EFFICIENT REVERSIBLE DATA HIDING TECHNIQUE FOR DIGITAL IMAGES

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

Master of Engineering
in
Computer Science and Engineering

Submitted By
Govind Ram Chhimpa
Registration No. - 801732012

Under the supervision of:

Dr. Singara Singh Kasana

Associate Professor

Dr. Rajesh Mehta

Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT

THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY

PATIALA – 147004

July 2019

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*Efficient Reversible Data Hiding Technique for Digital Images*", in partial fulfilment of the requirements for the award of degree of Master of Engineering in *Computer Science and Engineering* submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Singara Singh Kasana and Dr. Rajesh Mehta.*

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Govind Ram Chhimpa

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Dr. Singara Singh Kasana
Associate Professor
Computer Science & Engineering
TIET, Patiala

Dr. Rajesh Mehta
Assistant Professor
Computer Science & Engineering
TIET, Patiala

ACKNOWLEDGMENT

No volume of words is enough to express my gratitude towards my guide **Dr. Singara Singh Kasana** and **Dr. Rajesh Mehta**, Department of Computer Science & Engineering, Thapar University, Patiala, They have been very concerned and has aided for all the materials essentials for the preparation of this thesis report. They have helped me to explore this vast topic in an organized manner and provided me all the ideas on how to work towards a research-oriented venture.

I am also thankful to **Dr. S. S. Bhatia**, Dean of Academic Affairs, **Dr. Maninder Singh**, Head of Computer Science & Engineering Department and **Dr. Ashutosh Mishra**, P.G. Coordinator, for the motivation and inspiration that triggered me for the thesis work.

I would also like to thank the staff members and my colleagues who were always there at the need of the hour and provided with all the help and facilities, which I required, for the completion of my thesis work.

Most importantly, I would like to thank my parents and the almighty for showing me the right direction out of the blue, to help me stay calm in the oddest of the times and keep moving even at times when there was no hope.

Govind

Govind Ram Chhimpa

Registration No. - 801732012

ABSTRACT

The proposed efficient reversible data hiding technique is the extension of Peng *et al.'s* (2014) technique. In this technique, an original or cover image is divided into non-overlapped blocks of equal size. Each block is sorted in ascending order and then difference are calculated on the basis of location of the largest and smallest pixel value within the blocks. According to the value of difference, data is embedded in blocks. The difference can be negative or positive. In the Peng *et al.'s* technique only difference value 0 or 1 are used for data embedding and other difference value are used for create space. But in the proposed method, the difference value -1 is also used for data embedding. This can better exploit image redundancy and achieve a superior embedding performance. The reversibility is guarantees in the proposed method.

The proposed efficient work gain superior embedding capacity with low distortion than other existing technique. For low embedding capacity this work performance is likely to equal to Peng *et al*.'s (2014), and for large embedding capacity this work gives better result than Peng *et al*.'s (2014) and other reversible data hiding technique. In this proposed scheme image redundancy better exploited and more embedding capacity can be achieved.

TABLE OF CONTENTS

LIST OF TABLE

LIST OF FIGURE

CHAPTER-1: INTRODUCTION

1.1: Needs of Data Security: With the quick development in digital technology, these are become part of everyone life. Technology plays a role in net banking, online shopping, business, and infrastructure. Apart from the benefits of digital technology, there is some risk of modification of data. Recently, cyber-attacks are growing quickly to target anyone data. Many tools are available for modifying original data on the network. Everyone's data transfer from network to network, so there is a risk of modification in data. If anyone's information like payment information, personal files, bank account details, and original document grabbed by an attacker or unauthorized person, then there happen a big loss to details holder. Therefore, the security of data is needed.

1.1.1: Data Security: Data security means the protection of data, like a database. Data is secured from different illegal action and unwanted action from an unidentified user or unauthorized user. Today's environment is a network environment and all the things grow very fast on the network. Image processing and multimedia technologies are growing fast, there are many modifying tools available on network so anyone can change in original content using available tools so security is important. Using various software and hardware technologies, data can be secured from unauthorized user or attacks.

Data security also refers to privacy that is applied to stop impermissible access to system, websites, and database. Data security also used to protect data from corruption. Data security is the main and first priority for any institutions, organization. Data security also care the data from impermissible modification, destruction using many online tools like logic controls, administrative controls, and software. Data security include

Data encryption: Data encryption means to convert data in another format using the key that is not easily read by an unknown person. Data encryption is also used for authentication of data.

Tokenization: Tokenization is the process of replacing data with a unique symbol. These symbols retain all information without any changes in data. Tokenization mainly used for data security. Tokenization means to remove the unmeaning word or terms

from data. Using the help of tokenization we make our data more secure from unauthorized user. Tokenization is used in many fields like bank transaction, criminal record, driver information, and loan application and voter registration.

1.1.2: Importance of Data Security: In today internet environment the protection of data is the most important concern things. Everyone wants to keep our data safe on the network. There are many online tools to modified original data into unwanted data so data security is important. Need the security of data to protect from hacker and unauthorized user. Nowadays any kind of modification in data is not tolerant. If do not protect data than can face a big problem. Like unauthorized user create big problems for anyone by modification of data. In today's environments, there are many tools available to protect data from impermissible user and hacker. Many big organization provides data security tools to protect data. For example, if anyone modified transaction or divert transaction for a special purpose then happen big harm in money that's why security is needed.

1.2: Image Security:

Image security is a process to protect the image from unwanted modification. It is the same as data security. Anyone can change or modifies an image for any special purpose. So image security is an important issue.

The Need for Security of Images:

Security is the most important issue during the transmission of the image. Image security is an important issue when image and information about the image are transmitted through the public network. An image such as military image and medical image where any type of loss is not accepted so image security is important.

1.2.1: Types of Security of Image:

1.2.1.1: Cryptography: Cryptography is a process of converting one form of data into another form using a secret key. Cryptography is a process of hiding information. Cryptography is closely related to mathematics and computer science and used for security purpose. There are several uses of cryptography in information security. In cryptography without a key we can't read message or information, so for the encrypt or decrypt message there need a key. During transmission or storing information maintain integrity.

The Main Objective of Cryptography: There are mainly for the type of objective of cryptography.

i. Confidentiality: Confidentiality means information cannot be understood by anyone.
ii. Integrity: Integrity means the information between sender and receiver cannot be altered by anyone.
iii. Non-repudiation: Means the sender cannot deny information.
iv. Authentication: The sender and receiver believe in the identity of each other and the source of information.

Types of Cryptography: Mainly three types of cryptography used in general.

i. **Symmetric Key Cryptography**: In Public key cryptography only single key shared by both sender and receiver. Using this key, the sender encrypts text to cipher text and send to the recipient. The receiver converts cipher text to plaintext with the same key.
ii. **Public Key Cryptography:** In public key cryptography two key, public and private key used for encryption and decryption. For encryption public key used and for decryption private key used. Using the receiver public key, the sender encrypts the message and send it to the receiver, and other side receivers decrypt the message using own private key.
iii. **Hash Function:** In this, there is no concept of the key, a hash value is computed for plaintext and converted into cipher text.

The general model of cryptography:

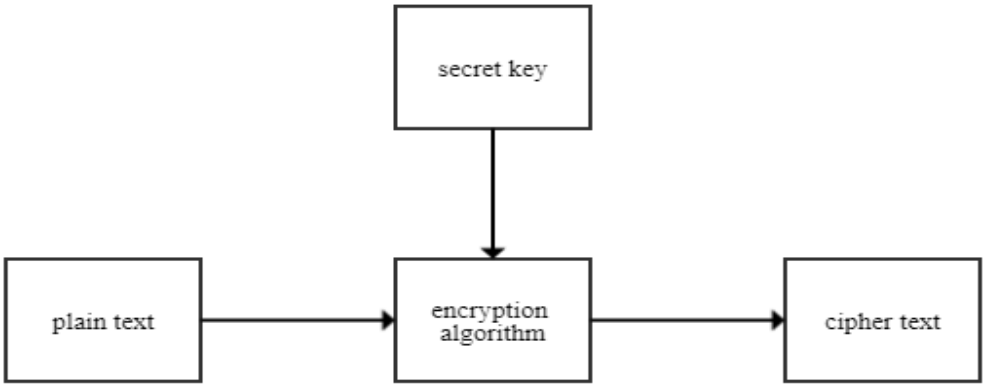

Fig. 1.1. Encryption Process of Cryptography

Cryptography is a process of encryption and decryption of information using a secret key. For encryption, the plain text is converted into cipher text using a particular key. Here the general model of cryptography for both encryption and decryption described by the diagram.

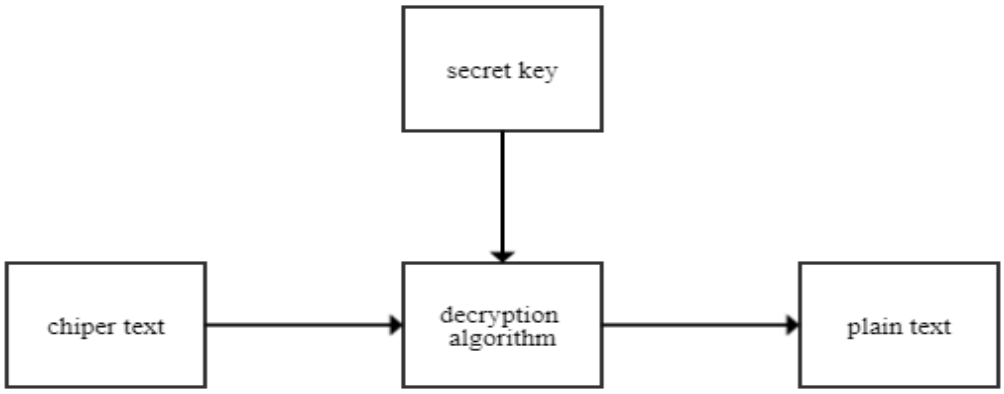

Fig. 1.2. Decryption Process of Cryptography

1.2.1.2: Watermarking: Watermarking is a process of hiding or embed information in images so that it cannot be misused by anyone. Watermarking is also used for authentication and authorization of information or signals. It is used for different purposes like hidden communication, copyright protection, and fraud detection, etc.

Types of Watermarking: There is a different type of watermark like

Visible Watermarking: This type of technique generate logo on watermark image. And the content is a sight to human.

Invisible Watermarking: This type of technique is used to hide information in the image which cannot be seen by anyone. Content is not scene to human.

Robust Watermarking: It is used to sign copyright information to the digital work. In robust watermarking, if the watermark image or video changed than no effect on the watermark.

Symmetric and Asymmetric Key Watermarking: In symmetric key watermarking only one key used for embedding and extracting but in Asymmetric, the different key used.

1.2.1.3: Steganography: It is a process of hiding text or confidential information into another file like image or text or video. It is used for any type of content like video,

audio, or text and images. It's used for hiding information in the above content and then back to recover original content. With the help steganography and cryptography, we can improve our security of data and keep safe from the unauthorized or impermissible user. Using steganography we provide better security to our data. Steganography creates a safe environment between two communicating parties. They can share our message or data safely.

It is also used for transmission of a top-secret message on between international government documents. It can hide or embed more capacity of data or information in a carrier signal which cannot detect by anyone. Steganography can save us for a big loss of our information when hacker attack on our data. It is a strong technique to protect our data from the unauthorized user or undetected user. It applies to any type of digital content like video, audio, text, and images for hiding or embeds information.

1.3: Data Hiding Scheme

Data hiding is a method of hiding important information or some useful data into original media. For this scheme two group of sets are required, one is an embedded information set and another one is original media.

Data invisibility is the major requirement of data hiding scheme, and another requirement is to minimize the distortion and maximize the payload.

In the data hiding process, distortion can occur when data is embedded to cover media and this can create trouble when data is extracted from original cover media.

Data hiding scheme is a two-step process, first is to embed data in cover media and second to extract data from marked media without any changes or distortion.

1.3.1: Reversible Data Hiding:

Reversible data hiding is a process of recover original data and original cover media without any distortion. Reversible data hiding (RDH) also known as lossless data embedding has an ability to eliminate embedding distortion. RDH usually used for copyright protection and data hiding of sensitive images such as military and medical image.

It is a type of data hiding technique whereby a host image recovered exactly without any loss.it is a process to reverse the marked media back to the original cover media

after the hidden data extracted. In the reversible data hiding technique, the reversible or lossless ability is required.

1.3.2: Irreversible Data Hiding:

Irreversible data hiding means can't proper recover or obtain original data from the marked image which is made after data embedding. It is the failure of reversible data hiding technique. In reversible data hiding technique first, hide some data or information in cover or original media and get marked media. This process is called embedding process of reversible data hiding technique. In the extraction phase of reversible data hiding, extract original data and original cover media from the marked image. And there is no distortion and error in the extracted process.

But in irreversible data hiding technique there is a problem in the extraction phase. Can't properly extract data or original media exact. In irreversible the original image and data can't be extracted so there is a problem in the extraction phase.

1.4: General Model of Data Hiding.

There are two model of data hiding technique. First one is for data embedding and the second one is for data extracting.

1.4.1: Data Hiding: Take a cover image and secret message and with the help of encryption algorithm and key, hide data in cover media and produce a marked image as an output.

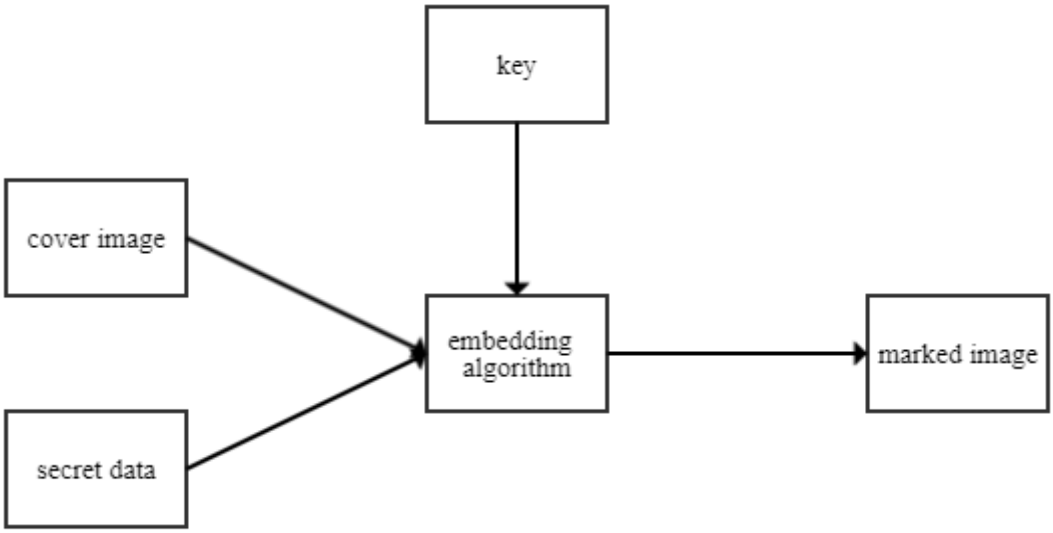

Fig. 1.3. Data Embedding Procedure

In the data hiding process, the embedding algorithm plays the main role in this procedure. Choose these embedding algorithm which is more efficient and hide more capacity of data and embedding and extracting process work properly. Every algorithm has own technique to embed data and other information. Before embedding secret message need to calculate some value like noise level and construct a location map to check underflow or overflow condition because all work doing on grayscales images. For embedding algorithm, two group of set required, a cover image and secret message. Secret message can be a binary data or binary image. The binary image is a watermarking image.

1.4.2: Data Extracting:

After the embed data into cover media, there is need to extract data also. There is an extraction algorithm for extract data. This extraction algorithm applied to the marked image which is the outcome of the cover image after embedding data.

The embedding and extracting algorithm both are for one concept. Developing an algorithm in which both embedding and extracting procedure describe. After extract data completely, there are no changes in the original image and secret data. All the method has its own procedure to extract data from the marked image.

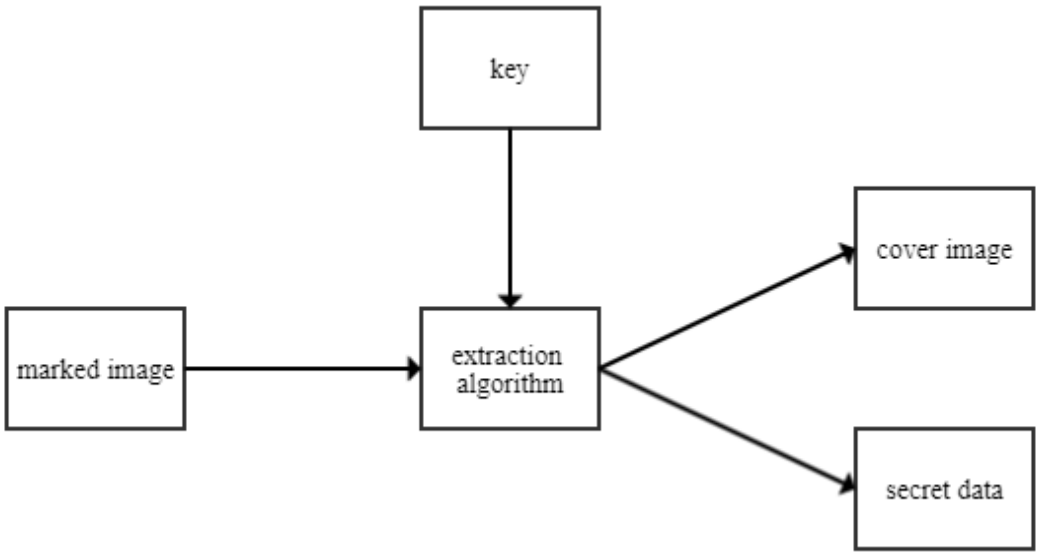

Fig. 1.4. Data Extraction Procedure

After the extraction of data, the cover image and secret message produce as an output. If any type of error faced in data extraction phase then there is a problem of data irreversible. Extraction phase applied to the marked image.

1.5: Application of Data Hiding:

- There is a different type of application of the data hiding scheme.
- It is used for secret communication.
- For authorization of images.
- For adding secret information to the images, text, video, and audio.
- It is used for fingerprinting.
- It is used for image integrity and authentication.
- Used for automatic copyright.
- Data hiding scheme used for security of images.
- It is mainly used for military, medical and satellite images where any type of distortion not accepted.
- It is used to protecting image confidentiality, integrity, and authenticity.

1.6: Characteristic of Data Hiding Scheme:

Characteristic is an important issue for data hiding scheme. There is a different type of properties for data hiding scheme. The task is to hide more capacity data and try to maintain transparency.

i. **Robustness.** The robustness means the ability to extract hidden data after applying the different operation. In image processing images are transmitted upon different network and applying different operation so there is a chance of misconception in hidden data. So robustness is more important. There are a different type of image processing operations like linear and non-linear filters, scaling, copying, re-coloring, re-shaping, printing, scanning, sampling, re-sampling, pixel adjusting, and compression, etc.

ii. **Low Distortion:** Distortion means quality or visibility of images. When data or information are embedded in the image then there is some change in image visibility. Always try to apply that algorithm which causes low distortion. Try to embed more capacity data while maintaining its quality.

iii. **Security.**

Security is an important issue for both image and data. In today's environment is a network environment. In this environment, information is transmitted through the network to network in the public domain. On networks, there are

many editing tools available for modifying the information or alter information or data so security is the most important issue for images or data.

Security protects our data and secret information from outside attack. The embedding information can't be attacked by an attacker when some strong embedding algorithm used. If an attacker gains the Knowledge of both the embedding algorithm and a hidden message then they can attack easily.

iv. **Invisibility.**

Invisibility means perceptual transparency concept. This concept is based on the properties of human video system or audio system.

v. **Embedding Capacity.** This is the main important properties of data hiding scheme. There are a different type of algorithm developed to hide or embed some information in images, audios or videos. In all these types of the algorithm, trying to increase embedding capacity. Embedding capacity means, embed more capacity of data or secret information in images or some other file. Embed more data because the marked image can't be attacked by an attacker easily. When increase embedding capacity than there needs to maintain its visual quality and low distortion. Always used that embedding algorithm which embeds more capacity data and maintains visual quality.

1.7: Quality Parameters:

Image quality is important when used in medical or military-related application because in those type of application if little bit distortion exists than not tolerated. There are different objective to measure the quality of images.

PSNR: Peak-signal-to-noise ratio is used to compute the quality between two images. These two images are the original image and marked image or compressed image. If the PSNR higher, quality is batter and the lower PSNR, the quality is not battered. For calculate PSNR, first, need to calculate MSE (mean square error).

MSE: The MSE is the squared error between the original image and the marked image. Digital images are represented in pixel. So MSE calculates the squared error between the original image and marked image by pixel to pixel. If the value of MSE lower than low error between two images. The MSE is calculated using the following equation.

$$\text{MSE} = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M * N}$$

Where M is total row and N is total column of original image.

$PSNR = 10 \log_{10}(R^2/MSE)$

Where *R* is the max instability in the cover media. If cover image is 8-bit unsigned integer data type, then *R*-value is 255.

1.8: Organization of Thesis: The Thesis is organized as

Chapter-1: In this chapter introduction of data hiding scheme and security of data are discussed.

Chapter-2: In this chapter, a literature survey is done.

Chapter-3: In this chapter Gaps, objective and methodology of work is described.

Chapter-4: In this chapter proposed techniques is describe.

Chapter-5: In this chapter experiment result and comparison are shown.

Chapter-6: In this chapter conclusion and Future Scope discussed.

CHAPTER-2: LITERATURE SURVEY

Data hiding is a process of hide information in media such as image, video, text or audio. It is used for authentication and copyright protection. After hiding data in media, will get some distortion in resultant media which is not accepted by some secured application like medical images or military images. So to reduce this distortion a new technique develop, known as Reversible Data Hiding. RDH can surely regain original media after extract the embedded data. RDH can provide more secured communication and more security to media.

Ni *et al.* (2006) discussed a reversible data hiding is a technic of hiding secret information and retrieving same information without any change. It is a technique of recovering original media after embedding and extraction without any distortion. In this paper pixel shifting concept used to modify the image. The maximum and minimum pixel concept used in this algorithm. In this algorithm first, generated a histogram of cover media and then find out maximum and minimum points of the histogram. In this paper, utilized the zero or minimum pixel to modify the greyscale value for data embedding.

For any RDH algorithm, Consider two things one is embedding capacity and another one is low distortion. The computing time of this algorithm is low and complexity is also low. The other important thing is the PSNR. The PSNR stand for peak-signal-to-noise ratio. This algorithm applied to different types of images like medical image, texture images, etc. In this proposed technique the more capacity data can be nearly about 5 kb-75 kb in the grayscale image of size $512 \times 512 \times 8$. The beauty of this proposed method is the PSNR of the marked image and the cover image is to above 48 db. The execution time of this method is very short and very easy to implement. This method has been applied to a different type of images successfully and it gives a better result than other existing technique. The main important feature of this algorithm is applicability. Applicability means related to the pixel position. In this algorithm not bother about where the maximum, minimum pixel is located.

Yang *et al.* (2013) represent high fidelity reversible data hiding technique for the image. This is also based on approach of PVO (pixel-value-ordering) and PEE (prediction error expansion). In this technique, the host image is divided into equal size non-overlapped block and then sort every block as well as index and then find the maximum and second

maximum or minimum and second minimum for embed secret information. In this scheme, data embedding is done by prediction error expansion. Prediction error expansion is calculated for each block and there is some formula to embedding secret information into the host image to create a marked image.

Using only prediction error expansion there is a problem of shifting pixel arise. To reduce this problem, this technique use pixel value order to reduce the problem of shifted pixel and it can improve the quality of the image after embed data. This method also embeds more data with low distortion. The PSNR of the marked image and the cover image is above 51.14 dB. In this method, the only the flat block is used to embed information while rough block remains unchanged. For comparing the results of the experiment, it gives a good result. For comparing with other existing reversible data hiding method it gains high PSNR on same embedding capacity. It is used only one bin so may not capable to provide good embedding.it can better for some image in case of higher embedding capacity.

Li *et al.* (2014) discussed improved pixel value ordering based reversible data hiding technique. This is the extension of reversible data hiding technique of Li *et al (2014)* which is based on prediction error expansion and pixel value ordering approach. In this method, mainly first divide the cover image in equal size block and then modify the minimum and maximum pixel of the block to add data or information. Reversibility is correct in Li *et al* (2014) method and pixel order are not change after data embedding. But in this method instead of calculating the difference between maximum and minimum pixel, calculate the difference by new histogram modification technique. In this work, important is the pixel location. The new difference is calculated by pixel location of maximum and second largest pixel or minimum or second largest minimum.

In Li *et al.'s* (2013) method there is a drawback for embed data.in this method, in this can't embed data where the largest and second largest pixel value is equal. But in Peng *et al* method, data can embedded, where the largest and second largest pixel value equal. In this method, can embed more capacity data and image redundancy is batter. This method gives better performance than Li *et al.'s (2013)* method according to PSNR. For 512 × 512 size grayscale image, on 1000 embedding bits the average PSNR for Peng *et al.'s (2014)* method is 62.76 DB but in Li.et al 62.07 dB.

Xiang *et al*. (2015) this work discussed reversible data hiding techniques to embed information in an image based on pixel value ordering approach. In all available data hiding scheme, first divide the cover image into equal size blocks and after dividing the blocks we sort every block in ascending order and then modify maximum and minimum pixel in block to embed secret data. In all existing scheme, there is some drawback like some technique has a low capacity drawback and some technique has distortion problem. These existing are well for low capacity if wanted to embed more capacity data then, have to take a smaller block size, which reduces the quality of the marked image.

So in this technique, overcomes all the problem of existing data hiding technique. In this method, the dynamic blocking strategy is used to divide the cover image instead of dividing in equal size block. Dividing the cover image in an unequal or various sized block according to the image area. The flat area is dividing into smaller size block and the rough area is dividing into larger size block to embed secret data. Smaller size block is used to embed more capacity data whereas larger block is used to decreasing peak signal to noise ratio. By the result, this technique embed more capacity data and keep distortion low. The experiments results show a good result comparing to existing reversible data hiding technique on the same image.

Wang *et al.* (2016) discussed pixel value ordering, means it's a technique where first order the values within the blocks of image and then modifying the maximum and minimum pixel within blocks for reversible data hiding. In all these existing reversible data hiding techniques talk about only pixel-Value-ordering and prediction-error-expansion. But this technique talking about a new strategy called 2-D implementation. This technique implements in 2-D and uses prediction pair for data embedding. The main focus to use 2D strategy to effective implementation of pixel value ordering and data embedding. The 2D form is the extension of pixel value ordering embedding. It extends to include pairwise prediction error and 2D reversible mapping. This technique is very useful to recognize a rough and smooth block of image for embed data and for shifting.

In this work, developed a pixel-value-ordering approach algorithm into a two-dimensional technique. Mainly Work on two smallest and two largest pixel value in every block. This technique develops to automatically choose rough are or smooth area

of the image for embedding. This scheme is more flexible and gives a good embedding performance. By comparing the PSNR of the marked image to another existing technique like Peng *et al.*'s (2014) or ou.*et al.'s (*2016), it gives good result and good performance. Our 10000 bits the average PSNR of Peng *et al* (2014) or Ou *et al*. (2016) technique are 58.88 dB and 59.17 dB, but this work gives an average of 59.62 dB PSNR for same data.

Red *et al.* (2016) this work is discussed about histogram shifting concept based on reversible data hiding techniques. After analysed above method then a novel histogram-shifting based on reversible data hiding discovered using adaptive group modification technique. The prediction error is computed between each pair of the pixel. The histogram of prediction error is generated by using adaptive group modification. This concept is named as AGM method. In AGM method there is some technique to hide secret data. In this AGM method, a number of bins are empty based on their frequency of occurrences. The aim to design according to this type of strategy is to hide more capacity data and reducing the shifting to maintain image quality and aim to achieve good PSNR between the original image and marked image. In this method, a new embedding process is also discovered. Instead, to hide one bit at a time, payload data or secret data are divided into different segments and each segment embed by a concept name as a triplet of prediction error.

This method mainly work in two-part first is histogram generation and second is data hiding. In this work according to pixel intensity value, a histogram of prediction error is generated. After that histogram is scanning to find space by selected bin to hide data. According to result this method achieve good embedding capacity and low distortion. According to results over different payload size, it outperforms Li *et al.*'s (2014) method.

Ou *et al.* (2016) this work discussed improved based pixel-value-ordering algorithm to achieve good performance. In this work, the embedding procedure is performed by multiple histogram modification technique. For a given histogram, bins are used to determine the embedding performance. For good performance selection of bin play an important role, different technique of data hiding have their own procedure of selection of bins. Multiple histogram modification used a function to select bin for data embed

known as expansion bin selection. For MHM firstly modify smooth pixel. By noise level, a technique can differentiate smooth area or texture area of the image.

Analysing the above MHM scheme this work present two-stage bin selection algorithm to achieve well performance. The advantage of using the two-stage bin-selection method is computational complexity can easily be controlled and the computational speed is fast. Embedding capacity is also a benefit of the two-stage bin selection algorithm. Experiments results show the performance of this method comparing the results of other PVO-based technique on the standard image. According to the result table of this method, this method gives good performance and it can obtain larger PSNR on more capacity of data comparing with PVO-based embedding method in recent. For a given standard image like Lena on capacity 10,000 and 20,000 bits, this method gain 2.85 dB and 2.85 dB PSNR more than average. Its means this method achieves good PSNR on more embedding capacity. In this method, the time complexity and space complexity is increased. This method is more effective in terms of processing speed and embedding capacity.

Cai *et al.* (2017) this work is discussed about dynamic blocking strategy which creates the various sized block. Wang *et al.'s (2015)* scheme of reversible data hiding simply chooses the maximum and minimum pixel block is taking and modified to embed data and pixel value order guarantees the reversibility. But in this work, choose a dynamic block of various sized and then further dividing flat block in four sub-block to gain larger embedding capacity. It can generate less high complexity for given embedding capacity. Still existing dynamic blocking strategy suffer from efficient and comprehensive drawback. But in this paper to reduce this drawback, an efficient and comprehensive blocking strategy develop known multistage blocking.

This paper is the extension of PVO-based Li *et al.'s* (2013), PVO-based scheme of Peng *et al.'s* (2014) and PVO-based scheme of Wang *et al.'s* (2015). In all these schemes only one or two bins of the prediction error are expanded to embed data. In Li *et al.'s* (2013) and Peng *et al*.'s (2014), large block size provide smaller embedding capacity whereas higher peak-signal-to-noise-ratio (PSNR). In Wang *et al.'s* (2015) generalized this as that the difference between the second smallest/largest pixel and the smallest/largest pixel lean to be smaller in a larger block. The experiments result revel

us that this scheme gains well superiority over Wang *et al.'s* (2015) scheme in complexity but also achieve low embedding distortion for given embedding capacity.

Zhou *et al* (2018) discussed improved reversible data hiding using pixel value grouping. In pixel value, grouping concept prediction error is generating in a block-by-block manner. The best advantage of this scheme is it reduces the number of a shifted pixel within the block. In this scheme, the embedding procedure switch from block to block and pixel are used to calculate the predicted value. Another advantage of this scheme is all the pixel are fully used and classified. The expandable prediction error obtained by utilizing pixel value in a smooth region of the image. As the analysis, it embed more capacity data with less distortion. This scheme is most effective to reduce redundancy in the block.

The main aim of the pixel value grouping is to reduce the number of shifted pixel and more and more pixel are used to embed secret data on low distortion. Pixel value grouping is a special type of prediction method wherein a modifiable set, pixel share one predicted value which is the reference pixel in pixel value grouping embedding procedure. In this scheme a special type of pixel selection strategy used. Mostly pixels selected in the smooth region of the image to embed more capacity data over low distortion. The experiments results of this scheme are good comparing with Fu *et al.'s* (2016), Li *et al.'s* (2013) and Qu *et al.'s* (2016) scheme. For these experiments, a different type of 512×512 grayscale image used. The better result of this work depends on the pixel selection strategy, specifically when embedding capacity is small. Pixel selected from the smooth reason of host image for data embedding. After those experiments result summarizing, this scheme also used for high-fidelity RDH for good performance.

Xiong *et al.* (2018) this work discussed reversible data hiding techniques using multi-pass pixel-value-ordering and pairwise prediction-error expansion. Firstly divided a cover image into a non-overlapped block, then find the largest and smallest pixel in block to get prediction error pair and 2D prediction error histogram. In this, the third-pixel value always not serve as the predicted value. It also works on the smooth block and normal block of the image in a different manner. For smooth block, information is considered and then expandable error obtained.

In this techniques, the basic idea was taken from Peng *et al.'s* (2014) improved pixel value ordering (2014) and ou *et al.'s (2016)* pixel value ordering based pairwise prediction error expansion. The experiments results are showing good performance comparing with other existing technique. In this for experiments 512 × 512 grayscale images used. In this scheme, prediction error generates a block-wise manner and the embedding procedure has to be for the different sized block. The blocks which have good performance, are select for embedding. This paper present a new reversible data hiding scheme based on optimized pixel-value-ordering based pairwise prediction error expansion. This technique generates a batter result and well utilize then original PVO-based pairwise PEE technique.

Singh *et al.* (2018) this work discussed about extended Peng *et al (2014)* reversible data hiding technique. Peng technique is the pixel value ordering reversible data hiding work in which cover media is dividing into equal size blocks. After dividing into equal size blocks, each block is sorted in ascending order. After sorted difference are calculated on the basis of largest and second maximum pixel value location. Peng *et al (2014)* provide good embedding capacity but if the predicted difference of blocks is negative then it's not embedded data. But in Singh *et al.'s* (2018) if the differences are negative then those blocks are used to utilize to create empty spaces and enhanced embedding capacity. Peng *et al.'s (2014)* failed when blocks are already sorted. If the block is already sorted then they are not used for embedding, this is the drawback of peng.et al method. But in Singh *et al.'s (2018)* this drawback is removed and used a sorted block for embed data to increase embedding capacity.

In this technique, used the formula of Li *et al.'s* (2014) and Peng *et al.'s (2014)* for embedding information in cover media. Using the embedding formula of both technique create the new formula for embed data. And drawback of the sorted block is removed. This technique is the improvement of the Peng *et al.'s* (2014) technique by adding a new formula in the embedding and extraction process. In this method, reduce redundancy in cover image to gain good performance in term of visual quality and embedding capacity. This technique is best for an image block size of 2 × 2. For correlated pixel, block size 2 × 2 is batter to embed more capacity data. But this technique also gives good result for larger sized blocks then Peng *et al.'s (2014)* its improve the PSNR close to 3.02 dB at a more embedding capacity approximate 20000 bits as compared to Peng *et al* (2014).

CHAPTER-3: RESEARCH ANALYSIS & METHODOLOGY

3.1: Gaps:

A gape is some missing part of the research that has been done or learned in any particular area. The gap is the information that learned from the research area. Information like what done till now and what to do in the future for the good result of any research study area. The gap gives a contribution to delivering good research knowledge of any area.

Now coming out to my research area, 'reversible data hiding for digital images' in which a specific procedure used to do research. In this research area for an image first, hide secret information in the image with a specific technique and then retrieve this secret information with this same technique keeping the security in mind. During a survey of this area, find different gaps like why this particular method used for this research area what are the weakness of this method and what to do to overcome this weakness.

There are so many techniques to perform reversible data hiding in better form but each technique has some advantage and some drawback. To overcome this drawback, many schemes are available. For reversible data hiding so many techniques like pixel value ordering, histogram shifting, histogram modification, and prediction error expansion, etc. in pixel value ordering scheme mainly first cover image divided into different size block and then examine the pixel within the block. Block size can be static or dynamic based on the technique developed by anyone. In PVO pixel within the block are sorted in ascending order and then find out first two maximum/minimum pixel to predict prediction error for vacant space and embed secret information or data. After complete embedding procedure, we get the marked image as an output. After that, there is a need to calculate peak-signal-to- noise-ratio to measure the noise or distortion between the original image and marked image. After calculating performance there is a need to extract data as well with the same technique which used for data embedding. In histogram shifting technique perform same like first find maximum and minimum pixel and then shift another pixel according to the maximum/minimum pixel. In some other technique of histogram shifting first, calculate prediction error and then make a

histogram of prediction error or modify histogram according to the need for embedding data.

After a survey on existing reversible data hiding scheme, realize there are so many gapes or missing part or weakness exist. Weakness like some technique is not working on an already sorted block of the image means block which is already sorted are not used for data embedding or vacant space or make room for data embedding. Some scheme is good for low capacity data but failed for more capacity data. The main Motive is to increase embedding capacity and give a good performance. In histogram-shifting based method in which the peak and minimum points of image histogram are modified to embed data. The drawback of this method is its embedding capacity is low and does not work well if the cover image has a flat histogram. Some of the methods use a pixel shifting method and some use static and dynamic block partitions scheme. Some methods drawback like they cannot embed data in the already sorted block. The gap in Peng *et al.'s* (2014) scheme which used for reversible data hiding. It is the extended work of Li *et al.'s* (2014) based on pixel value ordering. Li *et al.'s* (2014) scheme fail when a block is already sorted. Peng *et al.'s (2014).*

Overcome this problem to introduce a new method to calculate the difference between pixel and design new histogram modification strategy. This method embeds only one bit at a time so trying to improve this section and calculate noise level different from this method. Mainly trying to increase the embedding capacity without distortion or with very low distortion. In Peng *et al.* (2014) only, when prediction error 0 or 1 are used for data embedding, but in our method we used difference -1, doing this we can increase embedding capacity more than Peng *et al.* (2014). After implement this strategy, get good result as comparing to *Peng et al.'s* (2014), And this concept also used for further reversible data hiding techniques to get a good result and embed more capacity data in images.

3.2: Objective:

Reversible data hiding is a technique of hiding data in the image, video, and audio for security purpose. The reversibility is the most important part of this scheme means to extract the same data which are embedded without any loss. There are so many techniques for reversible data hiding but every technique has a drawback. Every new technique overcomes the weakness of the previous one. Preferred this technique which

has high embedding capacity and low image distortion while maintaining a security feature. High embedding capacity means, hide more secret data in images, video or audio. The objective of trying to increase embedding capacity in the cover image while maintaining its visual quality. Visual quality is determined by Peak signal to noise ratio value between the cover and marked images. We try to develop a good method for data hiding to increase data capacity and maintain peak signal to noise ratio. Whenever increase data capacity then PSNR decrease and distortion in the image is increased which is not good for image and security also. So in proposed work mainly focus on increasing data embedding capacity and maintain peak signal noise ratio and security of image. In today's network environment there are many tools to modify original content so for protection, need tight security so providing security is also an objective.

3.3: Methodology:

The methodology is a procedure performed on a research study. It consists of complete procedure and knowledge about the research study area. It is a strategy that defines the procedure which is used to perform our idea. Simply it gives an idea about what and which method is used by the researcher to complete their research goal. It is the most important part of a research which carries researcher idea in the right direction. Now discussed about which method or process took to carry out our research. Describe both the embedding and extraction algorithm process as follows.

3.3.1: Procedure for Data Embedding.

Step-1: Firstly take an image as a cover image and then divide the image into equal size non-overlapped block. Each block is sort in ascending order to get the index of the block.

Step-2: After dividing the image construct location map. Location map is constructed to check the underflow/overflow condition. If the value of the pixel is equal to zero then these pixel goes to underflow condition and if the value of the pixel is equal to 255 then these pixel goes under overflow conditions.

Step-3: In the third step, embedded a secret message into the cover image. Before embed data first, calculate the noise level of each block and define the threshold value to differentiate in which block data is embedded. Here some conditions define according to method knowledge over noise level or threshold for each block to embed

data. If the condition is satisfied for a block then these blocks are including in data embedding procedure.

Step-4: In this step, auxiliary information embedded in these block which remains from data carrying block and location map embedding also performs in this step.

3.3.2: Procedure for Data Extraction.

After embed data in the cover image, have to extract the same data also for reversibility and security purpose. For doing this have to follow some steps to extract data. These all are step are performed on a marked image. After completion of the embedding procedure, as a result get the marked image as an output.

Step-1: Take a marked image as an input and extracting auxiliary information which is embedded and extracts the location map also. Get location map by decompressing compressed location map. For doing this step, have knowledge about the size of the block, threshold value, and location of the last block where data embed.

Step-2: In this step, Extract sequence Slsb and restoration of image. This procedure is the same as data embedding procedure but in this, all work on the marked image which, made after data embedding procedure. Divide the marked image in non-overlapped block and then perform sorting on every block to find the index of each block. Here is also the need for threshold value and location map to extract the data from the marked image.

Step-3: In this step, Extract the message and after that restore the image. After performing this step successfully, get the original image as output and original data also without any change. So at last embedded data is successfully extracted and original image recovered.

CHAPTER-4: PROPOSED TECHNIQUES

In this chapter, discussed about the proposed method. Before discussing this first, summarize related work from which generated a new method. In today's networking environment, the security of data is an important issue. With the fast development of image processing and multimedia technology, there are different many tools available to modify content to the special purpose so security our content is important. Therefore data hiding technique is useful to provide security. Here discussed data hiding in image. So image data hiding is a scheme in which hide data in original or cover image and get a marked image as an output image. After hide data in the image, there is a need to recover the same data to maintain the visual quality of the image so reversible data hiding technique comes in mind. So to extract data completely from the marked image without any distortion, used a technique known as reversible data hiding technique. So there is much application of RDH like military and medical images. In recent, there are many RDH techniques available to improve visual quality and embedding capacity. Years ago, RDH techniques mainly work on lossless compression. Further, Fridrich *et al.'s* (2001) Develop a new concept in which cover image is compressed into smaller size and rest part of the image is used for data embedding.

After that a new technique difference expansion (DE) develop by Tian *et al.*'s (2003) in difference expansion scheme, the difference is calculated between two neighbour pixel and then according to these difference embed secret information. The benefit or advantage of this technique is to gain high embedding capacity with low distortion compared to another existing scheme. After all these schemes a new sorting of pixel technique is introduced by Kamastra and heijmans (2005). These techniques provide a high embedding capacity. After that, a new scheme histogram shifting technique is developed by Ni et *al.*'s (2006) in which the peak of the histogram is used to embed secret data ant rest part used for shifting.

To reduce the drawback of difference expansion (DE) and histogram shifting (HS), a new method prediction error expansion (PEE) scheme, introduced by Thodi and Rodriguez (2007). In these techniques, in which pixel data is embedded is determined by neighbouring correlated pixel. The prediction error is calculated by to minimum pixel or by two maximum pixels. And these difference is used to embed secret data or shifting. After that Li *et al.*'s (2013) improved the prediction error expansion (PEE) by

introducing a new pixel value ordering approach. In this, all the work is done on a block of equal size. Block may me different size depend on the technique which was used.

4.1: Related works:

4.1.1: Peng *et al.*'s (2014) work.

This part discussed Peng *et al.'s* (2014) pixel-value-ordering reversible data hiding technique. This technique is basically based on PVO (pixel value ordering) and PEE (prediction error expansion). In this method, simply divide the cover media into equal size blocks and then sort all the block in increasing orders to find maximum and minimum pixel value. According to maximum and minimum pixel, embed 1 bit of data. For each block, d_{max} and d_{min} for all block embed data where d_{max} and d_{min} are equal to 0 and 1. When d_{max} and d_{min} are less than zero or grater then 1, than no bit is embedded.

Here some notation used in Peng *et al.'s* (2014) techniques.

$d_{max} = x_u - x_v$, where

u=min (σ (n), σ (n-1)).

v=max (σ (n), σ (n-1)).

$d_{min} = x_u - x_v$, where

u=min (σ (1), σ (2)).

v=max (σ (1), σ (2)).

For all blocks, firstly calculate d_{max} and d_{min}, if the value of d_{max} and d_{min} is 0 or 1 then used these block for data embedding. These two value as a prediction error of blocks. The range of d_{max} and d_{min} is between (-∞, +∞).

For example, embedding data in the maximum pixel value of the block, after calculating d_{max} we have to modify $\bar{d}_{max}$ and $\bar{x}$ accordinaly. Where, $\bar{x}$ is a maximum pixel in the block. $\bar{d}_{max}$ is modified as

$$\bar{d}_{max} = \begin{cases} d_{max} + b, & if\ d_{max} = 1 \\ d_{max} + 1, & if\ d_{max} > 1 \\ d_{max} - b, & if\ d_{max} = 0 \\ d_{max} - 1, & if\ d_{max} < 0 \end{cases}$$

Where b is a binary bit {0, 1} which is used for embedding. The maximum pixel value is $\bar{x}_{\sigma(n)}$ modified as.

$$\bar{x}_{\sigma(n)} = \begin{cases} x_{\sigma(n)} + b, & if\ d_{max} = 1 \\ x_{\sigma(n)} + 1, & if\ d_{max} > 1 \\ x_{\sigma(n)} + b, & if\ d_{max} = 0 \\ x_{\sigma(n)} + 1, & if\ d_{max} < 0 \end{cases}$$

For minimum pixel value of the block, modification has also some formula like first calculate difference d_{min} value for all block.

$d_{min} = x_s - x_t$, where

s = min (σ (1), σ (2)).

t = max (σ (1), σ (2)).

And then difference $\bar{d}_{min}$ and $\bar{x}$ is modified as

$$\bar{d}_{min} = \begin{cases} d_{min} + b, & if\ d_{min} = 1 \\ d_{min} + 1, & if\ d_{min} > 1 \\ d_{min} - b, & if\ d_{min} = 0 \\ d_{min} - 1, & if\ d_{min} < 0 \end{cases}$$

Where b is data bit which is used to embed and at last final minimum pixel value of the block is modified as

$$\bar{x} = \begin{cases} x_{\sigma(1)} - b, & if\ d_{min} = 1 \\ x_{\sigma(1)} - 1, & if\ d_{min} > 1 \\ x_{\sigma(1)} - b, & if\ d_{min} = 0 \\ x_{\sigma(1)} - 1, & if\ d_{min} < 0 \end{cases}$$

In this above scheme, only bin 0 and 1 are used for data embedding but bins greater than 1 and less than zero not used for data embedding. Means if the value of d_{max} and d_{min} is zero or one then embed data otherwise not embed.

4.1.2: Li *et al.*'s (2013) work:

This technique is also based on a pixel value ordering approach. In this scheme, predict the maximum and minimum value of a block by using the second maximum and second minimum pixel value of the block. Use this prediction to check the interconnection or relation between neighbour pixels. For data embedding, predicted pixel value used.

In this scheme, firstly the cover image or original image is divided into non-overlapped blocks of equal size. After dividing the block into equal size, the value of the block is sorting in ascending order. Like for block R, the pixel value of block R, sort in

ascending order (R_1…….R_n) and these all value stored as ($R_{\sigma(1)}$.. ……$R_{\sigma(n)}$). Where σ (1) is the smallest pixel value of block and σ (n) is the largest pixel values of the block. Where (σ (1)……. σ (n)) is an index of the sorted pixel value of the block. After all these calculation, prediction error PE_{max} is calculated. PE_{max} is the difference between the maximum pixel value and the minimum pixel value of the block. For blocks, need to calculate the prediction error $PE_{max.}$ According to the value of PE_{max} we embed data in the block. For maximum value modification, calculate PE_{max} and for minimum modification, calculate $PE_{min.}$ The formula for calculating PE_{max} is.

$PE_{max} = R_n - R_{n-1}$

Where R_n is the largest pixel value of the block

R_{n-1} is second largest pixel value of the block.

The value of PE_{max} is always positive and the range in between (0, +∞). After the calculation of PE_{max} , generate a histogram of the value of $PE_{max.}$ If the value of PE_{max} =1, generally it's called bin_1 of the histogram.

If PE_{max} = 1, this is also the histogram peak. In this scheme, there are two regions, the inner region, and the outer region. Inner region bin used to embed secret data and outer region bin used for shifting. When the value of PE_{max}=1, then it's defined as an inner region and if the value of PE_{max} > 1, then define as an outer region. Largest pixel of each block and prediction error $\overline{PE}_{max}$ is modified as

$$\overline{PE}_{max} = \begin{cases} PE_{max} \quad , \ if\ PE_{max} = 0 \\ PE_{max} + b \ \ if\ PE_{max} = 1 \\ PE_{max} + 1 \ \ If\ PE_{max} > 1 \end{cases}$$

And the $\bar{R}_n$ is modified as

$$\bar{R}_n = \begin{cases} R_n, & If\ \mathrm{PE}_{max} = 0 \\ R_n + b, & If \mathrm{PE}_{max} = 1 \\ R_n + 1, & if\ \mathrm{PE}_{max} > 1 \end{cases}$$

Where b is a binary bit to be embedded. After doing these all process we get the marked image as an output.

4.2-Proposed Method:

In this section, discussed about proposed method. The proposed method is the improvement of Peng *et al.'s* (2014) scheme. In Peng et al.'s (2014) only when the value of d_{max} and d_{min} of blocks is zero or one then these blocks are utilized for data embedding. But in the proposed method when the value of d_{max} and d_{min} is -1 then these blocks also used for data embedding. Due to this improvement in the result and also increase the embedding capacity. The main motive is to increase the embedding capacity. Proposed method not only bin zero and one used for data embedding but bin -1 is also used for data embedding. The main advantage to do this is to increase data capacity while maintaining the visual quality of images. The reversibility is a guaranty for the proposed method. The complete procedure of embedding and extracting for minimum and the maximum pixel value is completely described in the next section with notation which is used in proposed method and compression and results also showing in the next section.

For the proposed method first, take a cover image and then divide the cover image into non-overlapped equal size blocks. After that for sort block in ascending order to get ($x_{\sigma(1)}$…….$x_{\sigma(n)}$). Where $x_{\sigma(1)}$ is the minimum pixel value and $x_{\sigma(n)}$ is the maximum pixel value. The value $x_{\sigma(1)} \leq$…….$\leq x_{\sigma(n)}$. For every block, calculate prediction error d_{min} and d_{max}. According to these value, data is embedded. Where σ (1), σ (2),…… σ(n) is the ascending order number of a pixel within the block. For example if a block contain values 50,40,70,55. After sorting this block order is 40,50,55,70 and value of (σ(1), σ(2), σ(3), σ(4)) is (2,1,4,3).

First, explain the data embedding and extraction procedure for minimum pixel modification and notation used for the procedure.

$d_{min} = x_u - x_v$, where

u = min (σ (1), σ (2))

v = max (σ (1), σ (2))

T =threshold value, the value of T can be 4, 8, 18…etc. According to the procedure. In the proposed method, the Threshold value is 8. NL (noise level) which is calculated for every block. If the noise level of block is less than the define threshold value then these

blocks are smooth block and if grater then threshold then these blocks are rough block. The formula for calculating noise level for proposed work is

NL = $x\sigma_{(n-1)}$-$x_{\sigma(2)}$ for block size 2×2.

4.2.1: Embedding Procedure for Smallest Value Modification.

After calculating the d_{min} for all block we have to modify $\bar{d}_{min}$ and $\bar{x}_{\sigma(1)}$ for every block which used in embedding procedure. The formula for calculate these two value is given below

$$\bar{d}_{min} = \begin{cases} d_{min} + b, & if\ d_{min} = 1 \\ d_{min} + 1, & if\ d_{min} > 1 \\ d_{min} - b, & if\ d_{min} = 0 \\ d_{min} - b\ , & if\ d_{min} = -1 \\ d_{min} - 1, & if\ d_{min} < -1 \end{cases}$$

$$\bar{x}_{\sigma(1)} = \begin{cases} x_{\sigma(1)} - b\ , & if\ d_{min} = 1 \\ x_{\sigma(1)} - 1, & if\ d_{min} > 1 \\ x_{\sigma(1)} - b, & if\ d_{min} = 0 \\ x_{\sigma(1)} - b\ , & if\ d_{min} = -1 \\ x_{\sigma(1)} - 1, & if\ d_{min} < -1 \end{cases}$$

After embed data, we have to extract the same data also. So the extraction procedure for minimum modification is given below.

4.2.2: Extraction Procedure for Smallest Value Modification

In this section, describe the proposed work data extraction procedure for minimum value modification. After extracting data, restored the original image. Extract data and embedding data should have the same value. In extraction procedure, all work done on the marked image which gets after data the embed procedure. To do the extraction process, have to use some notation which describes below.

$\bar{d}_{min}$ = y_s-y_t, where

s = min (σ (1), σ (2))

t = max (σ (1), σ (2))

If $\bar{d}_{min} > 0$, we know that σ (1) > σ (2), so s = σ (2), t = σ (1).

- If $\bar{d}_{min}$ ==1, then hidden bit b = $\bar{d}_{min}$ – 1, and original minimum value is $x_{\sigma(1)}$ = y_t +b.
- If $\bar{d}_{min}$ ==2, bit b = $\bar{d}_{min}$ – 1, original value is $x_{\sigma(1)} = y_t$ +b.
- If $\bar{d}_{min}$ > 2. Then there is no hidden bit and othe riginal value is $x_{\sigma(1)} = y_t$ +1.

If $\bar{d}_{min} \leq 0$, then σ (1) < σ (2), so s = σ (1), t = σ (2). I represent i^{th} number block.

- If $\bar{d}_{min}$ ==0, hidden bit b = - ($\bar{d}_{min}$), and original value is $x_{\sigma(1)} = y_s$+b.
- If ($\bar{d}_{min}$ (i) ==-1 && d_{min} (i) ==0), bit b = - ($\bar{d}_{min}$ (i)), original is $x_{\sigma(1)} = y_s$+b.
- If ($\bar{d}_{min}$ (i) ==-1 && d_{min} (i) ==-1), bit b = -$\bar{d}_{min}$ (i)-1, is $x_{\sigma(1)} = y_s$+b.
- If $\bar{d}_{min}$ ==-2, then bit b = $\bar{d}_{min}$ -1, and original is $x_{\sigma(1)} = y_s$+b.
- If $\bar{d}_{min}$ < -2, then no hidden bit and original is $x_{\sigma(1)} = y_s$+1.

4.2.3- Embedding Procedure for Largest Value Modification:

Here discussed embedding procedure for the proposed method and notation which are using for embed data. d_{max} is calculated for every block and the blocks have d_{max} value 0,1 or -1 then these blocks are used to embed data. The formula for d_{max} is given below.

$d_{max} = x_u - x_v$, where

u=min (σ (n), σ (n-1)).

v=max (σ (n), σ (n-1)).

Embedding data in the maximum pixel value of the block, after calculating d_{max} we have to modify $\bar{d}_{max}$ and $\bar{x}_{\sigma(n)}$ accordingly as.

$$\bar{d}_{max} = \begin{cases} d_{max} + b, & if\ d_{max} = 1 \\ d_{max} + 1, & if\ d_{max} > 1 \\ d_{max} - b, & if\ d_{max} = 0 \\ d_{max} - b\ , & if\ d_{max} = -1 \\ d_{max} - 1, & if\ d_{max} < -1 \end{cases}$$

$$\bar{x}_{\sigma(n)} = \begin{cases} x_{\sigma(n)} + b\ , & if\ d_{max} = 1 \\ x_{\sigma(n)} + 1, & if\ d_{max} > 1 \\ x_{\sigma(n)} + b, & if\ d_{max} = 0 \\ x_{\sigma(n)} + b\ , & if\ d_{max} = -1 \\ x_{\sigma(n)} + 1, & if\ d_{max} < -1 \end{cases}$$

Where b is binary data bit (0, 1), to be embedded.

4.2.4- Extraction Procedure for Largest Modification.

This section, describe the data extraction method for maximum value modification and notation to be used.

$\bar{d}_{max} = y_u - y_v$, where

u = min (σ (n), σ (n-1))

v = max (σ (n), σ (n-1))

If $\bar{d}_{max} > 0$, Then σ (n) < σ (n-1), so u = σ (n), v = σ (n-1).

- If $\bar{d}_{max} == 1$, then hidden bit b = $\bar{d}_{max} - 1$, and original minimum value is $x_{\sigma(n)} = y_u - b$.
- If $\bar{d}_{max} == 2$, bit b = $\bar{d}_{max} - 1$, original value is $x_{\sigma(n)} = y_u - b$.
- If $\bar{d}_{max} > 2$. Then there is no hidden bit and original value is $x_{\sigma(n)} = y_u - 1$.

If $\bar{d}_{max} \leq 0$, then σ (n) >σ (n-1), so u = σ (n-1), v= σ (n). I represent i^{th} number block.

- If $\bar{d}_{max} == 0$, hidden bit b = - ($\bar{d}_{max}$), and original value is $x_{\sigma(n)} = y_v - b$.
- If ($\bar{d}_{max}(i) == -1$ && $d_{max}(i) == 0$), bit b = -($\bar{d}_{max}(i)$), original is $x_{\sigma(n)} = y_v - b$.
- If ($\bar{d}_{max}(i) == -1$ && $d_{max}(i) == -1$), bit b = -$\bar{d}_{max}(i)$-1, is $x_{\sigma(n)} = y_v - b$.
- If $\bar{d}_{max} == -2$, then bit b = $\bar{d}_{max}$ -1, and original is $x_{\sigma(n)} = y_v - b$.
- If $\bar{d}_{max} < -2$, then no hidden bit and original is $x_{\sigma(n)} = y_v - 1$.

Where i, the number of i^{th} blocks.

4.3- Data Embedding and Extracting Procedure for the Proposed Method:

4.3.1: Data Embedding Method:

Here, explain the complete procedure for embedding and extraction. First of all, calculate the noise level for every block. For example, we take a block x of size 2×2 then noise level of block is calculated as

$NL = x\sigma_{(n-1)} - x_{\sigma(2)}$

Define a threshold value, T, in the proposed method select those blocks, satisfying NL<T condition. Generally for blocks where NL<T then these blocks considered as

smooth block and rest blocks consider as a rough block. We take smooth block for data embedding and rough block not used. Here explain the complete method for both maximum and minimum modification. We explain this algorithm in steps.

Step-1: In the first step basically take an image as a cover image and then divide the cover image into blocks. Divide image in such a manner that each block contains n pixels. After that sort blocks in ascending order to get ($x_{\sigma(1)}$……$x_{\sigma(n)}$).

Step-2: In this step, construct a location map. Check under/overflow situation for the block. If the block having pixel value grater then 255 then these blocks consider as an overflow and block having pixel value less than zero are considered as underflow. For every block x_i, if $x_{\sigma(1)}$=0 or $x_{\sigma(n)}$ = 255, then LM(i) = 1, otherwise location map LM(i) = 2. For block x_i, if LM (i) = 1 then these blocks include in embedding procedure and rest blocks exclude. After location map construction, it lossless compressed using arithmetic coding to get CLM to cut its length. The length of CLM is denoted as l_{CLM}.

Step-3: In this step secret message is embedded. For embedding, required some parameter like threshold value, noise level. For block x_i

If LM (i) =2, then these blocks point as over/underflow and nothing to do.

If LM (i) =1, and NL (i) > T, then these block point as noisy block and we have to nothing to do.

If LM (i) = 1 and NL (i) < T, then those blocks are selecting for data embedding. These blocks are known as a smooth block. d_{min} and d_{max} are calculated and according to the value of d_{max} and d_{min}, the minimum and maximum pixel value of blocks are modified.

When secret data completely embedded then this step stops and record p_{end} for auxiliary information.

Step-4: After secret data completely embedded, the auxiliary information is embedded in the rest part of the original image. Rest block means (X_{end} ……X_n), where end denotes last block index where data embedded and n denote the total block. To do this first, record the LSB of first several pixels. Record LSB using $12 + 2\lceil \log_2 N \rceil + l_{CLM}$ pixel of the image to obtain S_{lsb}. For doing this required some parameter like

- Block size n.
- Threshold value T.

- Last position P_{end} $\lceil \log_2 N \rceil$.
- Compressed location map length $L_{clm}\lceil \log_2 N \rceil$.

Finally, the auxiliary information is embedded in the rest block of the image using the procedure of data embedding.

4.3.2: Data Extracting Method: After embedding data, extract the same data also and guarantee of restore of the original image.

Step-1: Now all the work on the marked image which gets after embedding. First of all, extract location map and auxiliary information. Same as embedding here also read LSB of several pixels of the marked image. After extract auxiliary information, decompress location map.

Step-2: In this step, extract the secret message and binary sequence S_{lsb} and after that restore the image. This procedure is the same as data embedding procedure but this work is done on the marked image. Marked image is divided into equal size non-overlapped block ($Y_1 \ldots\ldots Y_n$) and after that sort block in ascending order. From ($Y_1 \ldots\ldots Y_{end}$) we have to extract the secret message and from ($Y_{end} \ldots Y_n$) we have to extract binary sequence $S_{lsb.}$

If LM (i) = 1 and NL < T then extract data and binary sequence.

If LM (i) = 2, then nothing to do.

Step-3: In this step, restored our original image after extracting secret data and binary sequence. LSB of first several pixels replaced by S_{lsb} using step-2. From ($Y_1 \ldots\ldots Y_{end}$) we have to extract the secret message and from ($Y_{end} \ldots Y_n$) we have to extract binary sequence $S_{lsb.}$ Finally, we get our original image after doing all the above processes.

4.4- Flow Chart for Embedding and Extracting.

In this section, the proposed method is described by the flow chart for both data embedding and extracting. The process or steps used for data embedding and extracting is described as

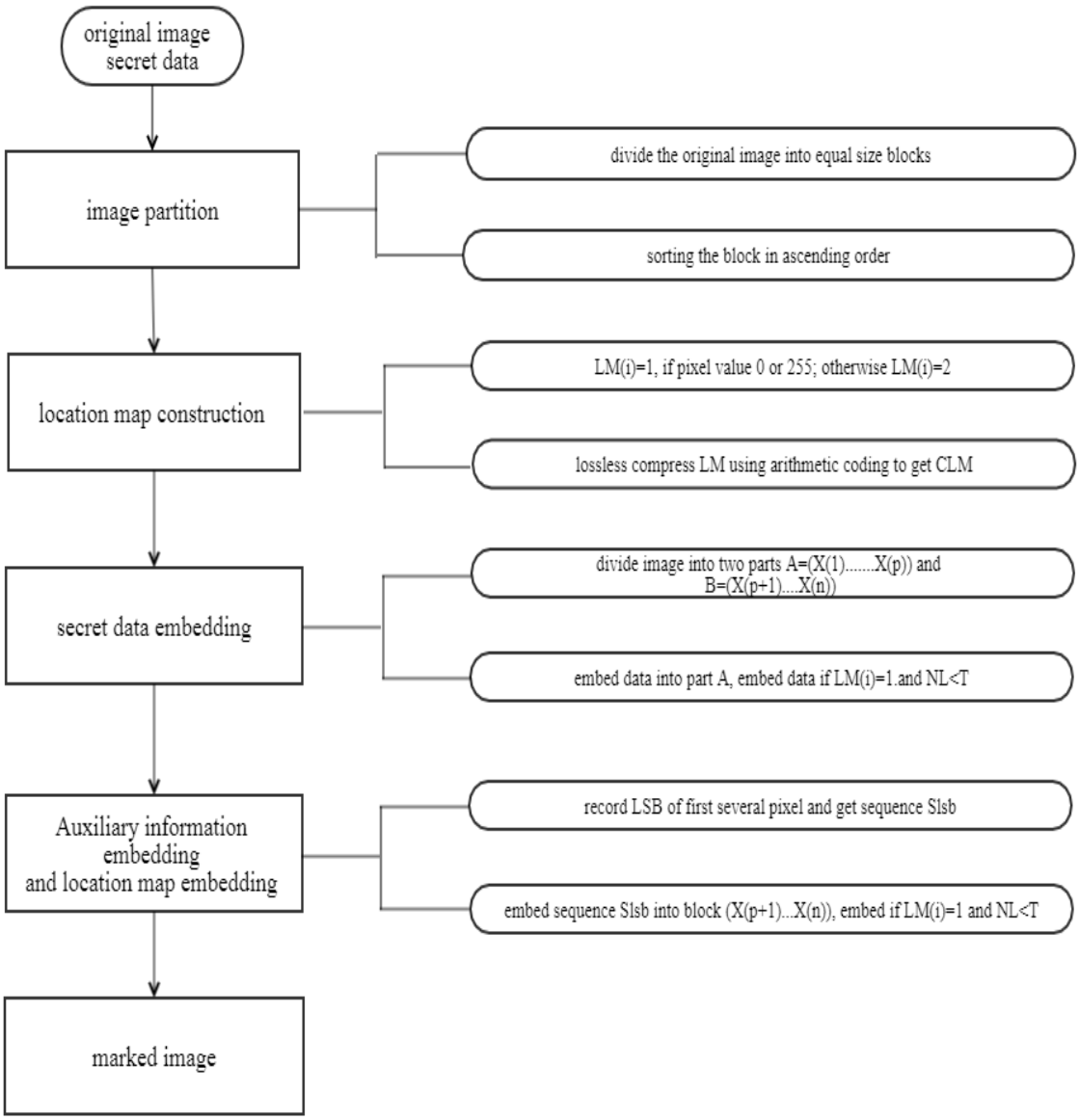

Fig. 4.1. Data Embedding Flow Chart

For data embedding, take a cover image as an input. After doing all the step explained in the previous section using defined parameters. After embedding, get the marked image as an output.

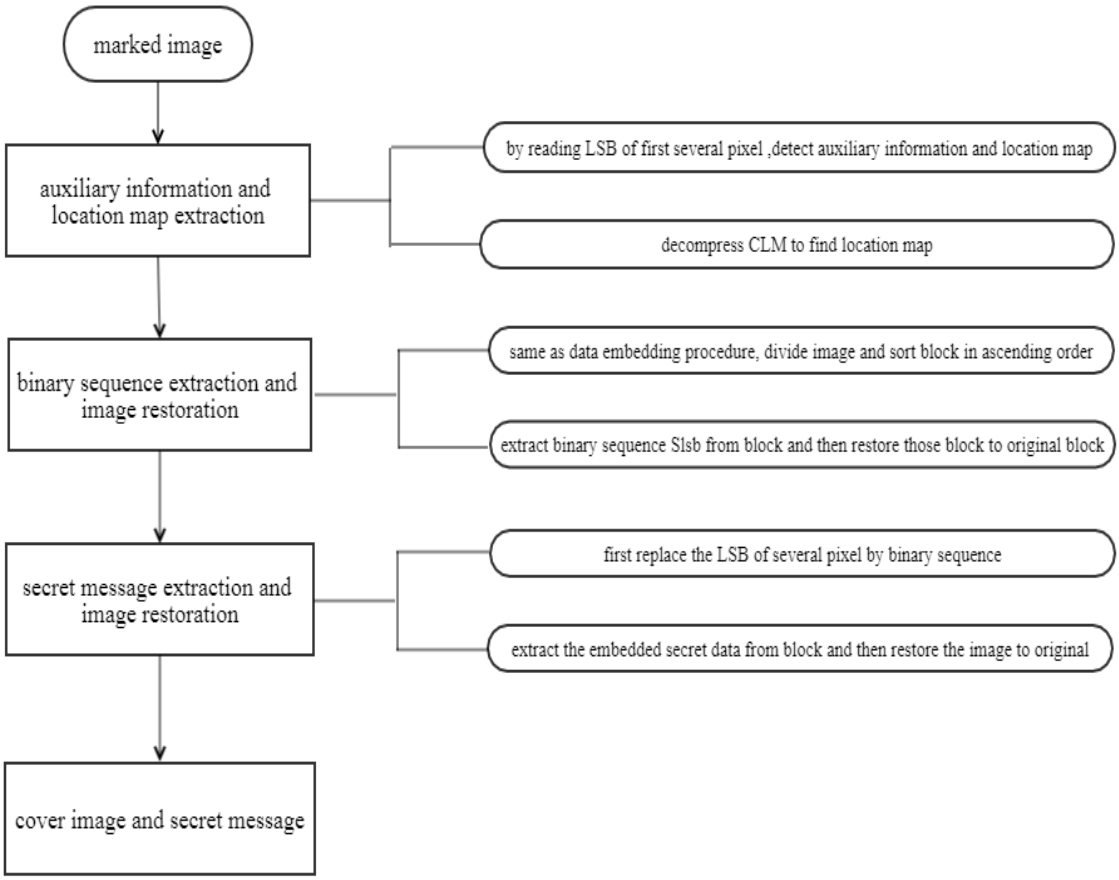

Fig. 4.2. Data Extraction Flow Chart

CHAPTER-5: EXPERIMENT RESULT

This section, present experimental result of proposed reversible data hiding techniques based on PVO (pixel value ordering) scheme. In this technique, the first image is dividing into the block and then select a block to for embed data. The proposed technique is implemented using MATLAB R2017b. for experiments, we take some standard image from the USC-SIPI database. We did an experiment on some image like Lena, baboon, Airplane (F-16), Barbara, peppers, fishing boat, man, and sailboat. All the images are grayscale image and size of images instead of man image are 512×512. The size of man image is 1024×1024. We divide the image in 2×2 block size. Means we perform all the experiments on block size 2×2. Proposed Reversible data hiding based on pixel value ordering has been implemented in MATLAB 2017b version, on a system having configuration 2.40 GHz processor, 4GB RAM, and 64-bit operating system. First, showing our experiments results on different images separate in tabular format and in graphical format. After that, showing the comparing of proposed scheme result with other existing techniques. After that, also shown from which techniques we take our concept and how the proposed technique is better than other existing technique and from which factor the proposed technique is better than other techniques. Factor like some techniques is given good data embedding capacity and some are the batter in form of PSNR.

Whenever data is embedded into the image then distortion occurs in the image. By the PNSR value, we can find how much distortion present in the image. In the proposed technique, for data embed we divide the image into blocks. If take larger block size then its batter in form of PSNR means low distortion and if we take smaller block size, then it's better in the form of data embedding capacity. In the proposed technique, we perform on both block size and we present result on only smaller block size.

Table-1: PSNR of Lena Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of the Marked image In (dB)	Payload(data capability) in bits
Lena image	72.15	1000
Lena image	67.4	3000
Lena image	64.49	5000
Lena image	61.50	7000
Lena image	60.68	10000
Lena image	58.46	13000
Lena image	57.75	15000
Lena image	56.49	20000

Fig. 5.1. Graphical Representation of PSNR of Lena Image

Table-2: PSNR of Peppers Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
Peppers	68.49	1000
Peppers	64	3000
Peppers	62.64	5000
Peppers	61.15	7000
Peppers	59	10000
Peppers	57.71	13000
Peppers	56.65	15000
Peppers	55.35	20000

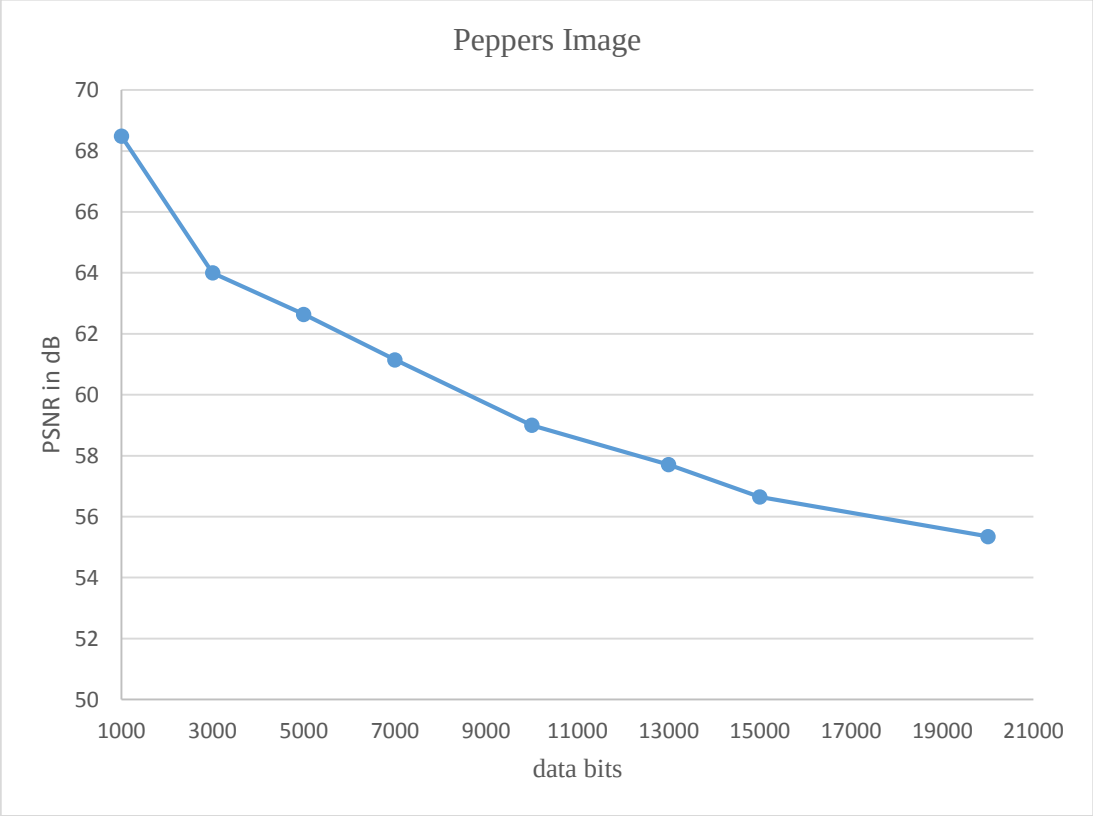

Fig. 5.2. Graphical Representation of PSNR of Peppers Image

Table-3: PSNR of Sailboat Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
Sailboat	68.07	1000
Sailboat	65.53	3000
Sailboat	63.63	5000
Sailboat	60.30	7000
Sailboat	58.62	10000
Sailboat	56.86	13000
Sailboat	56.18	15000
Sailboat	55.66	16675

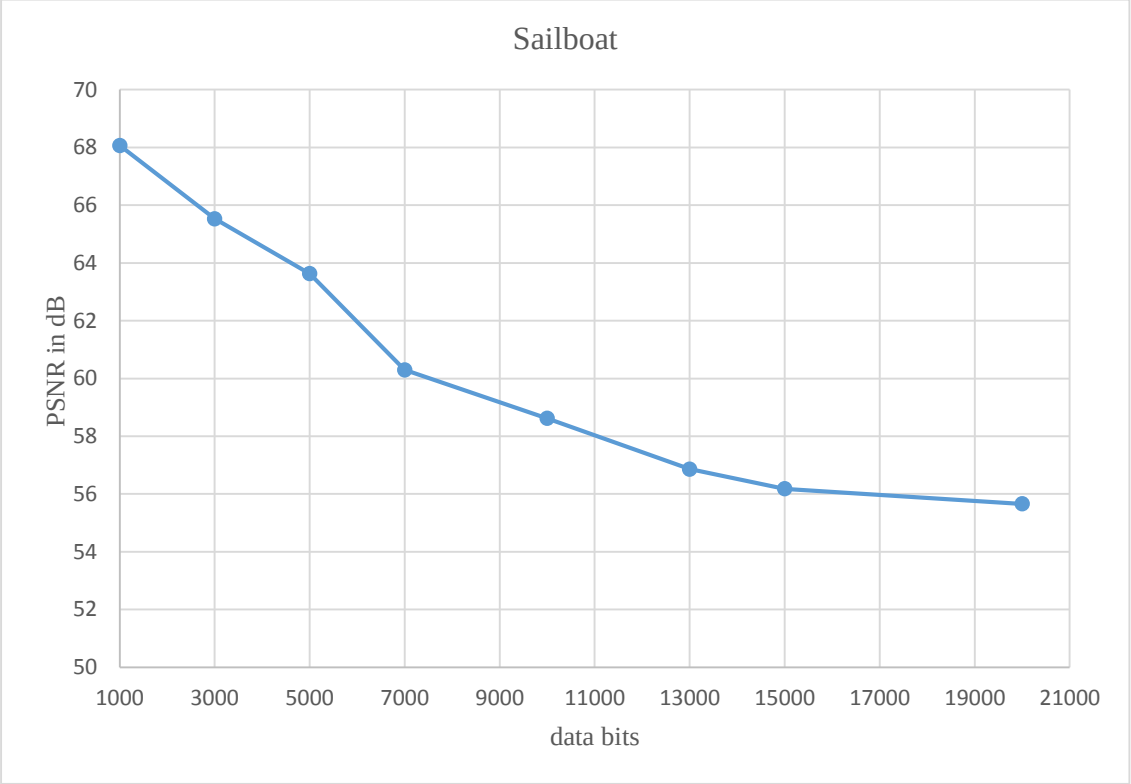

Fig. 5.3. Graphical Representation of PSNR of Sailboat Image

Table-4: PSNR of Airplane (F-16) Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
F-16	69.88	1000
F-16	67.23	3000
F-16	65.41	5000
F-16	64.06	6000
F-16	62.75	10000
F-16	60.05	12000
F-16	59.30	15000
F-16	57.75	20000

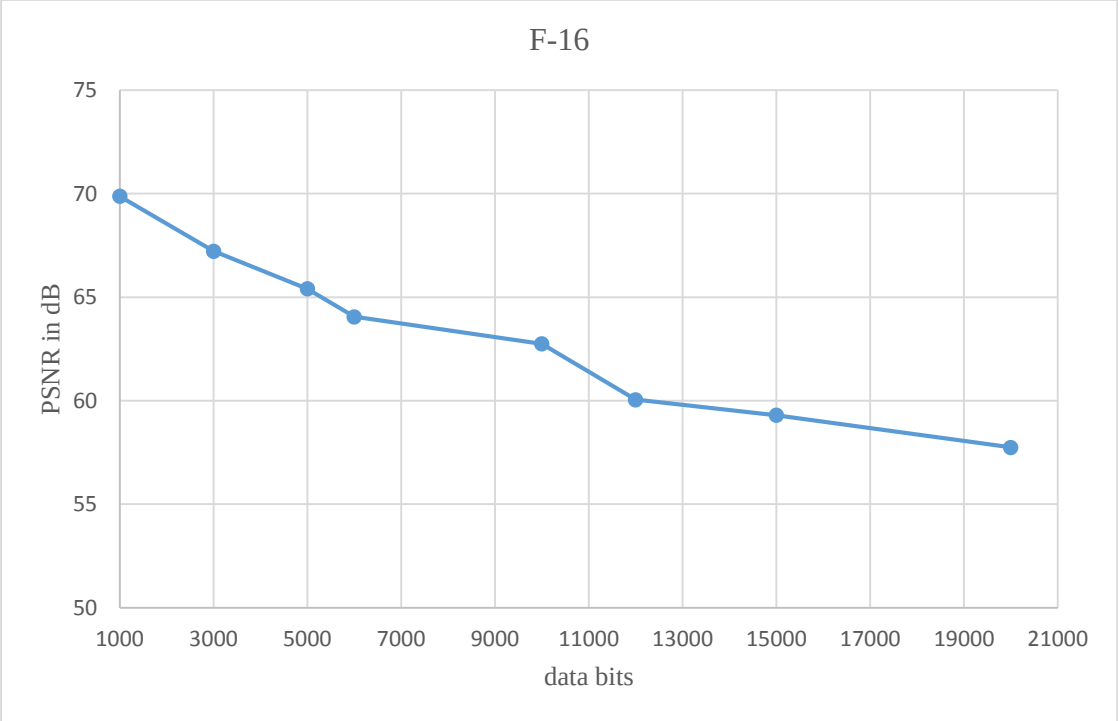

Fig. 5.4. Graphical Representation of PSNR of F-16 Image

Table-5: PSNR of Fishing Boat Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
Fishing boat	70	1000
Fishing boat	64	3000
Fishing boat	61.14	5000
Fishing boat	60	7000
Fishing boat	58.09	10000
Fishing boat	57.08	13000
Fishing boat	56.18	15000
Fishing boat	55.66	16500

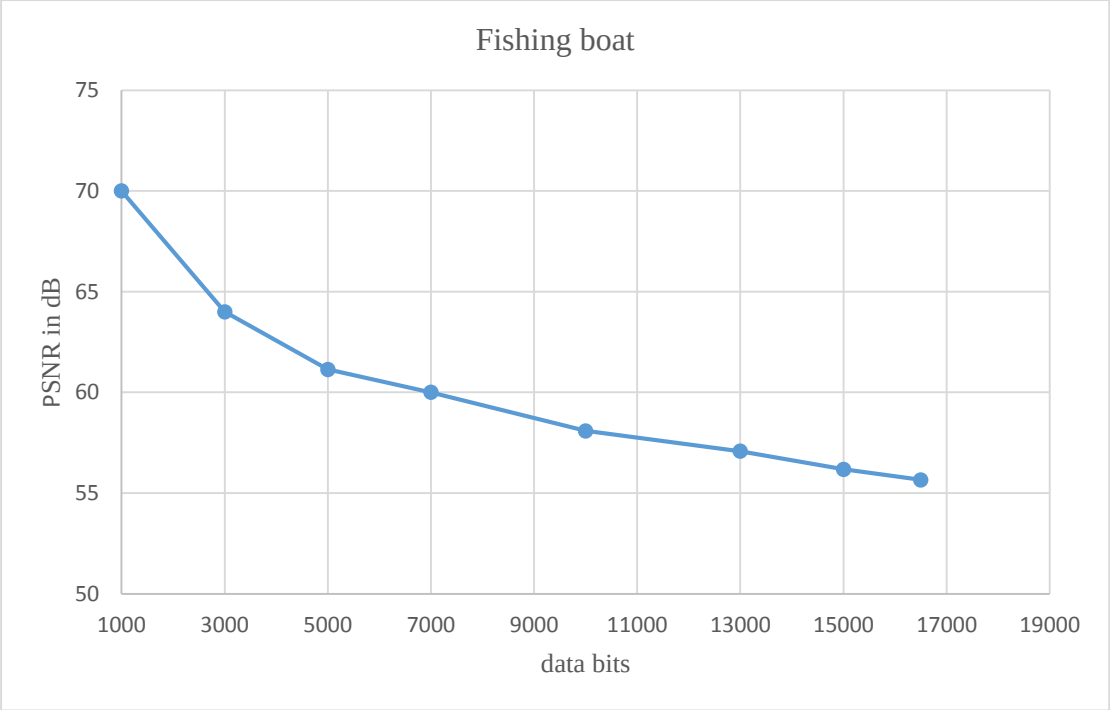

Fig. 5.5. Graphical Representation of PSNR of Fishing Boat Image

Table-6: PSNR of Barbara Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
Barbara	69.61	1000
Barbara	65	3000
Barbara	63.53	5000
Barbara	62.71	7000
Barbara	60.72	10000
Barbara	57.76	13000
Barbara	57.06	15000
Barbara	56.24	18000

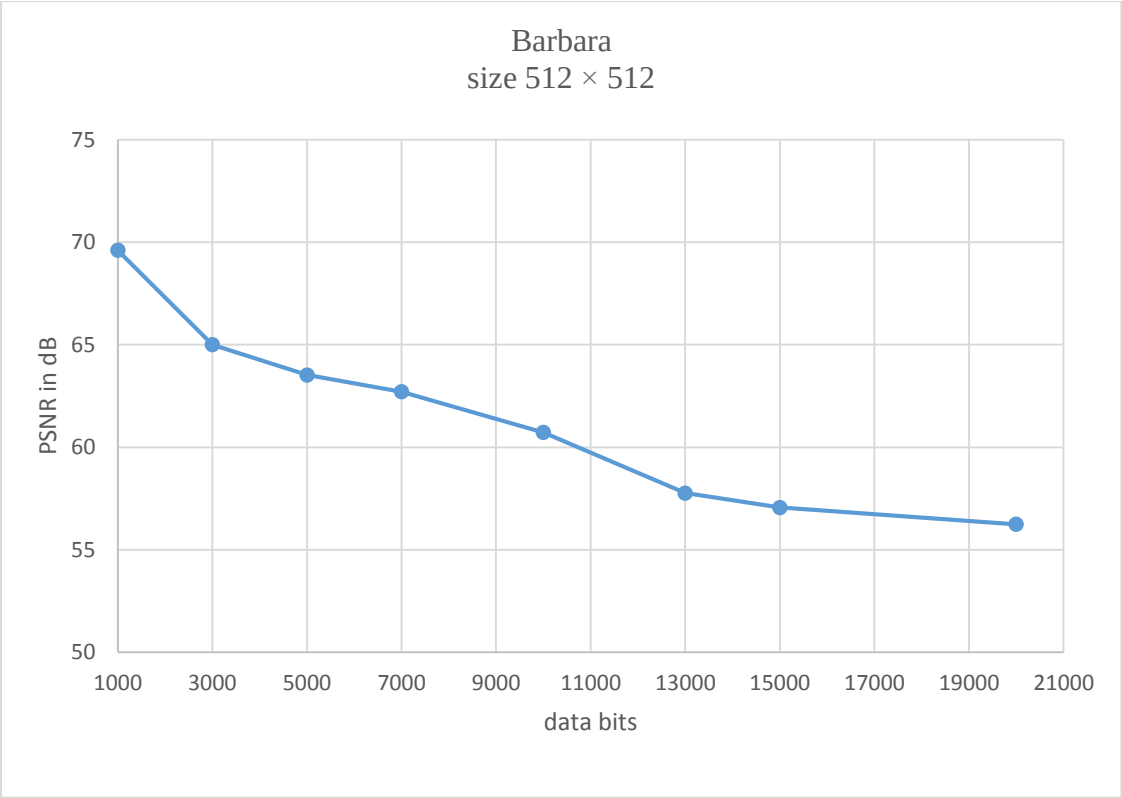

Fig. 5.6. Graphical representation of PSNR of Barbara image

Table-7: PSNR of Mandrill (Baboon) Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
Mandrill	64	1000
Mandrill	60.05	3000
Mandrill	59.50	5000
Mandrill	56.81	7000
Mandrill	55.73	10000
Mandrill	55.10	13000
Mandrill	54.06	15000
Mandrill	53.24	20000

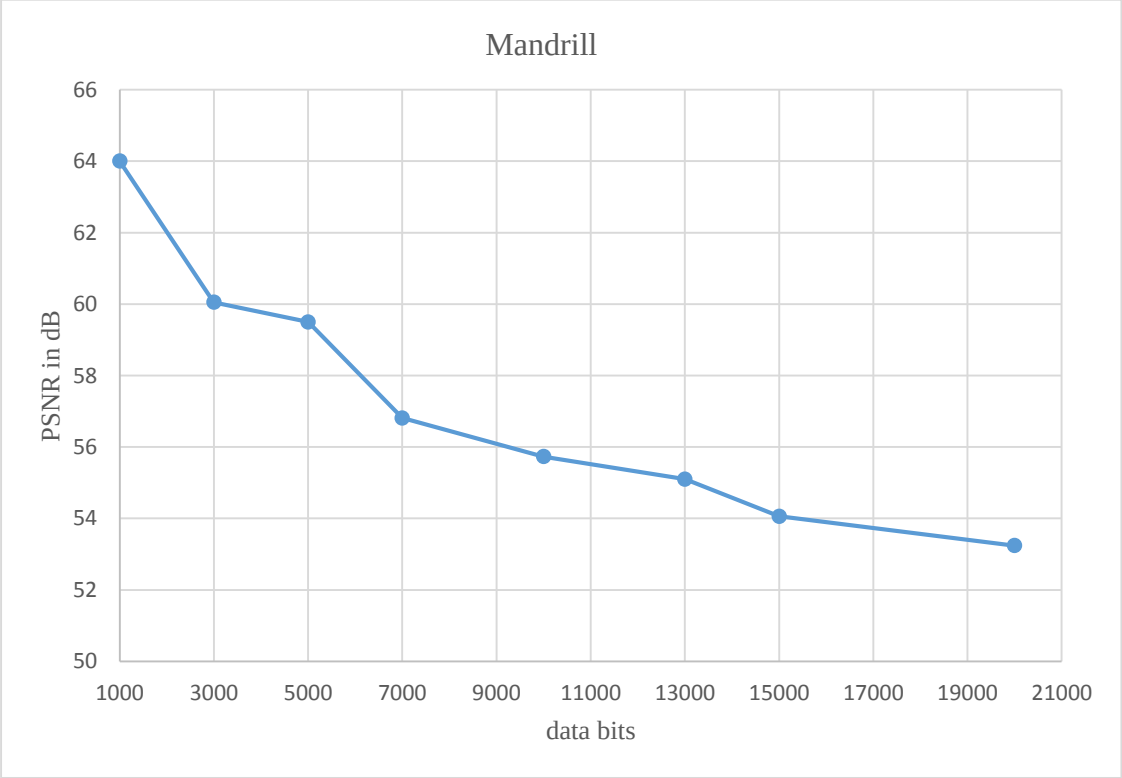

Fig. 5.7. Graphical Representation of PSNR of Mandrill (Baboon) Image

Table-8: PSNR of House Image at Different Data Capacity.

Name of the image (512 × 512)	PSNR of Marked image In (dB)	Payload(data capability) in bits
house	74.07	1000
house	68.66	3000
house	66.39	5000
house	64.70	7000
house	62.28	10000
house	59.37	13000
house	58.55	15000
house	57.23	20000

Fig. 5.8. Graphical Representation of PSNR of House Image

5.1: Comparison of the Proposed Method Result with Existing Method.

In this section, comparing the proposed method result with the existing technique. Comparing results of some standard image like Lena, airplane (f-16), etc. grayscale image of size 512 × 512. Compare our result for an embedding capacity of 10,000 bits with other technique. Show below in tabular format.

For comparison, the embedding capacity range from 5000 bits to 20000 bits are take and compare the result. The PSNR of the proposed scheme is good then other and it remains 54 dB for all standard image in all cases. In the proposed method embedding capacity increased by more than 12000 bit for the standard image. For comparison to another exist scheme, in the proposed method embedding capacity is more and PSNR values are well. Our proposed method is best when image divided into 2 × 2 size block. Different data embedding capacity are taking starting from 5000 bits and up to 20000 bits. For comparison, perform experiments on some standard image showing in tables.

Table-9: Comparison of PSNR for an EC of 10000 bits.

Name of the image	Proposed method	Peng *et al.* [2014]	Li *et al.* [2013]	Sachnev *et al.* [2009]	Hong *et al.* [2012]	Tsai *et al.* [2013]
Lena	60.68	60.47	59.86	58.18	58.77	58.45
Baboon	55.73	53.55	53.50	54.15	52.90	51.97
Airplane(F-16)	62.75	62.96	61.61	60.38	62.07	58.50
Fishing boat	58.09	58.27	57.85	56.15	56.53	54.88
Sailboat on lake	58.62	58.87	58.18	56.65	57.79	55.55
Barbara	60.72	60.54	59.98	58.15	58.34	56.16
peppers	59.0	58.98	58.55	55.55	56.04	55.34

All the result, from different embedding scheme, are performed on the image of size 2 × 2. Also showing the comparison between PSNR of different five scheme in graphical format for batter understanding.

According to the above result, the proposed method performs well and it is better from some reversible data hiding scheme. For doing this it can achieve larger embedding capacity and get well result with low distortion. All the work are done on grayscale image of size 512 × 512. For comparison to Peng *et al.'s* (2014) the proposed method give more PSNR for some standard images and for some images its equal of minor less. But in proposed scheme hide more secret data than Peng *et al.'s* (2014) in term of data capacity our method is better than Peng *et al.'s* (2014).

Now showing the comparison of proposed method result with different reversible data hiding scheme for different data capacity in graphical format. Comparing the proposed method result with Peng *et al.'s* (2014),

Li *et al.'s* (2013), Sachnev *et al.'s* (2009) , Hong *et al.'s* (2012) and Tsai *et al.'s* (2013).

Table-10: Performance Comparison of Lena Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al* (2014)	Li *et al.*'s (2013)	Sachnev *et al* (2009)	Hong *et al* (2012)	Tsai *et al.* (2013)
5000	64.49	64.0	63	62.50	62.30	62.70
7000	61.50	61.0	61.50	61.45	61.45	61.20
10000	60.68	60.47	59.89	58.18	58.77	58.45
13000	58.46	58.0	58.0	57.25	56.45	57.0
15000	57.75	57.10	57.30	56.30	56.20	56.20
20000	56.49	56.30	56.0	54.50	55.0	54.15

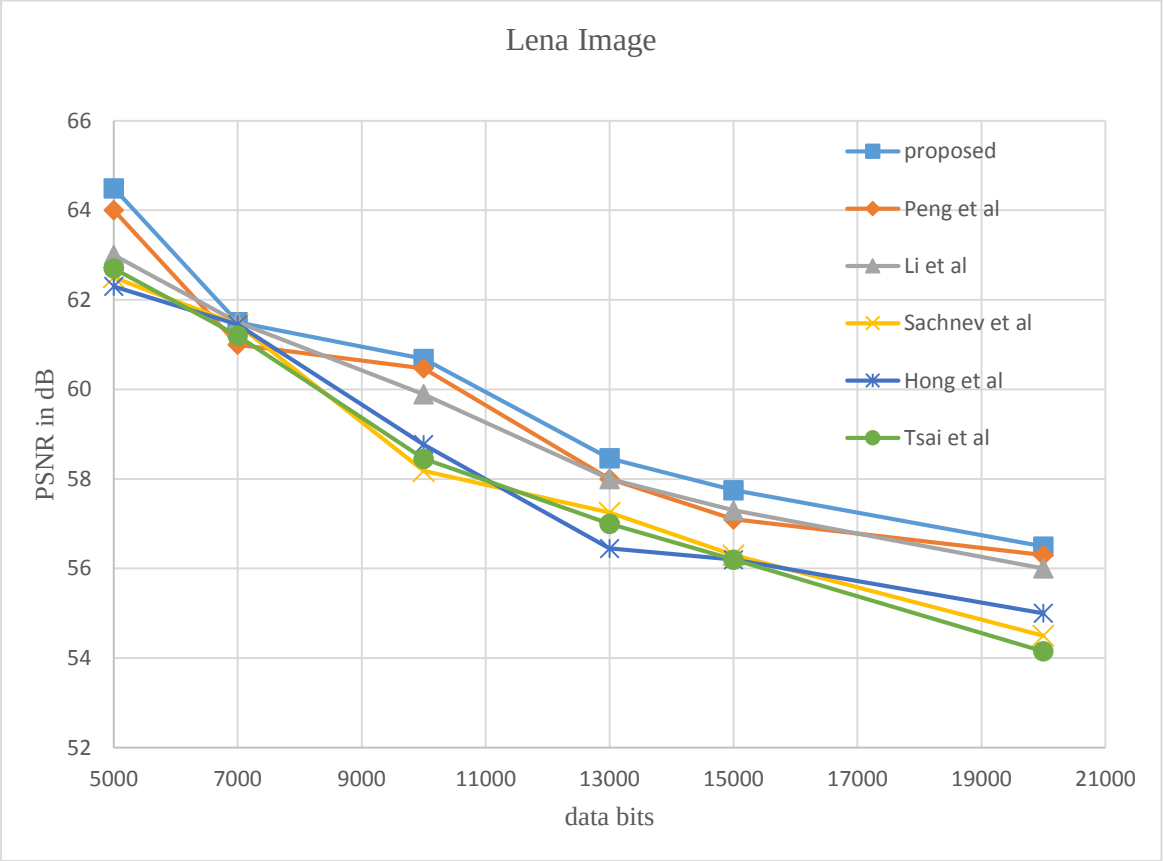

Fig. 5.9. Performance Comparison of PSNR of Lena Image

Table-11: Performance Comparison of F-16 Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al.* (2014)	Li *et al.*'s (2013)	Sachnev *et al* (2009)	Hong *et al* (2012)	Tsai *et al* (2013)
5000	65.41	66	65.10	64.10	65.30	61.0
7000	64.06	65.10	64	63.15	64.45	60.50
10000	62.75	62.96	61.10	60.30	62.10	58.50
13000	60.05	59.75	60	59.45	61	57.75
15000	59.30	59.60	59.2	58.50	59.0	56.50
20000	57.75	57	56.30	56.20	57	56

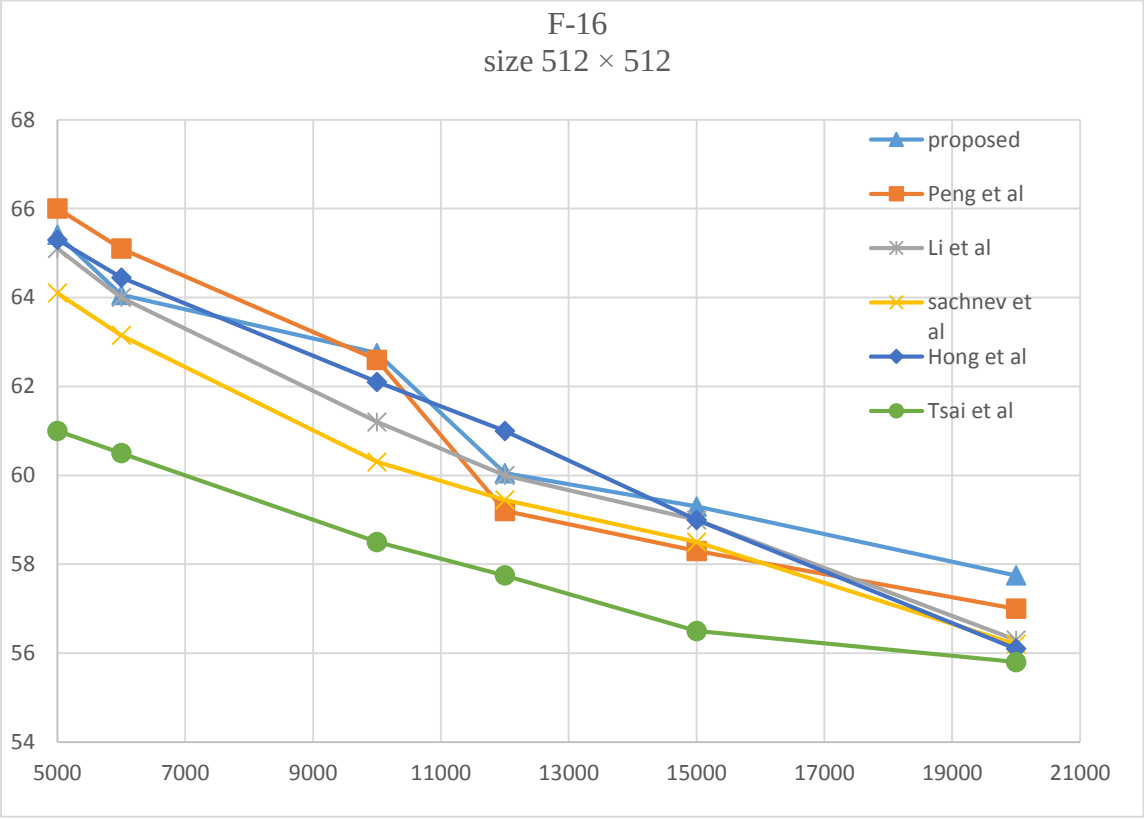

Fig. 5.10. Performance Comparison of PSNR of F-16 Image

Table-12: Performance comparison of Baboon Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al.* (2014)	Li *et al.*'s (2013)	Sachnev *et al* (2009)	Hong *et al* (2012)	Tsai *et al.* (2013)
5000	59.19	59	58	57.50	56.50	54
6000	57.55	57.50	57.15	55.90	55.80	53.50
7000	56.73	57	56.50	56	55	53.10
8000	56.40	56.10	55.50	55.30	54.10	52.90
9000	56.20	56.0	54.50	54.75	53.50	52.40
10000	55.73	54.40	53.55	54.15	52.90	51.97
13000	55.10	53.55	51.50	53.50	51	51.10

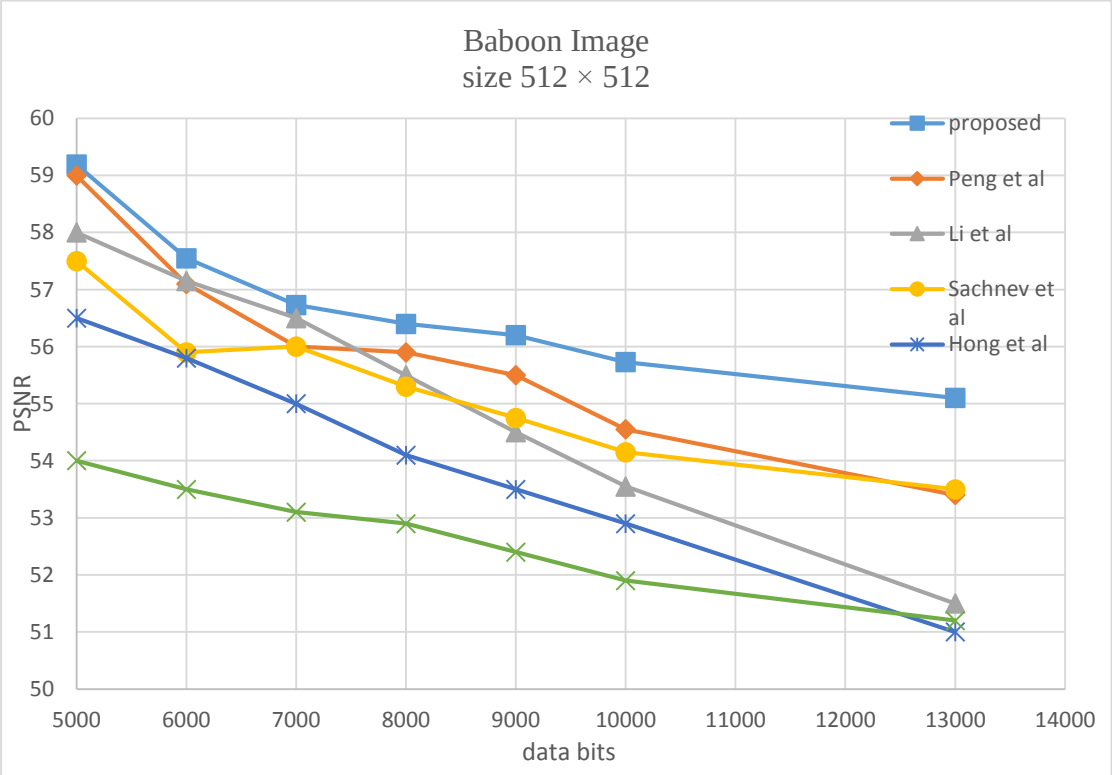

Fig. 5.11. Performance Comparison PSNR of Baboon Image

Table-13: Performance comparison of Fishing Boat Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al.*'s (2014)	Li *et al.*'s (2013)	Sachnev *et al.*'s (2009)	Hong *et al.*'s (2012)	Tsai *et al.*'s (2013)
5000	62.14	62.0	61.50	59.50	60.30	58.10
7000	60.0	60.30	59.80	57.40	58.20	56.0
10000	58.89	58.20	58.0	56.10	56.30	55.0
13000	57.08	56.50	56.0	54.80	55.0	53.80
15000	56.18	55.80	55.50	54.0	54.20	53.0
20000	55.66	54.0	53.20	53.0	52.50	52.0

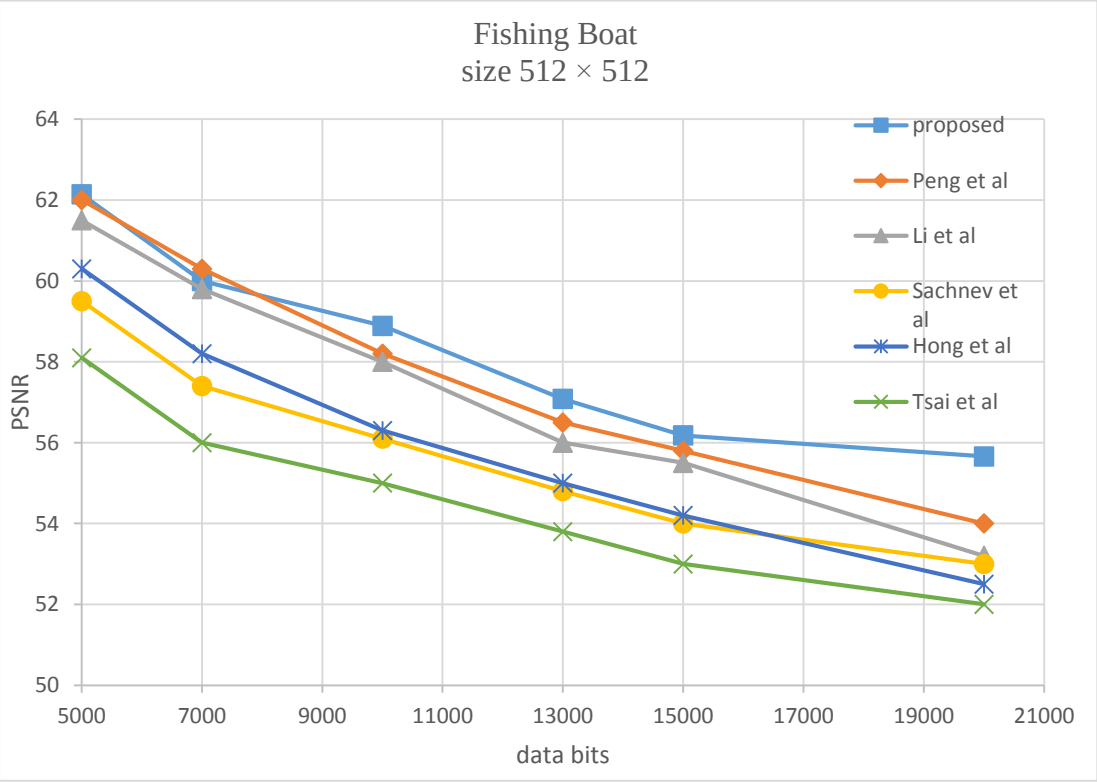

Fig. 5.12. Performance Comparison of PSNR of Fishing Boat Image

Table-14: Performance Comparison of Sailboat Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al.*'s (2014)	Li *et al.*'s (2013)	Sachnev *et al.*'s (2009)	Hong *et al.*'s (2012)	Tsai *et al.*'s (2013)
5000	63.63	63.90	63	60.10	62.90	58.0
7000	60.30	61.40	60.20	58.20	60.10	56.50
10000	58.62	58.87	58.10	56.30	57.30	56.0
13000	56.86	56.20	56.0	55.0	55.90	54.50
15000	56.18	56.0	55.90	54.0	54.20	54
20000	54.66	54.10	54.0	53.0	52	53.10

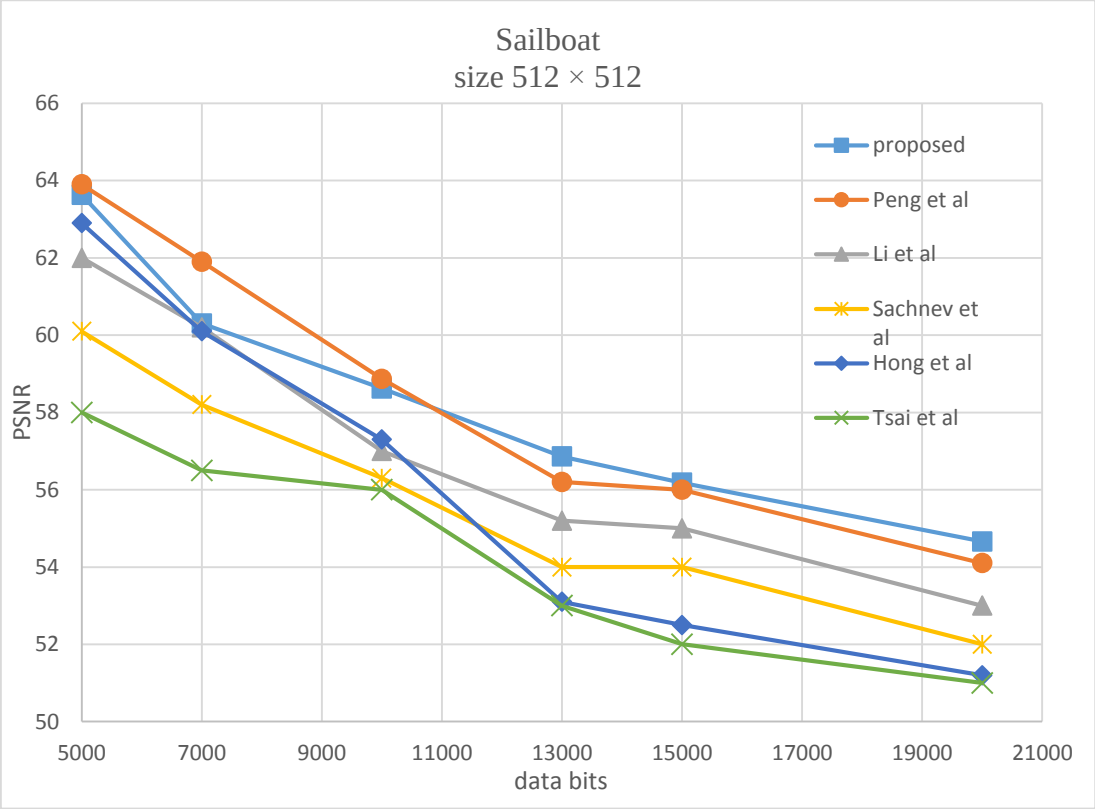

Fig. 5.13. Performance Comparison of PSNR of Sailboat Image

Table-15: Performance Comparison of Peppers Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al.*'s (2014)	Li *et al.*'s (2013)	Sachnev *et al.*'s (2009)	Hong *et al.*'s (2012)	Tsai *et al.*'s (2013)
5000	62.64	63	61.90	58.30	59.20	58.10
7000	61.15	61.10	60.80	57	58	56.80
10000	59	58.98	58.55	55.55	56.04	55.34
13000	57.71	57.10	57	54.10	54.50	54.10
15000	56.65	56.20	56.10	53.90	54	53.90
20000	55.35	55.10	55	52	51.90	52

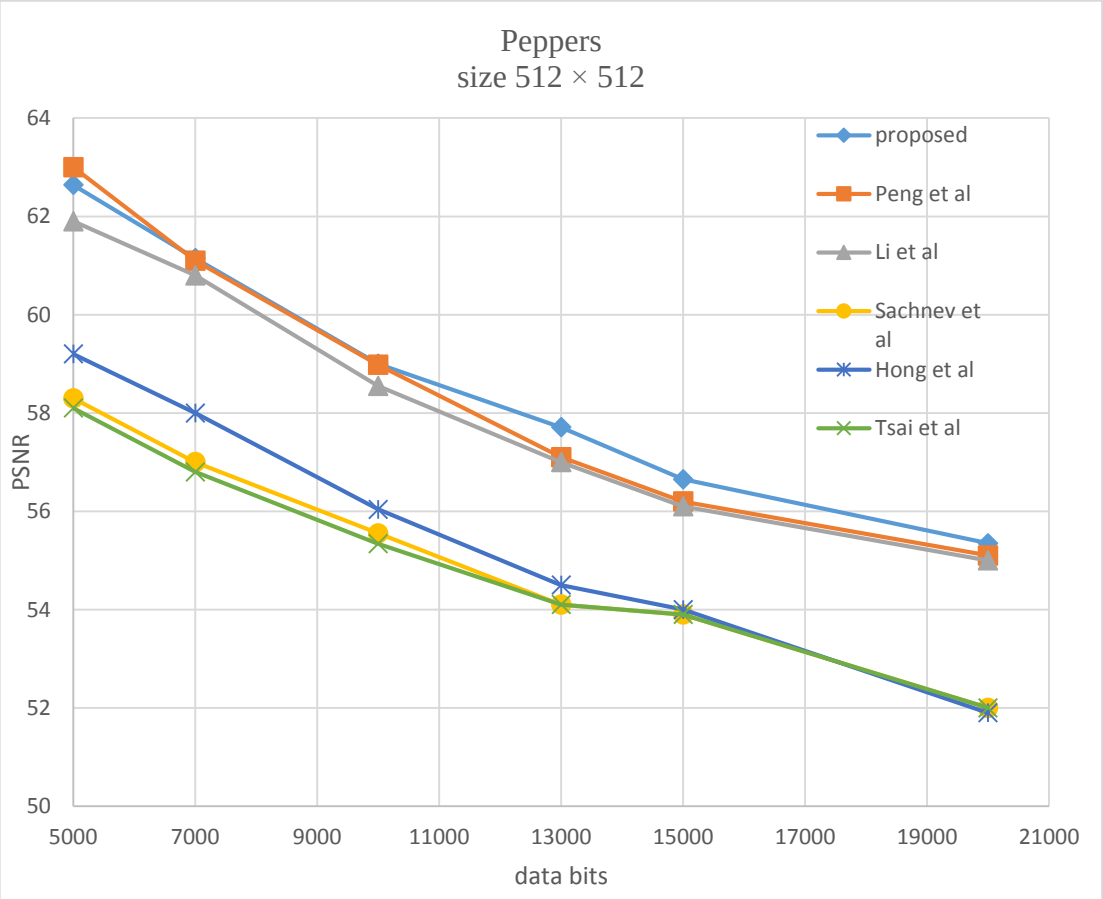

Fig. 5.14. Performance comparison of PSNR of Peppers Image

Table-16: Performance Comparison of Barbara Image of Size 512 × 512

Data capacity	Proposed method	Peng *et al.*'s (2014)	Li *et al.*'s (2013)	Sachnev *et al.*'s (2009)	Hong *et al.*'s (2012)	Tsai *et al.*'s (2013)
5000	63.53	64.0	63.0	61.0	61.20	59.0
7000	62.71	62.5	61.8	59.8	59	57.10
10000	60.72	60.54	59.98	58.15	58.34	56.16
13000	57.76	57.90	57.50	57.0	56.8	55.0
15000	57.06	57.0	56.90	56.1	55.50	54.50
20000	56.24	56.1	55.0	54.50	54.0	53

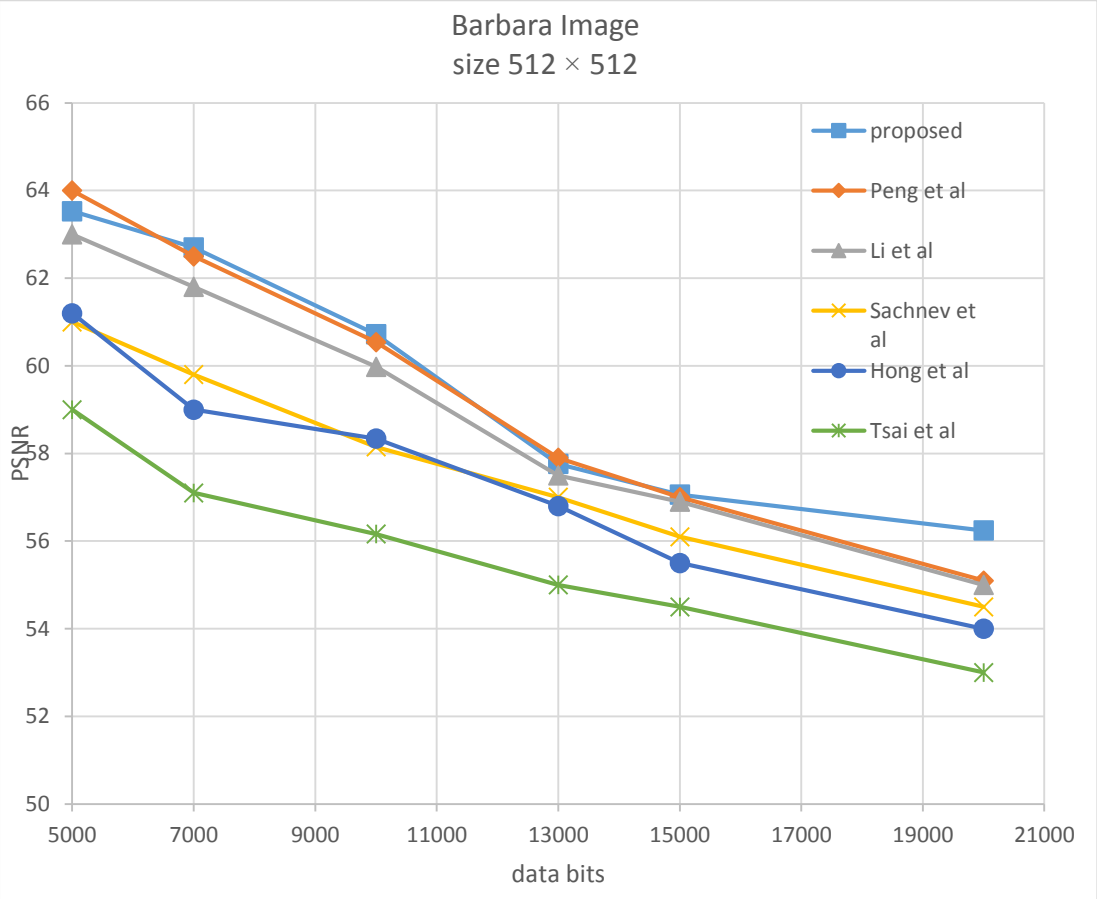

Fig. 5.15. Performance Comparison of PSNR of Barbara Image

CHAPTER-6: CONCLUSION and FUTURE SCOPE

Provided a new pixel-value-ordering based efficient Reversible data hiding scheme. Proposed work is derived from Peng *et al.*'s (2014), a new technique is used to embed secret data into the cover image. By the results, the proposed work gain superior embedding capacity with low distortion than other existing technique. For low embedding capacity this work performance is likely to equal to Peng *et al.*'s (2014), and for large embedding capacity this work gives better result than Peng *et al.*'s (2014) and other reversible data hiding technique. In this proposed scheme image redundancy better exploited and more embedding capacity can be achieved.

Recently, more attention has been paid to reversible data hiding (RDH) in encrypted pictures, as it retains the outstanding property of retrieving the initial cover without loss after extracting integrated information while preserving confidentiality of the image content. In this work, we develop an efficient method reserving space before encryption with an Existing RDH algorithm, and therefore it is easy for data to reversibly incorporate data into the encrypted image. The Proposed technique can attain true reversibility, i.e. there is no error in extracting data and recovering images.

REFERENCE

[1] Celik M, Sharma G, Tekalp A, and Saber E, "Lossless generalized-LSB data embedding," *IEEE Transactions on Image Processing*, vol. 14, no. 2, pp. 253–266, 2005.

[2] Fridrich J, Goljan M, and Du R, Invertible authentication "*Proc*. *Security and Watermarking of Multimedia Contents III"*, (2001), pp. 197-208.

[3] Hong W, "Adaptive reversible data hiding method based on error energy control and histogram shifting," *Optics Communications*, vol. 285, no. 2, pp. 101–108, 2012.

[4] He W, Cai J, Xiong G, and Zhou K, "Improved reversible data hiding using pixel-based pixel value grouping," *Optik*, vol. 157, pp. 68–78, 2018.

[5] He W, Cai J, Zhou K, and Xiong G, "Efficient PVO-based reversible data hiding using multistage blocking and prediction accuracy matrix," *Journal of Visual Communication and Image Representation*, vol. 46, pp. 58–69, 2017.

[6] He W, Xiong G, Weng S, Cai Z, and Wang Y, "Reversible data hiding using multi-pass pixel-value-ordering and pairwise prediction-error expansion," *Information Sciences*, vol. 467, pp. 784–799, 2018.

[7] He W, Zhou K, Cai J, Wang L, and Xiong G, "Reversible data hiding using multi-pass pixel value ordering and prediction-error expansion," *Journal of Visual Communication and Image Representation*, vol. 49, pp. 351–360, 2017.

[8] He W, Xiong G, Zhou K, and Cai J, "Reversible data hiding based on multilevel histogram modification and pixel value grouping," *Journal of Visual Communication and Image Representation*, vol. 40, pp. 459–469, 2016.

[9] Jain N. K and Kasana. S. S, "High-Capacity Reversible Data Hiding Using Modified Pixel Value Ordering Approach," *Journal of Circuits, Systems and Computers*, vol. 27, no. 11, p. 1850175, 2018.

[10] Kamstra L and Heijmans H, "Reversible data embedding into images using wavelet techniques and sorting," *IEEE Transactions on Image Processing*, vol. 14, no. 12, pp. 2082–2090, 2005.

[11] Li X, Li J, Li B, and Yang B, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Processing*, vol. 93, no. 1, pp. 198–205, 2013.

[12] Lee C.-F, Chang C.-C., Li J.-J, and Wu Y.-H., "A Survey of Reversible Data Hiding Schemes Based on Pixel Value Ordering," *2016 Nicograph International (NicoInt)*, 2016.

[13] Li X, Li J, Li B., and Yang B, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Processing*, vol. 93, no. 1, pp. 198–205, 2013.

[14] Li X, Li J, Li B, and Yang B, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Processing*, vol. 93, no. 1, pp. 198–205, 2013.

[15] Ni Z, Shi Y.-Q, Ansari N, and Su W, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–362, 2006.

[16] Ni Z, Shi Y, Ansari N, and Su W, "Reversible data hiding," *Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS 03.*

[17] Ou B, Li X, and Wang J, "High-fidelity reversible data hiding based on pixel-value-ordering and pairwise prediction-error expansion," *Journal of Visual Communication and Image Representation*, vol. 39, pp. 12–23, 2016.

[18] Ou B, Li X, and Wang J, "Improved PVO-based reversible data hiding: A new implementation based on multiple histograms modification," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 328–339, 2016.

[19] Ou B, Li X, and Zhang W, "PVO-based reversible data hiding for encrypted images," *2015 IEEE China Summit and International Conference on Signal and Information Processing (ChinaSIP)*, 2015.

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

[21] Peng F, Li X, and Yang B, "An adaptive PEE-based reversible data hiding scheme exploiting referential prediction-errors," *2015 IEEE International Conference on Multimedia and Expo (ICME)*, 2015.

[22] Jain N. K and Kasana S. S, "High-Capacity Reversible Data Hiding Using Modified Pixel Value Ordering Approach," *Journal of Circuits, Systems and Computers*, vol. 27, no. 11, p. 1850175, 2018.

[23] Rad R. M, Wong K, and Guo J.-M., "Reversible data hiding by adaptive group modification on histogram of prediction errors," *Signal Processing*, vol. 125, pp. 315–328, 2016.

[24] Rahmani P and Dastghaibyfard G, "A reversible data hiding scheme based on prediction-error expansion using pixel-based pixel value ordering predictor," *2017 Artificial Intelligence and Signal Processing Conference (AISP)*, 2017.

[25] 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*, vol. 19, no. 7, pp. 989–999, 2009.

[26] Su W, Wang X, Li F, Shen Y, and Pei Q, "Reversible data hiding using the dynamic block-partition strategy and pixel-value-ordering," *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 7927–7945, 2018.

[27] Su W, Wang X, and Shen Y, "Reversible Data Hiding Based on Pixel-Value-Ordering and Pixel Block Merging Strategy," *Computers, Materials & Continua*, vol. 58, no. 2, pp. 925–941, 2019.

[28] Shastri S and Thanikaiselvan V, "PVO based Reversible Data Hiding with Improved Embedding Capacity and Security," *Indian Journal of Science and Technology*, vol. 9, no. 5, 2016.

[29] Tsai Y. -Y, Tsai D. -S, and Liu C. -L, "Reversible data hiding scheme based on neighbouring pixel differences," *Digital Signal Processing*, vol. 23, no. 3, pp. 919–927, 2013.

[30] Tian J, “Reversible data embedding using a difference expansion,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003.

[31] Wang X, Ding J, and Pei Q, “A novel reversible image data hiding scheme based on pixel value ordering and dynamic pixel block partition,” *Information Sciences*, vol. 310, pp. 16–35, 2015.