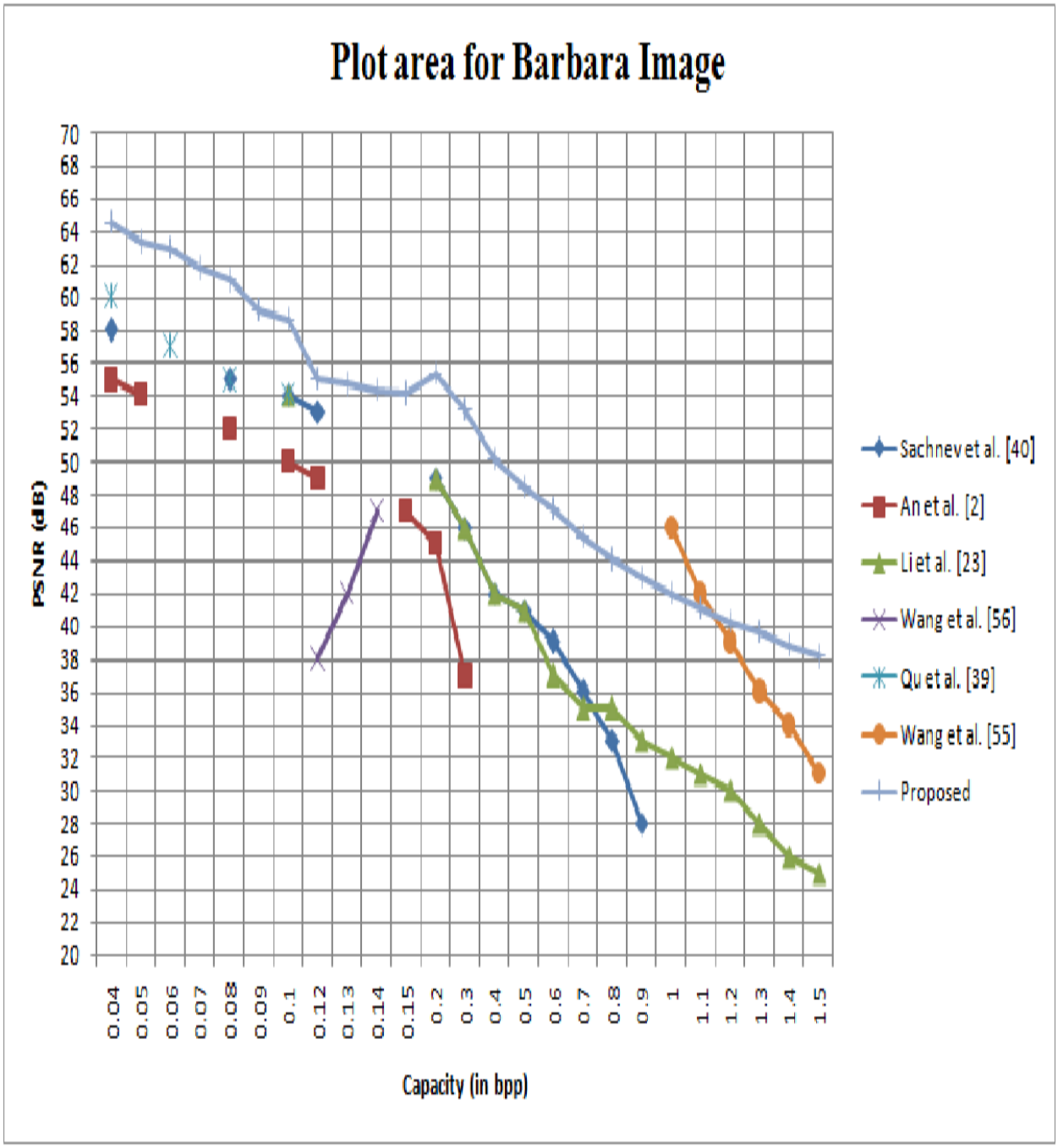
(b)


Plot area for Boat Image
PSNR (dB)
Capacity (in bpp)
68
66
64
62
60
58
56
54
52
50
48
46
44
42
40
38
36
34
32
30
0.01 0.02 0.03 0.04 0.05 0.06 0.07 0.08 0.09 0.1 0.11 0.12 0.13 0.14 0.15 0.16 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1 1.1 1.2
Ni et al.[35]
Fallahpur et al. [9]
Lin et al. [26]
Luo et al.[31]
Hong W. [12]
Wang et al. [52]
Qu et al. [39]
Lee et al.[20]
Proposed

(c)


Plot area for Baboon Image
PSNR (dB)
Capacity (in bpp)
0.01 0.02 0.03 0.04 0.05 0.06 0.07 0.08 0.09 0.1 0.11 0.12 0.13 0.14 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1 1.1 1.2
Luo et al.[31]
Li et al. [23]
Wang et al. [56]
Hong W. [12]
Wang et al. [52]
Hong et al. [13]
Qu et al. [39]
Wang et al.[55]
Lee et al.[20]
Tsai et al.[49]
Proposed

(d)



(e)

Figure 4.7: Comparison of hiding capacity in *bpp* versus image quality in *PSNR* with existing reversible techniques on five test images: (a) Lena image (b) Jet image (c) Boat image (d) Baboon image (e) Barbara image

This comparison also shows that proposed technique performs better at most of the hiding capacity than the existing techniques.

4.5 Conclusion

This work proposes a reversible data hiding technique based on blocks of difference image that exploits the simple and absolute differences to increase the hiding capacity and reduce image distortion. Secret data is embedded in both positive and negative peak points, one bit is embedded into each positive peak points and more than one bit are embedded into each negative peak points. Some side information is transmitted for each negative peak point to extract the hidden secret data on the receiver side. Proposed technique achieves high hiding capacity and better visual quality than existing reversible data hiding techniques. In addition, the performance of the proposed technique is more stable for different digital images.

CHAPTER 5

MULTILEVEL DATA HIDING USING HISTOGRAM SHIFTING AND VECTOR QUANTIZATION

5.1 Introduction

In this Chapter, a reversible data hiding technique based on a *VQ* index table as well as histogram shifting is proposed. Firstly, on the basis of the *VQ* index the codebook is rearranged by referring to the index occurrence frequency. Then the code words in the newly generated codebook are clustered into a number of groups so that the secret digits can be hidden with the help of the proposed technique. After applying *VQ* to the image, histogram shifting is applied to this vector quantized image thereby hiding data in the compressed image.

5.1.1 Vector Quantization

VQ is a lossy data compression and an efficient clustering technique. *VQ* is a map from the k-dimensional space R_k into its finite subset $Z = \{z_i ; i = 1,2, \ldots ,N\}$, where Z is the codebook and z_i are the codewords. Firstly by using the training vectors, a representative codebook is generated, for example one of the techniques is iterative clustering algorithm which is usually known as generalized Lloyd algorithm *(GLA)*. In *VQ*, firstly the image is decomposed into vectors and then every vector is encoded one by one in sequential manner. During encoding, every k-dimensional input vector $x = (x_1, x_2, \ldots, x_k)$ is compared with the existing codewords of the codebook and the best suitable match is recorded. The distortion between the input vector *x* being represented by codeword z_i is measured by the squared euclidean distance.

$$d(x_i, z_i) = \sum_{j=1}^{k} (x_j - z_{ij})^2$$

where x_j is the jth component of the input vector x, and z_{ij} is the jth component of the codeword z_i. The number of the bits needed to represent the indices is usually much less than those which are used to represent the pixels of the original image. Instead of transmitting the original image, it is much more proficient that the VQ indices are transmitted so that the bandwidth can be saved. At the time of the VQ decoding, received indices are used to reconstruct the input blocks by using the corresponding codewords from the same codebook. The prime focus while designing a VQ technique is to create an optimal codebook for the training set.

Quantization is the technique in which approximation is made of continuous discrete values; usually the values are mostly discrete which are provided as input to the procedure of quantization, but there resolution is finer in comparison to the output values. The aim of vector quantization is to maintain the usefulness as well as produce a compact representation of the data. For example the floating point values which lie in the range [0.0,1.0] are quantized to the integer values in the range [0-255] by storing the intensities of color which quantize the floating-point values that occur in the range [0.0, 1.0] to the integer values of the range 0-255, by representing them by using 8 bits, that is usually considered an optimum resolution for the applications that deal with color. In the current example, the spaces between the possible values is similar over the complete discrete set, so it is known as uniform quantization; usually, the non uniform spacing is more suitable over some parts of the given value range when better resolution is required. Representation of floating-point numbers is an example of non uniform quantization—as there can be any number of floating point values between 0.1 and 1 as there can be between 10 and 100.

Both the above examples describe scalar quantization— as both the input and output values are single numbers or scalars. VQ is also performed by replacing the vectors which are from a continuous input set with the vectors which are from a much sparse set. For example, if in an image there are colors of the pixels as triples of intensities of red, green, and blue in the range [0.0, 1.0] ,each of the three intensities can be quantized uniformly to a number of 8 bit; resulting in the traditional representation of 24 bits.

Not much is gained over standard scalar quantization by quantizing every vector component by utilizing itself; however, if all the vectors are quantized, substituting those with the vectors from the set of sparse non uniform vectors and after that saving only the indices in that set, a better

representation of that image can be obtained. This is the familiar representation of the image. In the terms of VQ the "palette," which is the collection of the possible quantized vectors is known as "codebook," as it is required to "decode" the indices into actual vector values.

Algorithms for Vector Quantization

The prime concern in *VQ* is to choose the vectors in such a way that the mean quantization error is minimum: and the input vectors are mapped to the codebook by guessing the suitable matches, after the codebook is ready. In the applications in which the quantization is completed within the real time, an approach to the step described above might be quite slow, but in some cases it is dependant on the orders of magnitudes which get much faster than generating an optimal codebook.

There are mainly two *VQ* algorithms, the classical *GLA* (generalized Lloyd algorithm, also known as K-means clustering), and Anthony Dekker's Neuquant. Both of these algorithms are very costly in terms of computations, as all the solutions to the problem are recorded by brute force.brute. And, there also exist much faster algorithms, but the speed is achieved by restricting the generality of the codebook that would lead to larger quantization error. Compression is used as a preprocessing stage to hide the data and compression times is of about few hours, which is within the timing range of the brute force algorithms.

Generalized Lloyd Algorithm

GLA is performed in iterations and every iteration is comprised of two phases: the codebook assignment phase and the codebook adjustment phase. In the codebook assignment phase, every vector of the input set is mapped to the nearest vector which is being selected from the codebook. While during the codebook adjustment phase, the centroid or average of all the input vectors replace every codebook vector. This process is proved to be convergent, with minimum mean square error of quantization.

Also, there are mainly two concerns with *GLA*: firstly, to initialize the codebook and to use the vacant entries. If there is a cell which is empty, when some vector of the codebook doesn’t get any input vector mapped to it during the assignment phase, it will not be modified in the second phase and hence the cell might remain vacant in every next following operations. Some kind of heuristic is required to receive a prospective replacement. The codebook vector is split into two closely related vectors, which is having highest number of assigned input vectors and let it

suppose that they are pull apart with multiple iterations; or it can split the one who has the most distant assigned vectors.

If the dead vector problem has some satisfying solution, the selection of the initial codebook does not matter much—it can be initialized with any random vectors, or with all the origin vectors, *GLA* may finally move all of them into their respective positions and remove the improper ones. This, however, takes a large number of iterations— which can be improved by choosing a better starting position.

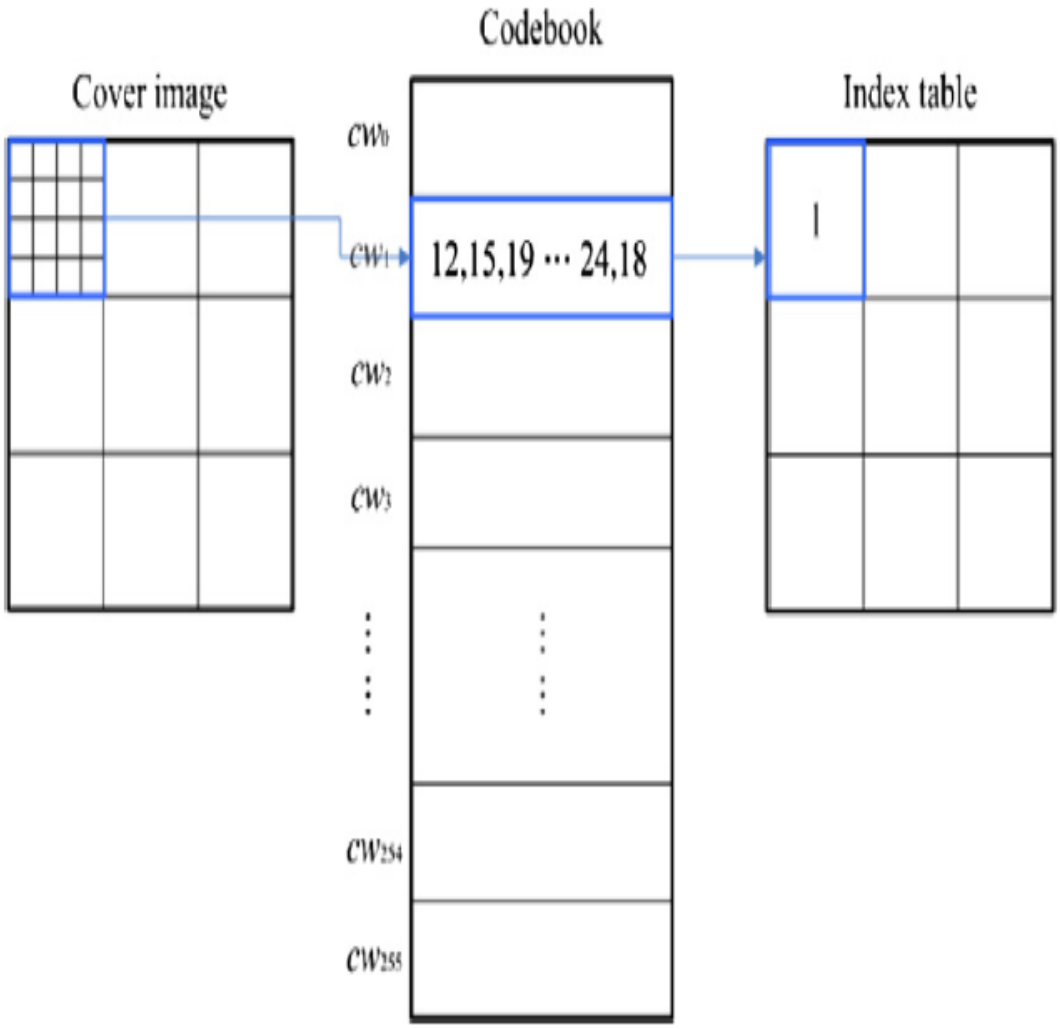


Figure 5.1: The process of VQ encoding

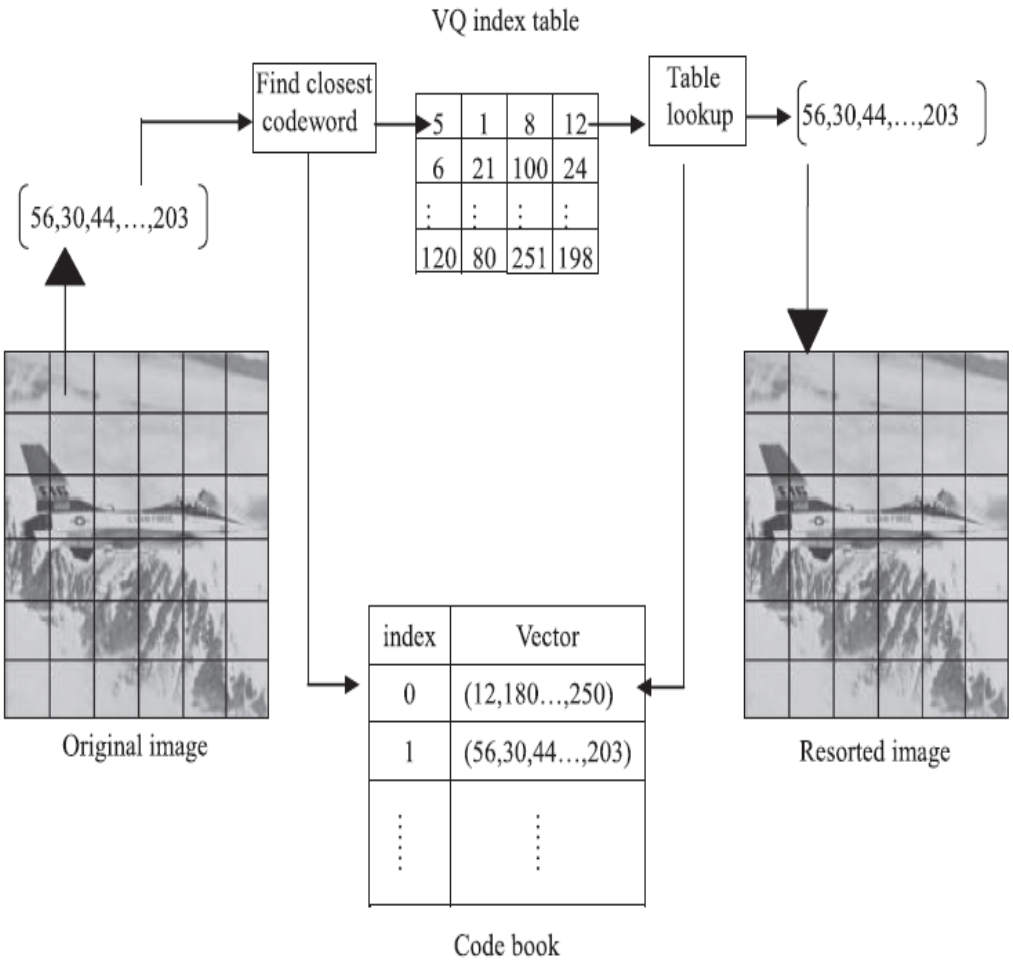


Figure 5.2: *VQ* encoding and decoding process

Here are some of the pros and cons of *VQ* for the compression of images:

Pros:

- High decompression rate (usually faster than the copying rate of uncompressed data)
- Remarkable quality
- Maintaining admirable compression ratios
- A flexible trade-off between the fidelity and compression ratio

Cons:

- Low compression rate.
- Nonstandard as it is not widely supported in every hardware.

5.2 Data Embedding Algorithm

The following technique has been proposed to embed the data in the compressed images based on histogram based reversible data hiding techniques along with *VQ* techniques. The data is embedded using the peak and zero points [26] of the *VQ* compressed images and is embedded in various levels.

For any given grayscale image, firstly its vector quantized image is generated with the help of the technique described above and for that vector quantized image its histogram is generated.

Step 1: With the help of the histogram, a zero point and a maximum point are recorded. Zero or point corresponds to the grayscale pixel value which is held by minimum number of pixels in the image. Whereas the maximum point refers to that grayscale value that the maximum number of pixels in the image hold. The number of pixels associated with the maximum peak point determine the number of bits which can be embedded in the image.

Step 2: The whole image is scanned row by row and column by column and the values of the pixels between the maximum and minimum point are incremented or decremented by 1 depending whether the minimum point lies to the right or left of the maximum point respectively, leaving the grayscale value corresponding to the maximum number of pixels empty.

Step 3: The complete image is scanned again in the same sequential order. Whenever pixel with grayscale value of maximum point is encountered, the to-be embedded bit is verified. If the to-be embedded bit is '1' the pixel value is incremented by 1. Otherwise the pixel value remains the same.

Step 4: In this way when the data is embedded in the image, a stego marked image is obtained. The above algorithm can be repeated again on this obtained stego image about 4-5 times, thus enabling multilevel data hiding.

5.3 Data Extraction Algorithm

The marked compressed image is received at the receiver side which has been compressed using the *VQ* techniques and in which data has been embedded at the sender's side with the help of the histogram shifting. The extraction algorithm should decompress the image and extract data as well as the cover media without any distortion. Firstly the image is decompressed and then the

data is retrieved out of it. Assume the grayscale value of the maximum points and minimum points of the last level are a and b respectively. The marked image is of size M × N, each pixel grayscale value x Є [0,255].

Step 1: Scan the marked image in the sequential order in the same way as that used at the time of embedding. If the pixel with a grayscale value a+1 is encountered, a bit "1" is extracted and if a pixel with the peak pixel value a is encountered, a bit "0" is extracted.

Step 2: Scan the image once again, for any pixel value x Є (a,b] , the pixel value is subtracted by 1.

Step 3: If there is some overhead bookkeeping information found in the extracted data, set the pixel grayscale value as b.

Step 4: This algorithm is repeated for all the number of levels till all the data is extracted and the cover media is obtained.

In this way, the original image can be extracted from the marked image without any distortion.

5.4 Experimental Results

Proposed data hiding technique is implemented in MATLAB. For this five different images have been taken and secret data was embedded into it. To evaluate the performance of the proposed technique, PSNR and PSNR HVS between stego image and cover image using the expressions described before.

PSNR, PSNR-HVS and hiding capacity of various images are shown below in the table 5.1

Table 5.1: *PSNR, PSNR-HVS* and hiding capacity of various images

Image	PSNR	PSNR HVS	Embedding Capacity (in bits)
Lena	22.36	28.31	55562
Baboon	20.75	24.18	90821
Pepper	20.48	24.10	114253
Boat	20.02	22.91	128173
Jet	20.52	22.76	220932

This tables shows the *PSNR, PSNR HVS* corresponding to the embedding capacity of the image. The technique has been tested on various images and the results for five images have been shown here.

5.5 Conclusion

The proposed multilevel reversible data hiding technique embeds data using histogram shifting on the compressed images and the obtained stego images guarantee the *PSNR* versus the original image to be above 20 *d*B. The algorithm has been applied to various images. The stego images can be decompressed and the data can be retrieved at the receiver side without any distortion.

CHAPTER 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this dissertation, various data hiding techniques for digital images have been proposed. In Chapter 3, multilevel data hiding technique based on histogram shifting has been proposed. The marked image obtained is again used to embed the data upto certain number of levels till its visual quality is maintained. Using this approach, high hiding capacity is obtained as compared to various previously existing techniques. In Chapter 4, another data hiding technique had been proposed which used the concept of difference images and histogram shifting. This technique produced better results in terms of data hiding capacity as compared to various existing techniques. In Chapter 5, a data hiding technique has been proposed which hides the data in the compressed images. The images are first compressed with the help of vector quantization techniques and then histogram shifting is applied on the compressed images, thereby hiding data into it. Usually by increasing hiding capacity, visual quality of an image is decreased, the proposed algorithms increased hiding capacity thereby maintain the visual quality to certain level. *PSNR* and *PSNR*-HVS is the quality factor used to analyze the visual quality of marked image obtained with respect to original image, after applying the proposed data hiding techniques.

6.2 Future Scope

The future scope of this dissertation will focus on the further enhancement in hiding capacity and visual quality.

The following future direction can be

- It can be extended for video files and medical images *etc*
- It can be combined with cryptography to provide double layer security.

References

[1] Alattar M., "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Transactions on Image Processing, 13(8), 1147–1156, 2004.

[2] An L., Gao X., Yuan Y., and Tao D., "Robust lossless data hiding using clustering and statistical quantity histogram", Neuro Computing, 77(1), 1-11, 2012.

[3] Celik M.U., Sharma G., Tekalp A. M., and Saber E., "Reversible data hiding", Proceedings of IEEE International Conference on Image Processing, Rochester, NY, 157-160, 2002.

[4] Chang C.-C., Chen K.-N.,Wang Z.-H. and Li M.-C., "Lossless Information Hiding in the VQ Index Table", Journal of Software, 8(3), 2013.

[5] Chang C.-C., Nguyen T.-S. and Lin C.-C., "A novel VQ-based reversible data hiding scheme by using hybrid encoding strategies", The Journal of System and Software, 86, 389-402, 2013.

[6] Chang C.-C., Nguyen T.-S. and Lin C.-C.,"A reversible data hiding scheme for VQ indices using locally adaptive coding", Journal of Visual Communication and Image Representation, 22, 664-672, 2011.

[7] Chang C.-C.,Chen G.-M. and Lin M.-H., "Information Hiding based on search order coding for VQ indices", Pattern Recognition Letters, 25, 1253-1261, 2004.

[8] Chang Y.F. and Tai W.L., "Histogram based reversible data hiding based on pixel differences with prediction and sorting", KSII Transactions on Internet and Information Systems, 6(2), 3100-3116, 2012.

[9] Fallahpour M. and Sedaaghi M.H., "High Capacity lossless data hiding based on histogram modification", IEICE Electron Express, 4(7), 205-210, 2007.

[10] Goljan M., Fridrich J., Du R., "Distortion-free data embedding", Proceedings of the Four Information Hiding Workshop, Lecture Notes in Computer Science, 2137, Springer, New York, 27–41, 2001.

[11] Guo J.-M. and Tsai J.-J., "Reversible data hiding in low complexity and high quality compression scheme", Digital Signal Processing, 22(5), 776-785, 2012.

[12] Hong W., "Adaptive reversible data hiding method based on error energy control and histogram shifting", Optics Communications, 285(2), 101-108, 2012.

[13] Hong W., Chen T.S. and Wu M.C., "An improved human visual system based reversible data hiding method using histogram modification", Optics Communications, 291, 87-97, 2013.

[14] Honsinger C., Jone P., Rabbani M., Stoffel J., "Lossless recovery of an original image containing embedded data", United States Patent #6278791, 2001.

[15] Jung S.W., "Adaptive post-filtering of JPEG compressed images considering compressed domain lossless data hiding", Information Sciences, 281, 355-364, 2014.

[16] Kamstra L, Heijmans H., "Reversible data embedding into images using wavelet techniques and sorting", IEEE Transactions on Image Processing, 14(12), 2082–2090, 2005.

[17] Kim H. J., Sachnev V, Shi Y. Q., Nam J, Choo H. G., "A novel difference expansion transform for reversible data embedding", IEEE Transactions on Information Forensic Security, 3(3), 456–465, 2008.

[18] Kim H.J., Sachnev V., Shi Y.Q., Nam J., and Choo H.G., "A novel difference expansion transform for reversible data embedding", IEEE Transactions on Information Forensics and Security, 3(3), 456–465, 2008.

[19] Lee C.C., Wu H.C., Tsai C.S., Chu Y.P., "Adaptive lossless steganographic scheme with centralized difference expansion", Pattern Recognitions, 41(6), 2097–2106, 2008.

[20] Lee C.-F. and Chen H.-L., "Adjustable prediction based reversible data hiding", Digital Signal Processing, 22(6), 941-953, 2012.

[21] Lee J.-D., Chiou Y.-H. and Guo J.-M., "Lossless data hiding for VQ indices based on neighboring correlation", Information Sciences, 231, 419-438, 2013.

[22] Leung H.Y.,Cheng L.M., Liu F. and Fu Q.K., "Adaptive reversible data hiding based on block median preservation and modification of prediction errors", Journal of systems and Software, 86(8), 2204-2219, 2013.

[23] Li X., Yang B., and Zeng T., "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," IEEE Transactions on Image Processing, 20(12), 3524–3533, 2011.

[24] Li Y.-C., Yeh C.-M. and Chang C.-C., "Data hiding based on the similarity between neighboring pixels with reversibility", Digital Signal Processing, 20(4), 1116-1128, 2010.

[25] Lin C.-C., Liu X.-L. and Yuan S.-M., "Reversible data hiding for VQ-compressed images

based on search-order coding and state-codebook mapping", Information Sciences, 293, 314-326, 2015.

[26] Lin C.C., Tai W.L., and Chang C.C., "Multilevel reversible data hiding based on histogram modification of difference images", Pattern Recognition, 41, 3582-3591, 2008.

[27] Lo C.C., Hu Y.C., Chen W.L. and Wu C.M., "Reversible Data Hiding Scheme for BTC-compressed Images based on Histogram Shifting", International Journal of Security and Its Applications, 8(2), 301-314, 2014.

[28] Lou D. C., Chou C. L., Tso H. K. and Chiu C. C., "Active steganalysis for histogram-shifting based reversible data hiding", Optics Communications, 285(10-11), 2510-2518, 2012.

[29] Lu T.-C., Tseng C.-Y. and Deng K.-M., "Reversible data hiding using local edge sensing prediction methods and adaptive thresholds", Signal Processing, 104, 152-166, 2014.

[30] Lu Z.-M., Wang J.-X. and Liu B.-B., "An improved lossless data hiding scheme based on image VQ-index residual value coding", The Journal of System and Software, 82, 1016-1024, 2009.

[31] Luo H., Yu F.X., Chen H., Huang Z.L., Li H., and Wang P.H., "Reversible data hiding based on block median preservation", Information Science, 181(2), 308-328, 2011.

[32] Luo L., Chen Z., Chen M., Zeng X., and Xiong Z., "Reversible image watermarking using interpolation technique", IEEE Transactions on Information Forensics and Security, 5(1), 187–193, 2010.

[33] Ma X., Pan Z., Hu S. and Wang L.,"Reversible data hiding scheme for VQ indices based on modified locally adaptive coding and double-layer embedding strategy", Journal of Visual Communication and Image Representation, 28, 60-70,2015.

[34] Mali S.N., Patil P.M., and Jalenkar R.M., "Robust and secured image-adaptive data hiding", Digital Signal Processing, 22, 314-323, 2012.

[35] Ni Z., Shi Y.Q., Ansari N., and Su W., "Reversible data hiding", IEEE Transactions on Circuit and System for Video Technology, 16(3), 354-362, 2006.

[36] Patra J.C., Karthik A. and Bornand C., "A novel CRT-based watermarking technique for authentication of multimedia contents", Digital Signal Processing, 20, 442–453, 2010.

[37] Peng F., Li X. and Yang B., "Improved PVO-based reversible data hiding", Digital Signal Processing, 25, 255-265, 2014.

[38] Qin C., Chang C.-C. and Chen Y.-C., "Efficient reversible data hiding for VQ-compressed images based on index mapping mechanism", Signal Processing, 93, 2687-2695, 2013.

[39] Qu X. and Kim H. J., "Pixel based pixel value ordering predictor for high-fidelity reversible data hiding", Signal Processing, 111, 249-260, 2015.

[40] Sachnev V., Kim H.J., Nam J., Suresh S., and Shi Y.Q., "Reversible watermarking algorithm using sorting and prediction", IEEE Transactions on Circuits and Systems for Video Technology, 19(7), 989–999, 2009.

[41] Saleh N.A., Boghdady H.N., Shaheen S.I. and Darwish A.M., "High capacity lossless data embedding technique for palette images based on histogram analysis", Digital Signal Processing, 20, 1629–1636, 2010.

[42] Sencar H.T., Ramkumar M. and Akansu A.N., "Data Hiding Fundamentals and Applications: Content Security in Digital Multimedia", Elsevier Academic Press, 2004.

[43] Shen and Ren J.M., "A robust associative watermarking technique based on vector quantization", Digital Signal Processing, 20, 1408–1423, 2010.

[44] Tai W.L., Yeh C.M., and Chang C.C., "Reversible data hiding based on histogram modification of pixel differences", IEEE Transactions on Circuits and Systems for Video technology, 19(6), 906–910, 2009.

[45] Tang J., Zheng J. and Guo L., "H.264/AVC Compressed Domain Data Hiding Algorithm Based on in-Loop Compensation", 4th International Congress on Image and Signal Processing, 371-375, 2011.

[46] Thabit R. and Khoo B. E., "A new robust lossless data hiding scheme and its application to color medical images", Digital Signal Processing, 38, 77-94, 2015.

[47] Tian J. "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits Systems and Video Technology, 13(8), 890–896, 2003.

[48] Tsai P., Hu Y.C., and Yeh H.L., "Reversible image hiding scheme using predictive coding and histogram shifting", Signal Processing, 89(6), 1129-1143, 2009.

[49] Tsai Y.-Y., Tsai D.-S. and Liu C.-L., "Reversible data hiding scheme based on neighboring pixel differences", Digital Signal Processing, 23, 255-265, 2014.

[50] Tseng H.W., Chang C.C., "An extended difference expansion algorithm for reversible watermarking", Image Visual Computing, 26(8), 1148–1153, 2008.

[51] Tu T.-Y. and Wang C.-H., "Reversible data hiding with high payload based on referred

frequency for VQ compressed codes index", Signal Processing, 108, 278-287, 2013.

[52] Wang J., Ni J. and Hu Y., "An efficient reversible data hiding scheme using prediction and optimal side information selection", Journal of Visual Communication and Image Representation, 25(6), 1425-1431, 2014.

[53] Wang J.-X. and Lu Z.-M., "A path optional lossless data hiding scheme based on VQ joint neighboring coding", Information Sciences, 179, 3332-3348, 2009.

[54] Wang W.-J., Huang C.-T.,Liu C.-M., Su P.-C. and Wang S.-J., "Data embedding for vector quantization image processing on the basis of adjoining state-codebook mapping", Information Sciences, 246, 69-82, 2013.

[55] Wang X.-T., Chang C.-C., Nguyen T.-S. and Li M.-C., "Reversible data hiding for high quality images exploiting interpolation and direction order mechanism", Digital Signal Processing, 38(2), 569-577, 2013.

[56] Wang Z. H., Lee C. F. and Chang C. Y., "Histogram shifting imitated reversible data hiding", Journal of Systems and Software, 86(2), 315-323, 2013.

[57] Yang C.-H., Wang W.-J., Huang C.-T. and Wang S.-J., "Reversible Steganography based on side match and hit pattern for VQ-compressed images", Information Sciences, 181, 2218-2230, 2011.

[58] Yang C.-H., Wu S.-C., Huang S.-C. and Lin Y.-K., "Huffman-code strategies to improve MFCVQ-based reversible data hiding for VQ-indexes", The Journal of System and Software, 84, 388-396, 2011.

Communicated Papers

- Sonal Kukreja and Singara Singh Kasana, “Histogram based Multilevel Reversible Data Hiding Scheme using Simple and Absolute Difference Images”, Signal Processing, SCI Indexed.

- Sonal Kukreja and Singara Singh Kasana, “Multilevel Reversible Data Hiding for Digital Images using Histogram Shifting” Journal of Cryptographic Engineering, Scopus Indexed.

Video Link

https://www.youtube.com/watch?v=jtHvLoItnS0