High Capacity Data Hiding Techniques for Digital Images

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

Master of Technology
in
Computer Science and Applications

Submitted By
Pankaj Garg
(Roll No. 601203014)

Under the supervision of
Dr. Singara Singh Kasana
Assistant Professor

SCHOOL OF MATHEMATICS AND COMPUTER APPLICATIONS
THAPAR UNIVERSITY
PATIALA –147004
JUNE 2014

CERTIFICATE

I hereby certify that the matter presented in this dissertation titled as **"High Capacity Data Hiding Techniques for Digital Images"** in the partial fulfillment of the requirements for the award of degree of M. Tech. (Computer Science and Applications) submitted in School of Mathematics and Computer Applications (SMCA), Thapar University, Patiala is my authentic work carried out under the supervision of **Dr. Singara Singh Kasana** and refers other researcher's work duly listed in the reference section.

The matter presented in this dissertation has not been submitted for award of any other degree of this or any other university.

Goulcat

(Pankaj Garg)
Roll No. - 601203014

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

Sasana 18.6.2014

(Dr. Singara Singh Kasana)
Assistant Professor, SMCA

Countersigned by:

(Dr. Rajesh Kumar)
Head,SMCA
Thapar University, Patiala

(Dr. S. K. Mohpatra)
Dean (Academic Affairs)
Thapar University, Patiala

ACKNOWLEDGEMENT

First of all, I would like to thank the Almighty, who has always guided me to work on the right path of the life.

I wish to express my sincere thanks and deep sense of gratitude to my guide **Dr. Singara Singh Kasana**, Assistant Professor, SMCA, Thapar University, Patiala, Punjab, for his constant inspiration, scholarly guidance and helpful suggestion throughout the course of my dissertation work.

I am equally grateful to **Dr. Rajesh Kumar**, Associate Professor and Head, SMCA for motivation and inspiration that triggered me for the dissertation work.

I also express my gratitude to **Dr. S. K. Mohapatra,** Senior Professor and Dean of Academic Affairs, Thapar University for making provisions of infrastructure such as library facilities, computer labs equipped with net facilities, immensely useful for the learners to equip themselves with the latest in the field.

I am also thankful to the entire faculty and staff members of SMCA for their help, cooperation, love and affection, which made my stay at Thapar University memorable.

Last but not least, I would like to thank my parents for their wonderful love and encouragement, without their blessings none of this would have been possible. I would also like to thank my friends for their constant support.

Pankaj Garg
601203014
M. Tech (CSA)

ABSTRACT

Today, the demand of internet has made the transmission of digital media much easier and faster. Open nature of internet, risks of illegitimate accessing and unauthorized tempering with transmitted data is increased day by day. Protection of secret information from unauthorized users in a public network has become an important issue. Data hiding is one of the most demanding techniques to protect the security of digital media. In this dissertation, we have proposed three data hiding techniques.

We have proposed a histogram based reversible data hiding technique for digital images. In this technique, cover image is divided into blocks of equal size. Then modulus operator is used to increase the occurrence of peak points in the histogram of blocks. Extracted secret image is similar to original secret image. Maximum capacity is more than 96,000 bits and Peak Signal Noise Ratio (PSNR) is also higher than 50 dB. Embedding capacity and PSNR are higher than existing histogram based data hiding techniques.

Histogram based reversible data hiding technique is modified to embed more secret data using the concept of multilevel embedding. Modulus operator is also used to increase the occurrence of peak points of histogram of blocks. Secret information is embedded into peak points of histogram but in the modified technique minimum point is not necessary to a zero point. Extracted secret image and cover image are similar to original secret image and original cover image respectively. Maximum capacity is more than 2.6 bit per pixel (bpp) and PSNR is also higher than 44 dB. Proposed technique provides better embedding capacity and better visual quality of marked image than existing multilevel data hiding techniques.

Interpolation based blind data hiding technique is also proposed in this dissertation. In this technique, difference images are generated using interpolation of sub sampled images and on the basis of even or odd state of the difference pixel value; the secret information is embedded into the cover image. Maximum capacity is more than 196,000 bits and PSNR is also higher than 50 dB. Proposed technique provides higher embedding capacity, better visual quality marked images and less computational complexity than interpolation based data hiding techniques.

LIST OF PUBLICATIONS

Paper Communicated

[1] Garg P. and Kasana S. S., "Block based reversible data hiding using histogram and modulus operator of digital images", Security and Communications Networks.

[2] Garg P. and Kasana S. S., "Modulus based multilevel reversible data hiding using histogram shifting", KSII Transactions on Internet and Information Systems.

[3] Garg P. and Kasana S. S., "Bind data hiding technique using interpolation of subsampled images", IET Electronics Letters.

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

BPP	Bit Per Pixel
DE	Difference Expansion
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
G-LSB	Generalized-Least Significant Bit
LSB	Least Significant Bit
MSB	Most Significant Bit
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio
PVD	Pixel Value Difference
SIM	Similarity Index Modulation

TABLE OF CONTENTS

CHAPTER 1
INTRODUCTION

1.1 Introduction

Now a day's digital media is being immensely used in various type of applications such as medical, military, law enforcement, fine art work protection and so on. Security is the main concern which is to be taken care of while transferring confidential data on the Internet. Since text, images, audio, video are the part of digital data that are transferred over open public network so there is need to protect this digital data. From the last few decades, various methods have been developed to enforce security in various types of applications. Generally, two methods are used to secure the data *i.e.* cryptography and data hiding (Sencar *et al.*, 2004).

Cryptography is the art of secret writing. This is achieved by scrambling the secret information and the scrambled information is unscrambled only by some key or some program. Cryptography emphasis on data integrity, data confidentiality, authentication, non repudiation of data *etc*. Data hiding is the art of hiding secret information in cover media without any perceptual distortion of the cover media (Bender *et al.*, 1996).

Data hiding is form of subliminal communication which uses a variety of multimedia as a cover media and embeds the secret information into this media to generate marked media (Artz, 2001; Cox *et al*., 2007). Data hiding technique s used for copyright protection, temper detection, covert communication, data integrity *etc*. It is generally accepted that a data hiding technique must possess following two important properties:

- Imperceptibility:
- Embedding capacity:

First property guarantees that embedded data is undetectable and second means efficiency in hidden communication. These properties are discussed in details in further subsections.

1.2 Principle of data hiding

Embedding process and extracting process are the two main processes of data hiding. In embedding process, secret data is embedded into cover media. Cover media is modified after embedding the secret data. This modified cover media which contain secret data is known as marked data. Secret data is extracted from the marked data and recovers the original cover media.

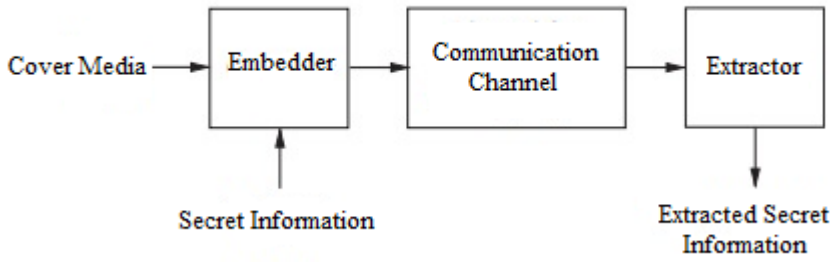


Fig 1.1 Traditional Data Hiding System

A traditional data hiding system, shown in Fig. 1.1, includes embedder and extractor. The input to the embedder is multimedia data and secret data, which is to be embedded into original multimedia data. The output of embedder is marked data. There are different types of file/data formats which are used for data hiding, as shown in Fig. 1.2. In this dissertation, image file format is used to embed the secret data.

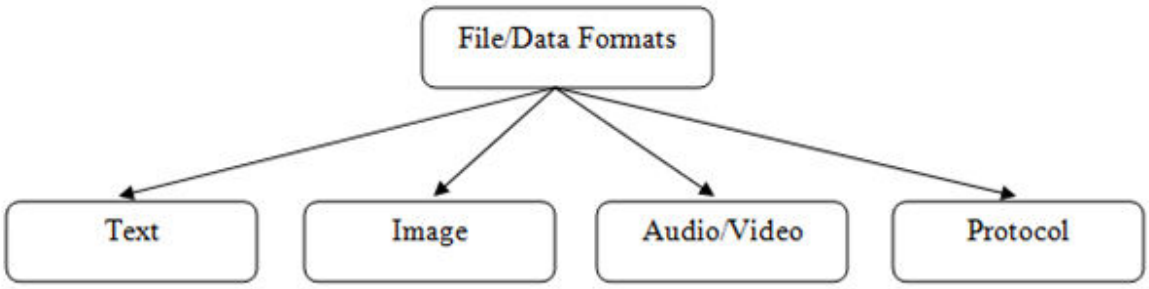


Fig. 1.2 Different Type of Files used for Data Hiding

1.3 Need of Data Hiding

- Covert communication using images (secret information is hidden in a cover media)
- Ownership of digital images, authentication, copyright
- Data integrity, fraud detection, self-correcting images
- 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, automatic copyright information, viewing a movie in a given rated version
- Copy control (secondary protection for DVD)
- Device control

1.4 Type of data hiding

In literature, there are different kinds of data hiding techniques, which can be classified into four categories and further classified.

1.4.1 Recovery of cover media based data hiding techniques

Based on recovery of media, data hiding techniques could be divided into two categories.

1.4.1.1 Reversible data hiding technique

In this technique, secret information is embedded in cover media and at the time of extraction, secret information is extracted along with cover media exactly same as before embedding. Reversible techniques are used to recover the cover media from marked media by extracting secret media. Cover media is as important as secret media in many areas such as medical, military etc.

1.4.1.2 Irreversible data hiding technique

In this technique, secret information is embedded in cover media and at the time of extraction, only secret information is extracted but cover media is lost i.e. from marked media cover media cannot be recovered in extraction process.

1.4.2 Extraction based data hiding techniques

According to extra information required at the time of extraction, data hiding techniques could be divided into three categories

1.4.2.1 Blind data hiding technique

It is a data hiding technique which does not require the cover media during the extraction to get the secret media.

1.4.2.2 Semi blind data hiding technique

It is a data hiding technique which does not require the cover media but extra information is required to get the secret media.

1.4.2.3 Non blind data hiding technique

It is a technique in which the cover media is required in the extraction to get the secret media.

1.4.3 Domain based data hiding techniques

According to domain of data embedding, data hiding techniques could be divided into three categories.

1.4.3.1 Spatial domain data hiding technique

In this data hiding technique, secret media is directly embedded in cover media i.e. secret information is stored directly in the pixels of cover image. This technique is easy to implement. Least Significant Bit (LSB) is an example of spatial domain data hiding technique in which secret information is stored in the LSB of cover image.

1.4.3.2 Transform domain data hiding technique

In this data hiding technique, secret media is not directly embedded in the cover media rather it is embedded into transform domain which is obtained by applying some transformation such as Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) *etc.* to the cover media.

1.4.3.3 Compressed domain data hiding technique

In this data hiding technique secret information is embedded into coefficient of compressed code of a cover media.

1.4.4 Application based data hiding techniques

According to recovery of application, data hiding techniques could be divided into two categories.

1.4.4.1 Steganography

Steganography is derived from Greek words steganos which means covered and graphein means writing. Steganography is the art of covert communication and art of communicating in such a way presence of secret information cannot be detected. Steganographic technique must have high embedding and high imperceptibility so that no one can detect the presence of secret information in the cover image.

1.4.4.2 Watermarking

Watermarking is the process of hiding secret information in cover image. Watermarking is used for data integrity and authenticity of the cover image. It is not necessary that watermark is imperceptible but watermark is more robust against modification in cover image.

1.5 Properties of data hiding techniques

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

1.5.1 Imperceptibility

Imperceptibility is the fundamental requirement of data hiding in which marked data or image looks similar as the original data or image. The secret information should be invisible to human

eye. To compute imperceptibility, PSNR is generally used. This concept is based on the properties of the human visual system. The embedded secret information should not introduce any perceptible distortion, that is, if an average human subject is unable to differentiate between cover media that contain hidden data and those that do not. Human perceptual modeling is the solution that can be used to solve this problem in embedding process. A concept of imperceptibility would result if the visibility of distortion would be tested by presenting both covers with or without embedding information.

1.5.2 Robustness

Robustness determines the algorithm behavior towards data distortions introduced through standard and malicious data processing. If the presence of embedded information can be detected reliably even after tempering an image but not have any distortion beyond reorganization then this embedded information said to be robust. Linear and nonlinear filters (blurring, sharpening, median filtering), lossy compression, contrast adjustment, gamma correction, recoloring, resampling, scaling, rotation, small nonlinear deformations, noise adding, cropping, pixel permutation in small neighborhood, are some of the examples of tempering. Robustness does not include attacks on the embedding scheme that are based on the knowledge of the embedding algorithm or on the availability of the detector function. A good data hiding technique should be robust against filter processing, noise addition, lossy compression and geometrical transformations such as translation, rotation, scaling.

1.5.3 Security

Based on a knowledge of the embedding algorithm and detector (except the secret key) and the knowledge of at least one carrier with secret information if embedded information cannot be removed beyond reliable detection by targeted attacks then, the embedding algorithm is said to be secure. Attacks attempt to remove, modify or embedded unnecessary information into marked image. Attacks are of two types namely, active attack and passive attack. Active attack attempts to modify the secret information while passive attack detects only the secret information.

1.5.4 Complexity

The time and effort needed to embed and retrieve the secret information is known as complexity of the data hiding system. As the complexity of technique increases more hardware and software resources are required to implement it, which results in increase of the computation cost. In order to reduce the computational cost of data hiding system, it should be less complex. Such as in telemedicine domain, during the transmission of medical data, less complex data hiding techniques are implemented to cut the cost of bandwidth consumption data capacity.

1.5.5 Capacity

Capacity of the data hiding system describes embedding of maximum amount of secret information. By comprising either the robustness or imperceptibility of technique higher capacity of embedded information in data can be obtained. Trade off between embedding capacity, imperceptibility and robustness in data hiding is as shown in fig. 1.3.

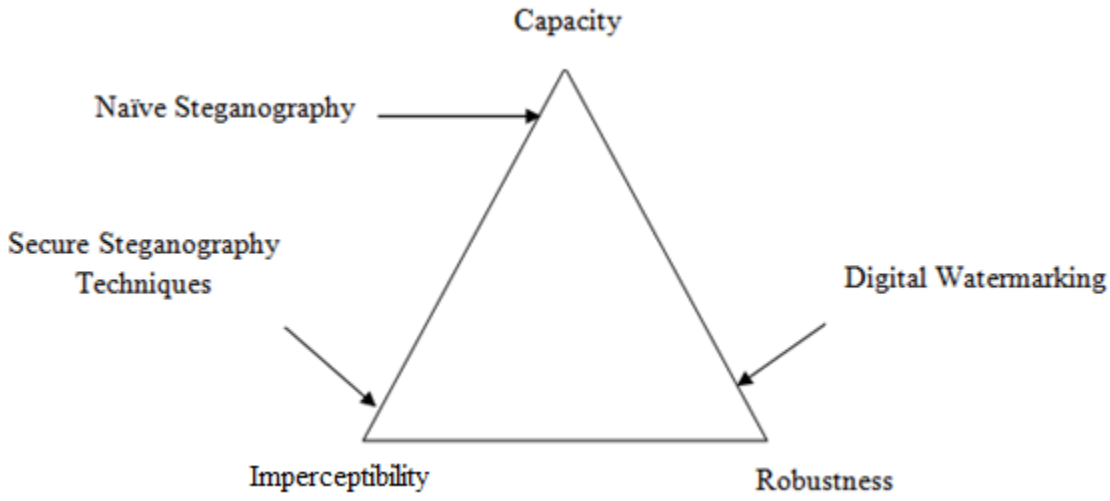


Fig. 1.3 Trade off between Embedding Capacity, Imperceptibility and Robustness in Data Hiding

1.6 Quality parameters

The visual quality of marked image is the most important property of data hiding because it is hard to detect by detectors. In this work, PSNR is taken as the quality parameter which is

calculated using the cover image and marked image. It gives the statistical difference between the cover image and marked image and is calculated using following equation:

$$PSNR = 10log_{10}\frac{255}{MSE}$$

where *MSE* is the mean square error and is defined as

$$MSE = \sum_{m=1}^{h}\sum_{n=1}^{w}\frac{(X(m,n) - Y(m,n))^2}{h \times w}$$

where $Y(m,n)$ is the pixel of marked image and $X(m,n)$ is the pixel of cover image, h and w is the height and width of image respectively(Anderson, 1998).

Similarity Index Modulation (*SIM*) is defined as

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

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

1.7 Contribution of the dissertation

Data hiding is the process of hiding the secret information in the cover media. Most of the techniques developed for the data hiding take into consideration of only one parameter from PSNR or embedding capacity. But in this dissertation, the main focus lies on the hiding of data in cover media with high embedding capacity with high PSNR. For this particular to put into practice we make the use of histogram shifting which is proposed by Ni *et al.* (2006), and the modulus operator to enhance the embedding capacity. In this dissertation reversible and blind data hiding algorithms proposed. Reversible data hiding is basically used by area such as medical, military etc. and blind data hiding is used in covert communication. The main focus is to increase the embedding capacity keeping high PSNR between marked image and cover image. The contributions of the dissertation, in summary are:

- First, a data hiding technique is proposed in which histogram shifting is used along with modulus operator. The modulus operator is used to increase the number of peak points in the histogram of block of an image. The input cover image is firstly decomposed into blocks followed by histogram shifting. Peak point is used to embed the secret information. Thus, we propose a method for data hiding which is high capacity in terms of embedding and high PSNR value.
- Further multi level data hiding technique based on the histogram shifting is proposed in which modulus operator is also used. This multi level data hiding technique produces even better results as compared to the previous discussed technique. In this technique multi level concept is used to embed the secret information.
- Another blind data hiding technique is proposed in this dissertation in which interpolation method is used with even-odd strategy. In this technique sub sampled image is used to embed the secret information. Computation complexity is very much low as compared to previous technique.

1.8 Organization of the thesis

Several techniques for data hiding using the histogram shifting along with modulus operator and interpolation method along with even-odd strategy are proposed in this dissertation. The dissertation is organized as follows.

In Chapter 2, current literature on data hiding is specified which generally includes techniques used in reversible data hiding using histogram and techniques which used interpolation method to embed the secret information.

Reversible block based data hiding technique is discussed in Chapter 3. In this chapter, modulus operator is used to increase the peak points of histogram after decomposing image into sub blocks.

In Chapter 4, multilevel data hiding based on the histogram shifting and modulus operator is discussed which leads high embedding capacity and therefore leads to better PSNR followed by the blind data hiding technique as discussed in Chapter 5 in which the secret information is embed in subsampled images using the interpolation method and even-odd strategy.

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 technique.

CHAPTER 2
LITERATURE REVIEW

2.1 Introduction

In this chapter, we shall review the literature related to data hiding techniques. We have surveyed these techniques and that lead us to the formulation of the problems we have solved in this dissertation. The comparative results given in the subsections of this chapter are the results published in the research articles reviewed in this work. Section 2.2 contains the literature review related to the basic reversible data hiding techniques. Histogram based data hiding techniques are analyzed in section prior to literature review of Pixel Value Difference (PVD) techniques in section 2.4. Section 2.5 contains the literature review related to the Histogram and PVD based techniques are reviewed in section 2.5. Literature review related to the interpolation based data hiding techniques are reviewed in Section 2.6.

2.2 Reversible data hiding techniques

Honsinger *et al.* (2001) firstly proposed reversible data hiding technique for reversible authentication. This technique utilized a robust spatial additive data hiding technique combined with modulo additions to achieve reversible data embedding but it suffered from salt and pepper visual artifact.

Fridrich *et al.* (2001) proposed two data hiding techniques for authenticating digital images. One technique is based on robust spatial additive with modulo addition and another one is based on lossless compression and bit plane encryption. In second technique, cover image losslessly compressed using the LSB plane of selected pixels. Compressed data is combined with the secret

information to form bitstream. Bitstream was embedded into the cover media by using LSB substitution. The algorithm is completely reversible but embedding capacity is very low.

Fridrich *et al.* (2002) proposed another reversible data hiding technique. In this technique pixel of cover image divided into three group: Regular group (R), Singular group (S) and Unusable group (U). R and S groups were used for data embedding using flip function. 1 and 0 were embedded into R and S groups respectively.

Celiket *et al.* (2002) proposed a technique for reversible data hiding using LSB modification. The original image is losslessly recovered using signal's compressing portion that is prone to embedding distortion and these compressed descriptions contain secret information. An entropy coder which is based on prediction is used to improve efficiency of compression. This LSB technique is more efficient than traditional LSB embedding technique.

Celik *et al.* (2005) proposed an improved technique by using Generalized-Least Significant Bit (G-LSB) embedding which losslessly recovered the cover image after extracting secret information. In this technique, secret information is firstly converted from binary to L-ary, and then lossless compression is used to compress the quantization residues as side information. In This technique the embedding parameters are adjusted for satisfying capacity requirements. The presented G-LSB technique is efficient over traditional LSB technique.

2.3 Histogram based data hiding techniques

Ni *et al.* (2006) firstly utilize histogram for reversible data hiding. Image histogram is generated by calculating occurrence of all pixel value. Firstly peak and zero point are searched in image histogram. Peak and zero points are the pixel value with the maximum and zero or minimum occurrence in the histogram. Pixel with their value between peak and minimum pint are shifted in right or left to generate embedding space then secret information is embedded at the pixel that having value equal to value of peak point. PSNR of marked image generated with this technique is always greater or equal to 48 dB.

Hwang *et al.* (2006) proposed a histogram based reversible data hiding technique. This technique used the concept of adjusting the pixel values that are located on both sides of a peak point of histogram to embed the secret information. This technique overcomes the problem of storing

peak and minimum points that are needed at the time of extraction of secret information. Peak point and minimum point are not required to transmit at the receiver side. Location map is used to recursively embed the secret information into the cover media which enhance the embedding capacity.

Lee *et al.* (2006) proposed a reversible data hiding technique which is based on the histogram shifting and uses the characteristic of difference image. In this technique, MD5 algorithm is used to secure the cover media. Secret information is embedded into the modified difference image. Lower bound of PSNR of marked image is 51.14 dB. Execution time of this technique is shorter than previous technique.

Fallahpour *et al.* (2007) proposed a technique which is based on block division and histogram shifting. This technique utilizes the peak and zero point of the blocks of cover image to embed secret information. Firstly it decomposes the whole cover image into blocks of same size then histogram shifting is applied to generate the embedding space. Secret information is embedded in that space. This technique is quite simple.

Kuo *et al.* (2008) proposed histogram based reversible data hiding technique. In Hwang *et al.* (2006) technique, it is not necessary that minimum point in cover image is zero. To overcome this shortcoming block division method in which cover image decomposed into sub blocks is proposed in this technique. This block division method enhances the embedding capacity and recovers the cover image exactly.

Chung *et al.* (2012) proposed a reversible data hiding technique which is based on the histogram modification which reduces distortion took place in Ni et al. (2006) data hiding technique by using block based complement method.

Wang *et al.* (2012) proposed a reversible data hiding technique based on the multilevel histogram embedding. Iterative multi histogram strategy is used to reduce the overhead information during data embedding. This technique is not suffered from underflow and overflow problem and provide PSNR around 48.13 dB for embedding capacity 1 bpp.

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

other pixel value in the same segment instead of peak point of a histogram. To extract secret information exactly, a location map is used. Multilevel data embedding concept is used to enhance the embedding 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.

2.4 PVD based data hiding 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 embedding 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 embedding secret information. This technique provides nearly double embedding 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 embedding 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 embedding capacity.

2.5 Histogram and PVD based data hiding 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 embedding capacity. After 9^{th} level of this technique it provides average PSNR value greater than 30dB and average embedding 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 embedding capacity is enhanced. This technique provides better visual quality and embedding 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. Embedding 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 embedding 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 embedding 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 embedding 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 embedding a rhombus prediction is used. To enhance correlation of neighbor pixels, prediction and sorting is used which enhance the embedding 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 embedding capacity.

2.6 Interpolation based data hiding techniques

Yang *et al.* (2008) proposed a data hiding technique based on the interpolation and LSB substitution. In this technique cover image is divided into non overlapping blocks of size 5×5. A blocks of size 3×3 is obtained by shrinking blocks of size 5×5 and again blocks of size 5×5 is obtained by interpolating of blocks of size 3×3. If the difference between interpolated block pixel value and original pixel value is less than a threshold value or equal to zero then embed the secret information using the pseudo random number generator. Scrambling is used in this technique to provide more security.

Jung *et al.* (2009) proposed a data hiding technique based on the scaling-up neighbor mean interpolation method. This technique used a neighborhood pixel value to compute the mean value. This technique is better than nearest neighbor and bilinear interpolation techniques. This technique provides PSNR value of marked image always higher than 35 dB and high embedding capacity.

Abadi *et al.* (2010) proposed a reversible data hiding technique based on the interpolation and histogram. 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 embedding 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 embedding secret information. Prediction technique is used to reduce the reference pixel in smooth region which enhance the embedding 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 embedding 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 embedding 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 embedding capacity.

CHAPTER 3

REVERSIBLE DATA HIDING USING HISTOGRAM AND MODULUS OPERATOR

3.1 Introduction

In this chapter, a reversible data hiding technique using histogram and modulus operator is proposed in which secret information is embedded in blocks of the cover image. Proposed data hiding technique is based on histogram shifting of the cover image with the help of prediction value which is generated using the modulus operator. In histogram shifting based data hiding technique, the secret information is embedded into peak points occurring in the histogram of cover image and embedding capacity is directly proportional to the number of peak points of image histogram. The proposed technique is based on the observation that if modulus operator using some integer number is applied on the cover image then the occurrence of peak points in the image increases and it increases the embedding capacity of a cover image. This technique consists of three algorithms. First algorithm is used to find out optimize modulus operator number and then generate keys using this number. Second and third algorithms are used for data embedding and data extraction, respectively.

3.2 Selection of optimal modulus operator and key generation algorithm

A cover image C of size $r \times r$ is input to this algorithm. It generates keys K and n as an output which are used in data embedding and data extraction algorithms.

Step 1: Decompose cover image C into cover blocks CB_j of size $t \times t$, where $j = 1,2, \ldots \ldots, \frac{r \times r}{t \times t}$.

Repeat Step 2 and 3 for each cover block.

Step 2: (Estimation of Data Hiding Capacity of a block) To compute the highest hiding capacity of cover image, repeat following steps for each $n \in (2, e)$, where $e = 2^b - 1$ where b is the bit depth of the cover image.

(i) Apply module n on each pixel of each cover block CB_j to generate prediction block PB_j.

(ii) (ii) Generate histogram H_j of block PB_j and find the peak point $p_j \in [0, n-1]$ and zero point $z_j \in [0, n-1]$. If zero point not exists then go to step 2(i).

(iii) $H_j(p_j)$ is the number of occurrence of peak point p_j for block PB_j.

(iv) Sum up $H_j(p_j)$ into G_n to get the total hiding capacity, for particular n.

Step 3: Select n which has highest hiding capacity G_n.

Step 4: (Key Generation) Take modulo with selected n on each pixel of each block

(i) Generate histogram H_j of each block and find the peak point $p_j \in [0, n-1]$ and zero point $z_j \in [0, n-1]$.

(ii) $K(j,1) = p_j$ and $K(j,2) = z_j$ where K is the key which is used in data embedding and data extraction.

3.3 Data embedding algorithm

A grayscale cover image C of size $r \times r$, a binary secret image S and Key K and n are input to this algorithm and generates a marked image M.

Step 1: (Block Decomposition) Decomposition cover image C into blocks of size $t \times t$.

Step 2: (Data Embedding) For each cover block CB_j perform the following operations.

(i) Apply Module n on each pixel of original cover block CB_j to generate prediction block PB_j.

(ii) Shift each pixel of original cover block CB_j to generate the embedding space in right or left according to the key $K(j,1)$ and $K(j,2)$ with the help of prediction block as using following expression.

If $K(j,1) < K(j,2)$

$$MB_j(u,v) = CB_j(u,v) + 1 \quad for\ K(j,1) < PB_j(u,v) < K(j,2)$$

$$MB_j(u,v) = CB_j(u,v) \qquad otherwise$$

If $K(j,1) > K(j,2)$

$$MB_j(u,v) = CB_j(u,v) - 1 \quad for\ K(j,1) > PB_j(u,v) > K(j,2)$$

$$MB_j(u,v) = CB_j(u,v) \qquad otherwise$$

(iii) Scan the pixel of prediction block PB_j and secret image S in raster scan order in order to embed the data in original blocks CB_j to get marked block MB_j using the following expressions.

If $S = 1\ and\ PB_j(u,v) = K(j,1)$

$$MB_j(u,v) = CB_j(u,v) + 1$$

If $S = 0\ and\ PB_j(u,v) = K(j,1)$

$$MB_j(u,v) = CB_j(u,v)$$

Step 3: Combine the each block MB_j to form marked image M which is used to send the secret image.

3.4 Data extraction algorithm

Input: A grayscale marked image M of size $r \times r$ and Key K and n are input to this algorithm. It generates same cover image C' and secret image S' as an output.

Step 1: (Block Decomposition) Decompose marked image M into blocks MB_j' of size $t \times t$.

Step 2: For each block MB_j' perform the following operations.

(i) Apply Module n function on each pixel of block MB_j' to generate prediction block PB_j'.

(ii) Scan the pixel of $PB_j^{'}$ in raster scan method and extract the data using the following expressions.

If $K(j,1) < K(j,2)$

$$S^{'} = 1 \quad if\ PB_j^{'}(u,v) = K(j,1) + 1$$

$$S^{'} = 0 \quad if\ PB_j^{'}(u,v) = K(j,1)$$

If $K(j,1) > K(j,2)$

$$S^{'} = 1 \quad if\ PB_j^{'}(u,v) = K(j,1) - 1$$

$$S^{'} = 0 \quad if\ PB_j^{'}(u,v) = K(j,1)$$

(iii) Reverse shift each pixel of $MB_j^{'}$ in right or left according to the key $K(j,1)$ and $K(j,2)$ to get original cover block as using following expression.

If $K(j,1) < K(j,2)$

$$CB_j^{'}(u,v) = MB_j^{'}(u,v) - 1 \qquad for\ K(j,1) < PB_j^{'}(u,v) < K(j,2)$$

If $K(j,1) < K(j,2)$

$$CB_j^{'}(u,v) = MB_j^{'}(u,v) + 1 \qquad for\ K(j,1) > PB_j^{'}(u,v) > K(j,2)$$

Step 3: Combine each block $CB_j^{'}$ to form cover image $C^{'}$.

Proposed technique is illustrated using an example. Cover block size considered in this example is of 4×4 size and secret data is '011011'. Modulo number is 6 which is applied to this cover block.

155	156	178	179
123	124	125	179
123	125	133	132
123	111	121	233

Fig. 3.1 Cover Block CB

After taking modulo with 6 of each pixel of cover block, prediction block is as given below.

5	0	4	5
3	4	5	5
3	5	1	0
3	3	1	5

Fig. 3.2 Embedding Prediction Block PB

For this block, Peak point is 5 and Zero point is 2 which shows that it increase occurrence of peak point by 2 as compared to original cover block. Key for this block is 5 and 2. Original cover block is modified using peak and zero points of prediction block. As peak point is 5 and zero point is 2, the each pixel of original cover block are decremented by 1 on those positions where prediction block has values between 2 and 5 to generate intermediate marked, as shown in block given below.

155	156	177	179
122	123	125	179
122	125	133	132
122	110	121	233

Fig. 3.3 Intermediate Marked Block

Then data is embedded using proposed technique in original cover block using the position of peak points of the prediction block. After embedding, the marked block is obtained.

155	156	177	178
122	123	124	179
122	124	133	132
122	110	121	232

Fig. 3.4 Final Marked Block MB

At the extraction side marked block is again modified using same modulo number which is 6 in this example. The prediction block obtained is

5	0	3	4
2	3	4	5
2	4	1	0
2	2	1	4

Fig. 3.5 Extracting Prediction Block PB'

As key used on embedding side is 5 and 2. If value of sample in prediction block is 5 then corresponding extracted bit is 0 and no changes are done in the marked block at corresponding position and if value of sample in modified block is 4 then corresponding extracted bit is 1 and value of the corresponding pixel in marked block is incremented by 1 to get the intermediate cover block.

155	156	177	179
122	123	125	179
122	125	133	132
122	110	121	233

Fig. 3.6 Intermediate Cover Block

Now reverse shifting is performed using prediction block and keys (2 and 5). Prediction block having value between [2,5) are incremented by 1 in the corresponding position of marked block to get the original cover block.

155	156	178	179
123	124	125	179
123	125	133	132
123	111	121	233

Fig. 3.7 Final Cover Block CB'

This example shows that proposed technique is reverse.

3.5 Experimental results

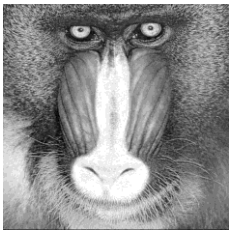
Proposed technique is implemented using MATLAB software tool. The input images considered in this work are uncompressed standard images named as Airplane, Baboon, Barbara, Boat, Bridge, Couple and Lena, which are used by the researchers to compare their results with the existing algorithms. Block size considered in this experiment are 16×16, 8×8 and 4×4. Some of the cover images and their marked images at different block size are shown in Fig. 3.8

(a) Original Airplane Image

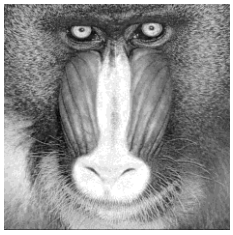
(b) Marked Airplane Image Using 16×16 block Size

(c) Marked Airplane Image Using 8×8 block Size

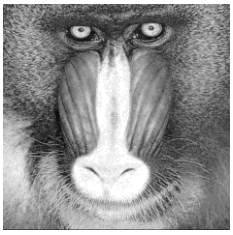
(d) Marked Airplane Image Using 4×4 block Size



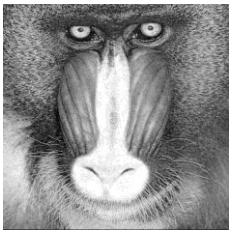
(e) Original Baboon Image



(f) Marked Baboon Image Using 16×16 block Size



(g) Marked Baboon Image Using 8×8 block Size



(h) Marked Baboon Image Using 4×4 block Size

(i) Original Boat Image

(j) Marked Boat Image Using 16×16 block Size

(k) Marked Boat Image Using 8×8 block Size

(l) Marked Boat Image Using 4×4 block Size

(m) Original Lena Image

(n) Marked Lena Image Using 16×16 block Size

(o) Marked Lena Image Using 8×8 block Size

(p) Marked Lena Image Using 4×4 block Size

Fig. 3.8 Different original cover images and their marked images using different block size

SIM of all extracted secret images and cover images is exactly 1, which shows that proposed method is reversible. Hiding capacity, *PSNR* of each image for optimal Modulus operator *n* are shown in Table 3.1.

Table 3.1 Hiding capacity (in bits) and PSNR (in dB) of proposed method for different images and different block size

Block Size →	**16×16**			**8×8**			**4×4**		
↓ **Image**	Optimal *N*	Capacity	*PSNR*	Optimal *N*	Capacity	*PSNR*	Optimal *N*	Capacity	*PSNR*
Airplane	79	30668	49.62	35	42888	50.27	18	66015	50.16
Baboon	93	12033	51.48	36	23935	52.20	17	51086	51.75
Barbara	85	23253	51.47	36	38372	51.37	17	66876	51.13
Boat	75	19608	51.39	35	29908	51.62	17	53551	51.61
Bridge	40	38589	51.95	34	47881	51.01	16	96690	50.51
Couple	61	21535	51.03	35	33865	51.21	13	65208	51.43
Lena	75	24627	50.86	35	37679	50.93	16	62124	50.90

From this table, one can observe that maximum capacity is 38,589 bits and maximum PSNR is 51.95 dB for Bridge image when block size is 16×16**;** maximum capacity is 47,881 bits for Bridge image and maximum PSNR is 52.20 dB for Baboon image when block size is 8×8; maximum capacity is 96,690 bits for Bridge image and maximum PSNR is 51.75 dB for Baboon

image when block size is 4×4. It can be observed that hiding capacity increases when the block size decreases. Also, the proposed technique is compared with the existing histogram based data hiding techniques on the basis of hiding capacity and PSNR. The optimal block size is considered for each of the technique in this comparison. Four standard images, named as Lena, Boat, Baboon and Airplane are considered in this comparison.

Table 3.2 Comparison of capacity (in bits) and PSNR (in dB) of the proposed technique with existing techniques.

Image → / **Technique** ↓	**Block Size**	**Lena**		**Airplane**		**Boat**		**Baboon**	
		Capacity	**PSNR**	**Capacity**	**PSNR**	**Capacity**	**PSNR**	**Capacity**	**PSNR**
Ni *et al.* (2006)	No Block	5460	48.2	16171	48.30	7301	48.2	5421	48.2
Fallahpour *et al.* (2007)	128×128	13868	47.29	29250	48.56	15579	46.73	7874	47.12
Kuo *et al.* (2008)	8×8	33931	48.73	50920	49.15	40379	48.81	12909	48.46
Lin *et al.* (2008)	No Block	65394	48.67	69941	48.67	56713	48.67	38465	48.67
Tsai *et al.* (2009)	No Block	47912	49.06	64996	49.24	-	-	15820	48.73
Luo *et al.*(2011)	4×4	29813	48.68	44786	48.83	-	-	9522	48.50
Chang *et al.* (2012)	No Block	45038	48.98	65698	49.54	46425	49.01	14361	48.38
Mali *et al.* (2012)	No Block	14357	41.72	-	-	21063	41.08	40075	39.67
Proposed	4×4	62124	50.90	66015	50.16	53551	51.61	51086	51.75

From referenced table one can observe that maximum capacity of Ni et al.(2006) method is 16,171 bits and maximum PSNR is 48.3 dB**;** maximum capacity of Fallahpour *et al.* (2007) method is 29,250 bits and maximum PSNR of Fallahpour *et al.* method is 48.56 dB; maximum capacity of Kuo *et al.* (2008) method is 50,920 bits and maximum PSNR of Kuo *et al.* (2008) method is 49.15 dB; maximum capacity of Chang *et al.* (2012) is 65,698 bits and maximum PSNR is 49.54 dB. Maximum capacity of proposed technique is 66,015 bits and maximum PSNR is 51.75 dB. One can conclude that hiding capacity and PSNR of our proposed technique are better than the existing techniques.

3.6 Conclusion

In this chapter, a histogram based reversible data hiding technique for digital images is proposed. Modulus operator is used to increase the occurrence of peak points of a cover image. Extracted secret image is similar to original secret image. Maximum capacity is more than 96,000 bits and PSNR is also higher than 50 dB. Embedding capacity and PSNR are higher than existing histogram based data hiding techniques (Ni *et al.*,2006; Fallahpour *et al.*,2007; Kuo *et al.*, 2008; Lin *et al.*, 2008; Tsai *et al.*, 2009; Luo *et al.*, 2011; Chang *et al.*, 2012; Mali *et al.*, 2012).

CHAPTER 4

MODULUS BASED MULTILEVEL REVERSIBLE DATA HIDING USING MODIFIED HISTOGRAM

4.1 Introduction

In this chapter, a multilevel reversible data hiding technique using histogram and modulus function is proposed. The cover image is divided into non overlapping blocks of same size and histogram of each block is generated after applying modulus function. Histogram shifting approach is used to embed the secret information in the blocks of the cover image; secret information is embedded into pixel of cover image using peak points occurring in its histogram of a cover image. The proposed technique is based on the observation that if modulus operator using some integer number is applied on the cover image then the occurrence of peak points in the histogram of an image increases and this increases the embedding capacity of a cover image. Data embedding and data extraction algorithm used in proposed technique are explained in following subsection.

4.2 Data embedding algorithm

Input: Cover image C of size $m \times m$, a secret image S of size $r \times r$ and modulus factor t

Output: A marked image M.

Step 1: Cover image C is decomposed into cover blocks CB_b of size $n \times n$ where $b = 1,2,..,\frac{m \times m}{n \times n}$

Step 2: To embed the secret information into each cover block CB_b perform following operations.

(a) Apply modulus function on each pixel of cover block CB_b to get prediction block PB_b.

(b) Generate histogram H_b of $\mathrm{PB_b}$ and find the peak point $p_b \epsilon\, [0, n-1]$ and minimum point $z_b \epsilon\, [0, n-1]$ and generate location map for minimum point z_b as overhead information. This overhead information is required on the receiver side to extract the hidden information.

(c) Shift each pixel of cover block CB_b in right or left according to p_b and z_b to get the marked block MB_b using prediction block.

if $p_b < z_b$

if $p_b < PB_b(u,v) < z_b$

$$MB_b(u,v) = CB_b(u,v) + 1$$

else

$$MB_b(u,v) = CB_b(u,v)$$

endif

endif

if $p_b > z_b$

if $\mathrm{p_b} > \mathrm{PB_b(u,v)} > \mathrm{z_b}$

$$MB_b(u,v) = CB_b(u,v) - 1$$

else

$$MB_b(u,v) = CB_b(u,v)$$

endif

endif

(d) Scan pixels of block CB_b and secret image S in raster scan order and embedded the secret information in original blocks CB_b to get marked block MB_b using the following expressions.

if $PB_b(u,v) = p_b$

if $S = 1 \ and \ p_b < z_b$

$$MB_b(u,v) = CB_b(u,v) + 1$$

elseif $S = 1 \ and \ p_b > z_b$

$$MB_b(u,v) = CB_b(u,v) - 1$$

elseif $S = 0$

$$MB_b(u,v) = CB_b(u,v)$$

endif

endif

Step 3: Combine each block MB_b to form marked image M.

4.3 Data extraction algorithm

Input: Marked image M of size $m \times m$, modulus factor t and overhead information.

Output: A cover image C' and secret image S'

Step 1: Decompose marked image M' of size $m \times m$ into blocks MB_b' of size $n \times n$ where $b = 1,2,..,\frac{m \times m}{n \times n}$

Step 2: To extract the secret image from each block MB_b', perform the following operations

(a) Apply modulus function on each pixel of block MB_b' to get prediction block PB_b'.

(b) Scan the pixel of PB_b' in raster scan method and extract the data using the following expressions

if $p_b < z_b$

if $PB_b'(u,v) = p_b + 1$

$S' = 1$

elseif $PB_b'(u,v) = p_b$

$S' = 0$

endif

endif

if $p_b > z_b$

if $PB_b'(u,v) = p_b - 1$

$S' = 1$

elseif $PB_b'(u,v) = p_b$

$S' = 0$

endif

endif

(c) Reverse shift each pixel of MB_b' in right or left according to the peak point (p_b) and minimum point (z_b) as using following expression.

if $p_b < z_b$

if $p_b < PB_b'(u,v) \leq z_b$

$CB_b'(u,v) = MB_b'(u,v) - 1$

else

$CB_b'(u,v) = MB_b'(u,v)$

endif

endif

If $p_b < z_b$

if $p_b > PB_b'(u,v) \geq z_b$

$CB_b'(u,v) = MB_b'(u,v) + 1$

else

$CB_b'(u,v) = MB_b'(u,v)$

Step 3: Combine all blocks CB_b' to get cover image C'.

An example to illustrate the proposed technique with modulus factor 16 is shown in Fig. 4.1 – 4.7. A 6×6 block of an image, shown in Fig. 4.1 is predicted using modulus factor 16, as show in Fig. 4.2. Secret data considered is '10110011'. Intermediate marked block and final marked blocks are shown in Fig. 4.3 and Fig. 4.4 respectively. Extraction process steps are shown in Fig. 4.5-4.7.

155	176	185	171	112	121
123	134	123	136	117	136
146	147	198	120	111	115
156	165	176	119	125	114
149	166	187	105	106	107
137	136	187	189	195	199

Fig. 4.1 Cover Block (peak point : 123)

11	0	9	11	0	9
11	6	11	8	5	8
2	3	6	8	5	3
12	5	0	7	13	2
5	6	11	9	10	11
11	8	11	13	3	7

Fig. 4.2 Embedding Prediction Block (peak point : 11 and minimum point : 14)

155	176	185	171	112	121
123	134	123	136	117	136
146	147	198	120	111	115
157	165	176	119	126	114
149	166	187	105	106	107
137	136	187	190	195	199

Fig. 4.3 Intermediate Marked Block (after shifting)

156	176	185	171	112	121
124	134	124	136	117	136
146	147	198	120	111	115
157	165	176	119	126	114
149	166	187	105	106	107
138	136	188	190	195	199

Fig. 4.4 Marked Block (after embedding secret data : 10110011)

12	0	9	11	0	9
12	6	12	8	5	8
2	3	6	8	5	3
13	5	0	7	14	2
5	6	11	9	10	11
12	8	12	14	3	7

Fig. 4.5 Extracting Prediction Block

155	176	185	171	112	121
123	134	123	136	117	136
146	147	198	120	111	115
157	165	176	119	126	114
149	166	187	105	106	107
137	136	187	190	195	199

Fig. 4.6 Intermediate Cover Block

155	176	185	171	112	121
123	134	123	136	117	136
146	147	198	120	111	115
156	165	176	119	125	114
149	166	187	105	106	107
137	136	187	189	195	199

Fig. 4.7 Final Extracted Cover Block

This example show how secret data is embedded onto blocks of a cover image and extracted using 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.

4.4.1 Experimental Results

Proposed technique is implemented using MATLAB software tool and different standard test images namely Airplane, Baboon, Barbara, Boat, Bridge and Lena each of size 512 × 512 are used as the cover images. The visual quality of marked image is the most important property of data hiding because it is hard to detect by detectors. Copyright image shown in Fig. 4.8 is taken as the secret image. The data of this secret image is embedded into cover images using different embedding level.

Fig. 4.8 Copyright Image

Some of the cover images and their marked images after different level of embedding are shown in Fig. 4.9.

(a) Bridge image

(b) Marked bridge image using 8×8 block size (level 1)

(c) Marked bridge image using 8×8 block size (level 3)

(d) Marked bridge image using 8×8 block size (level 6)

(e) Marked bridge image using 8×8 block size (level 9)

(f) Lena image

(g) Marked lena image using 8×8 block size (level 1)

(h) Marked lena image using 8×8 block size (level 3)

(i) Marked lena image using 8×8 block size (level 6)

(j) Marked lena image using 8×8 block size (level 9)

(k) Boat image

(l) Marked boat image using 8×8 block size (level 1)

(m) Marked boat image using 8×8 block size (level 3)

(n) Marked boat image using 8×18 block size (level 6)

(o) Marked boat image using 8×8 block size (level 9)

(p) Barbara image

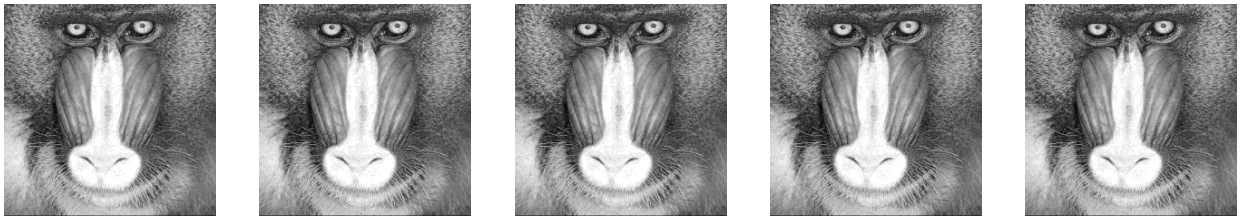
(q) Marked barbara image using 8×8 block size (level 1)

(r) Marked barbara image using 8×8 block size (level 3)

(s) Marked barbara image using 8×8 block size (level 6)

(t) Marked barbara image using 8×8 block size (level 9)

(u) Airplane image | (v) Marked airplane image using 8×8 block size (level 1) | (w) Marked airplane image using 8×8 block size (level 3) | (x) Marked airplane image using 8×18 block size (level 6) | (y) Marked airplane image using 8×8 block size (level 9)



(z) Baboon image | (aa) Marked baboon image using 8×8 block size (level 1) | (ab) Marked baboon image using 8×8 block size (level 3) | (ac) Marked baboon image using 8×18 block size (level 6) | (ad) Marked baboon image using 8×8 block size (level 9)

Fig. 4.9 Different cover images and their marked images after different level of embedding

Table 4.1 shows the embedding capacity in (bpp), PSNR (in dB) for different block size, different modulus factors and different level for all images considered in this work.

Table 4.1 Embedding capacity (in bpp) and PSNR (in dB) of proposed technique for different images at different block size and different modulus factor

Block Size	Module Factor	1st Level		3th Level		6th Level		9th Level	
		Total Capacity (bpp)	PSNR (dB)	Total Capacity (bpp)	PSNR (dB)	Total Capacity (bpp)	PSNR (dB)	Total Capacity (bpp)	PSNR (dB)
Bridge Image									
4×4	16	0.3688	52.7187	1.0367	48.6675	1.9050	45.6657	2.6600	44.4435
	32	0.2959	53.7793	0.8349	48.6899	1.5452	44.6844	2.1711	43.2977
	64	0.2717	54.2526	0.7672	48.449	1.4196	43.6195	1.9947	41.9760
	128	0.2696	54.3171	0.7614	48.21795	1.4093	42.9487	1.9801	41.1367
	256	0.2696	54.3214	0.7614	48.01339	1.4093	42.6611	1.9801	40.7571
8×8	16	0.2876	53.6369	0.8139	49.70696	1.5128	46.2170	2.1300	44.7684
	32	0.2095	55.2041	0.5935	50.72986	1.1011	47.7447	1.5527	46.1187
	64	0.1825	55.9458	0.5149	51.15873	0.9540	47.8235	1.3451	46.4013
	128	0.1798	56.0944	0.5079	50.8099	0.9421	47.2381	1.3282	45.8720
	256	0.1798	56.1111	0.5079	50.61054	0.9421	47.0361	1.3282	45.6646
16×16	16	0.2395	54.1901	0.6848	50.11989	1.2875	46.1719	1.8302	44.8874

	32	0.1598	56.2112	0.4544	51.85125	0.8539	47.3765	1.2152	44.8207
	64	0.1312	57.307	0.3728	52.43878	0.6976	48.9936	0.9894	46.9110
	128	0.1276	57.5498	0.3620	52.02886	0.6777	48.4870	0.9609	46.9898
	256	0.1276	57.5971	0.3620	51.55242	0.6777	48.0536	0.9609	46.6675
32×32	16	0.2092	54.0937	0.6033	50.16141	1.1485	46.0668	1.6484	45.5199
	32	0.1315	56.7756	0.3755	52.5402	0.7130	46.3149	1.0247	43.5876
	64	0.0995	58.2864	0.2832	53.54428	0.5386	48.4903	0.7726	45.6526
	128	0.0953	58.7973	0.2721	53.2387	0.5156	48.5047	0.7380	46.5267
	256	0.0953	58.8721	0.2721	52.16089	0.5156	47.7759	0.7380	45.8887
Lena Image									
4×4	16	0.2369	51.9877	0.6735	44.601	1.2579	42.0691	1.7830	40.8391
	32	0.2235	52.7294	0.6364	45.2928	1.1916	42.4341	1.6909	40.6649
	64	0.2197	52.8685	0.6258	45.2767	1.1702	42.2033	1.6581	40.3231
	128	0.2187	52.9447	0.6232	45.3652	1.1660	42.1967	1.6531	40.2048
	256	0.2186	53.0268	0.6228	45.3926	1.1656	42.0954	1.6520	39.9817
8×8	16	0.1590	51.3822	0.4574	44.1874	0.8757	42.5748	1.2706	41.9065
	32	0.1446	52.119	0.4130	43.5198	0.7780	40.4104	1.1096	38.4959
	64	0.1396	52.626	0.3989	44.2374	0.7509	41.1687	1.0699	39.1323
	128	0.1381	52.765	0.3946	44.4583	0.7426	41.414	1.0577	39.4224
	256	0.1379	52.8791	0.3943	44.7051	0.7421	41.8297	1.0572	39.9731
16×16	16	0.1168	51.2241	0.3510	45.3744	0.7004	44.4831	1.0461	44.1421
	32	0.1000	51.3194	0.2883	42.7353	0.5518	39.6504	0.7983	37.5775
	64	0.0947	51.8499	0.2729	42.5153	0.5198	38.7197	0.7474	36.2765
	128	0.0926	52.3992	0.2665	43.0801	0.5072	39.3249	0.7288	36.9603
	256	0.0922	52.6259	0.2655	43.6302	0.5057	39.9605	0.7267	37.648
32×32	16	0.0944	51.4586	0.3040	48.2679	0.6283	47.1543	0.9515	46.9866
	32	0.0745	51.354	0.2188	43.0946	0.4262	40.4447	0.6256	38.6591
	64	0.0675	51.5959	0.1962	42.1785	0.3780	38.1086	0.5486	35.7379
	128	0.0648	52.1375	0.1880	42.2859	0.3615	37.7911	0.5237	35.0905
	256	0.0643	52.6529	0.1864	42.8653	0.3586	38.477	0.5194	35.7626
Boat Image									
4×4	16	0.2081	53.0925	0.5941	46.4800	1.1158	44.4051	1.5951	43.5233
	32	0.1860	54.1826	0.5316	47.4433	0.8180	44.9450	1.4371	43.4561
	64	0.1796	54.4793	0.5140	47.4548	0.7904	44.6539	1.3881	42.9823
	128	0.1775	54.5502	0.5079	47.4189	0.7803	44.4848	1.3693	42.6723
	256	0.1772	54.6205	0.5072	47.3720	0.7795	44.1256	1.3687	41.9843
8×8	16	0.1386	51.9948	0.4012	46.3758	0.6389	45.6069	1.1433	45.1499
	32	0.1160	53.1127	0.3324	44.6942	0.5121	41.8399	0.9001	40.1397
	64	0.1086	53.9818	0.3107	45.9372	0.4783	43.0390	0.8407	41.0717
	128	0.1064	54.1624	0.3043	46.1173	0.4690	43.2454	0.8240	41.2886
	256	0.1059	54.3149	0.3030	46.3793	0.4666	43.5871	0.8194	41.7708
16×16	16	0.1071	51.7868	0.3245	48.0888	0.5502	47.5097	0.9921	47.2083
	32	0.0830	51.9748	0.2400	44.0074	0.3781	41.5169	0.6710	39.9226

	64	0.0756	52.2349	0.2173	43.1240	0.3384	39.6178	0.5969	37.4172
	128	0.0732	52.8260	0.2108	43.6155	0.3285	39.9218	0.5788	37.5360
	256	0.0725	53.1745	0.2088	44.2256	0.3254	40.7072	0.5731	38.5057
32×32	16	0.0914	51.6958	0.2952	50.6739	0.5235	49.5968	0.9357	49.1183
	32	0.0659	51.6479	0.1943	44.6319	0.3155	42.8603	0.5647	41.6045
	64	0.0571	51.5035	0.1658	42.4431	0.2609	38.8035	0.4611	36.3998
	128	0.0547	51.8255	0.1582	41.7297	0.2479	37.2464	0.4375	34.3364
	256	0.0537	52.7125	0.1553	42.9584	0.2434	38.5993	0.4297	35.9173
Barbara Image									
4×4	16	0.2581	52.2417	0.7301	44.5285	1.3531	41.8145	1.9041	40.5963
	32	0.2378	53.0785	0.6740	45.0946	1.2523	41.8975	1.7642	40.1247
	64	0.2297	53.4753	0.6506	45.0418	1.2078	41.3623	1.6990	39.3409
	128	0.2275	53.5616	0.6437	45.0238	1.1926	41.2182	1.6754	39.0528
	256	0.2275	53.5940	0.6435	44.9885	1.1927	41.0516	1.6766	38.7673
8×8	16	0.1703	51.7263	0.4865	45.1289	0.9214	43.0738	1.3279	42.1127
	32	0.1485	52.7468	0.4211	44.1505	0.7840	41.1027	1.1058	39.3168
	64	0.1393	53.8403	0.3940	45.4915	0.7316	42.0945	1.0295	40.1321
	128	0.1366	54.0676	0.3865	45.7442	0.7179	42.3429	1.0091	40.3725
	256	0.1364	54.1561	0.3864	45.8023	0.7167	42.4343	1.0075	40.4052
16×16	16	0.1231	51.6684	0.3684	46.8800	0.7338	45.4752	1.0928	44.9288
	32	0.0996	51.7280	0.2844	43.9809	0.5389	41.3018	0.7753	39.5569
	64	0.0896	52.4924	0.2548	43.5246	0.4780	40.0730	0.6792	38.0466
	128	0.0866	53.4152	0.2459	44.2432	0.4605	40.4679	0.6536	38.3177
	256	0.0861	53.7289	0.2446	44.6033	0.4582	41.0195	0.6499	38.8702
32×32	16	0.0968	51.6302	0.3164	48.9911	0.6517	47.7307	0.9839	47.5529
	32	0.0718	51.4964	0.2123	45.0274	0.4147	42.6619	0.6094	40.9752
	64	0.0610	52.0414	0.1756	43.4025	0.3343	40.3512	0.4811	38.2086
	128	0.0571	52.5465	0.1642	42.8269	0.3111	38.5621	0.4441	36.0470
	256	0.0560	53.5828	0.1607	43.7681	0.3037	39.4993	0.4336	36.7890
Airplane Image									
4×4	16	0.2554	51.2253	0.7240	43.6666	1.3478	41.1771	1.9061	44.4435
	32	0.2418	51.8930	0.6867	44.3972	1.2816	41.4372	1.8127	43.2977
	64	0.2375	52.0211	0.6741	44.2940	1.2569	41.2524	1.7755	41.9760
	128	0.2358	52.1924	0.6690	44.4293	1.2460	41.2574	1.7594	41.1367
	256	0.2355	52.1991	0.6682	44.3861	1.2449	41.0815	1.7581	40.7571
8×8	16	0.1785	50.6897	0.5093	43.5714	0.9640	41.5562	1.3884	44.7684
	32	0.1642	51.3243	0.4665	42.9257	0.8732	40.0052	1.2382	46.1187
	64	0.1591	51.8078	0.4518	43.3932	0.8445	40.2844	1.1960	46.4013
	128	0.1575	52.1033	0.4478	43.9497	0.8362	41.0757	1.1844	40.0076
	256	0.1571	52.1238	0.4463	43.9224	0.8337	40.9943	1.1811	39.6652
16×16	16	0.1384	50.5135	0.4082	44.5865	0.8009	42.9162	1.1820	39.4632
	32	0.1233	50.7378	0.3539	42.3170	0.6708	39.0442	0.9611	39.3129
	64	0.1177	51.0723	0.3376	41.9666	0.6360	38.2331	0.9075	39.0955

	128	0.1160	51.6249	0.3326	42.718	0.6258	39.0933	0.8928	40.6375
	256	0.1152	51.7614	0.3300	42.9198	0.6216	39.2952	0.8869	38.0661
32×32	16	0.1152	50.5538	0.3581	46.1208	0.7178	44.2136	1.0659	38.2517
	32	0.0992	50.5909	0.2861	42.4927	0.5495	39.3185	0.7985	39.207
	64	0.0935	51.1573	0.2688	41.6454	0.5113	37.5851	0.7333	39.1841
	128	0.0915	51.4843	0.2632	41.4210	0.4984	37.2876	0.7143	41.9632
	256	0.0901	51.9573	0.2595	41.9123	0.4904	37.8053	0.7019	36.9892
Baboon Image									
4×4	16	0.1986	53.2139	0.5669	46.5098	1.0683	44.6737	1.5323	43.9238
	32	0.1644	55.0162	0.4736	48.4808	0.9019	46.2722	1.2948	44.9866
	64	0.1498	55.7116	0.4317	48.3510	0.8187	45.4376	1.1712	43.8733
	128	0.1438	55.9648	0.4138	48.1101	0.7846	44.6901	1.1240	42.6632
	256	0.1432	56.0186	0.4120	47.8797	0.7805	43.9789	1.1180	41.4617
8×8	16	0.1280	52.2342	0.3731	47.3913	0.7325	46.9893	1.0875	46.7661
	32	0.0946	54.0010	0.2723	45.9080	0.5197	44.0835	0.7511	43.0100
	64	0.0798	56.1013	0.2293	48.4464	0.4367	45.6348	0.6298	43.4839
	128	0.0746	56.5754	0.2145	48.9508	0.4085	46.2229	0.5889	44.3863
	256	0.0742	56.7037	0.2133	49.1380	0.4059	46.4058	0.5847	44.5814
16×16	16	0.0946	52.0843	0.3008	51.3672	0.6251	50.4730	0.9536	49.9860
	32	0.0626	52.4099	0.1834	46.3088	0.3616	45.1855	0.5375	44.5689
	64	0.0491	52.7415	0.1417	44.1530	0.2717	41.1879	0.3953	39.3043
	128	0.0445	54.2412	0.1281	44.9363	0.2458	41.2760	0.3572	38.6999
	256	0.0440	54.5957	0.1268	45.5814	0.2431	42.1099	0.3527	39.6933
32×32	16	0.0791	51.8997	0.2903	54.3762	0.6240	52.8330	0.9529	52.4060
	32	0.0480	52.092	0.1518	49.4564	0.3131	48.0918	0.4727	47.5623
	64	0.0346	51.6597	0.1017	43.9851	0.1996	40.7976	0.2951	38.5474
	128	0.0301	51.7979	0.0872	42.1186	0.1680	38.2505	0.2454	35.5878
	256	0.0295	52.3616	0.0856	42.4860	0.1649	38.2639	0.2408	35.3454

Table 4.1 shows the effect of different modulus factor, different block size and different embedding level on test images. One can infer that embedding capacity increases with level of embedding. Multilevel embedding increases the security because no one would know how many levels has been used in data embedding.

Proposed technique is compared with existing multilevel data hiding techniques and this comparison is shown in Table 4.2 Embedding capacity and PSNR between cover image and marked image are taken as comparison parameter. This comparison shows that embedding capacity of proposed technique is higher and distortion in marked images is low than existing multilevel data hiding techniques.

Table 4.2 Comparison of embedding capacity (in bpp) and PSNR (in dB) of proposed technique with different existing techniques for different images at different embedding level.

Image	Technique		1st	2nd	3rd	6th	9th
Lena	C. C. Lin *et al.*(2008)	Capacity	0.2492	0.4423	0.6058	1.000	1.3220
		PSNR	48.67	43.02	39.64	33.7	30.19
	C. T. Wang *et al.*(2012)	Capacity	0.1084	0.3765	0.7879	0.9994	1
		PSNR	50.75	49.81	48.78	48.18	48.14
	Proposed Technique	Capacity	0.2369	0.4609	0.6735	1.2579	1.7830
		PSNR	51.98	47.25	46.31	43.07	41.72
Airplane	C. C. Lin *et al.*(2008)	Capacity	0.2668	0.4717	0.6438	1.0542	1.3841
		PSNR	48.67	43.02	39.64	33.7	30.19
	C. T. Wang *et al.*(2012)	Capacity	0.1924	0.3804	0.5762	0.9311	0.9927
		PSNR	50.75	49.81	48.78	48.18	48.14
	Proposed Technique	Capacity	0.2554	0.4959	0.7240	1.3478	1.9061
		PSNR	51.22	46.35	45.44	42.13	40.79
Baboon	C. C. Lin *et al.*(2008)	Capacity	0.1467	0.2698	0.3785	0.6513	0.8776
		PSNR	48.67	43.02	39.64	33.7	30.19
	C. T. Wang *et al.*(2012)	Capacity	0.0543	0.5907	0.9568	0.9999	0.9999
		PSNR	50.75	49.81	48.78	48.18	48.14
	Proposed Technique	Capacity	0.1986	0.3871	0.5669	1.0683	1.5323
		PSNR	53.21	48.88	48.02	45.35	44.50

Maximum embedding capacity of proposed technique at 1st level is nearly same as Lin *et al.* (2208) technique but higher than Wang *et al.* (2012) technique whereas PSNR of proposed technique is higher than both techniques around 0.9 dB. As the level increases, embedding capacity of proposed technique is higher than both Lin et al. (2008) and Wang et al. (2012) techniques. At 9th level embedding capacity of proposed technique is 1.7830, 1.9061, 1.5323 bpp for lena, airplane and baboon respectively which is 0.45 bpp higher than Lin et al. (2008) and Wang et al. (2012) techniques.

4.5 Conclusion

In this chapter, histogram based multi level reversible data hiding technique is proposed. Modulus operator is used to increase the occurrence of peak points of a cover image. Secret information is embedded into blocks of cover image using histogram technique. Extracted secret image and cover image are similar to original secret image and original cover image

respectively. Proposed technique provides better embedding capacity and better visual quality of marked image than existing multilevel data hiding techniques.

CHAPTER 5

BLIND DATA HIDING TECHNIQUE USING INTERPOLATION OF SUBSAMPLED IMAGES

5.1 Introduction

In this chapter, difference images are generated using interpolation of sub sampled images and on the basis of even or odd state of the difference pixel value; the secret information is embedded into the original image. In terms of data hiding performance, the proposed technique not only has low computational complexity, it also significantly improves the embedding capacity and distortion in the marked images.

Image interpolation is an image processing technique using which a small image is scaled-up into its larger version. Interpolating methods stretch the size of the image by using known data to estimate values at unknown points. Some image quality is lost in interpolated image when interpolation is performed. Data hiding scheme embeds secret information within the estimated values of the interpolated image. Many data hiding techniques have been proposed using interpolation approaches (Yang, 2008; Jung, 2009; Luo, 2010; Abadi, 2010; Hong, 2011; Wang, 2013).

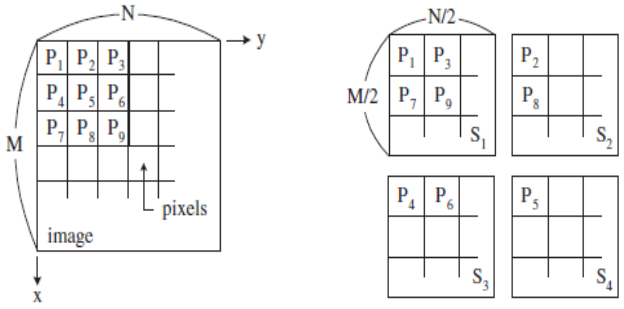
5.2 Image subsampling

It is a process of selecting the pixels from the image. Suppose that an image of size $m \times n$ is denoted by $I(x,y)$, where $x = 0, 1, 2, \ldots, m-1$and $y = 0, 1, 2, \ldots, n-1$. Two sampling factors, Δu and Δv are used to set the desired sum-sampling intervals in a row and column directions, respectively. As shown in Fig. 1, an image is sampled at uniform intervals. This process is called sub-sampling and each subsampled image S_K of size $\frac{m}{\Delta u} \times \frac{n}{\Delta v}$ is obtained as follow:

$$S_k(i,j) = I(i.\Delta u + floor\left(\frac{k-1}{\Delta v}\right), j.\Delta v + \left((k-1) mod\ \Delta u\right) \quad ...(1)$$

Where i = 0, 1, 2, . . .m/Δu and j=0,1,2,. . .n/Δv.

For example, if m = n = 512 and $\Delta u = \Delta v$=5. The size of subsampled image is set at the nearest integer less than or equal to the number: $\left\lfloor\frac{512}{5}\right\rfloor$ = 102 in both height and width. Residue pixels are neither included in any subsampled images nor targeted embeddable components by proposed technique.



(a) (b)

Fig. 5.1 Sub-Sampling Example at Sampling Factor (a) Original (b) $\Delta u = \Delta v = 2$

5.3 Data embedding algorithm

Input: A grayscale cover image C of size $m \times n$ and a binary secret image H.

Output: A marked image M'.

Step 1: Generate sub-sampled images S_i of size $\frac{m}{\Delta u} \times \frac{n}{\Delta v}$ of the cover image C using (1), where i = 1, 2,..,..$\Delta u \times \Delta v$.

Step 2: Take a reference sub-sampled image S_{ref} from sub-sampled images S_i. This sub-sampled image S_{ref} is used on the extraction side to recover the secret data.

Step 3: Interpolate sub sampled image S_{ref} by a factor of Δu and Δv, to generate interpolated image Ic.

Step 4: Generate interpolated sub-sampled images IS_i of size $\frac{m}{\Delta u} \times \frac{n}{\Delta v}$ of the interpolated image Ic using (1), where i = 1, 2, ..$\Delta u \times \Delta v$.

Step 5: Create the difference images D_i between the sub-sampled images S_i and interpolated sub-sampled images IS_i, except the reference sub-sampled image S_{ref} and its corresponding interpolated sub-sampled image, using the expression.

$$D_i(x,y) = S_i(x,y) - IS_i(x,y)$$

where $0 \le x \le \frac{m}{\Delta u}$ and $0 \le y \le \frac{n}{\Delta v}$

Step 6: (Data Embedding)

$$S_i'(x,y) = \begin{cases} S_i(x,y), & if\ H = 0\ and\ mod\ (D_i(x,y),2) = 0 \\ S_i(x,y)+1, & if\ H = 0\ and\ mod\ (D_i(x,y),2) = 1 \\ S_i(x,y), & if\ H = 1\ and\ mod\ (D_i(x,y),2) = 1 \\ S_i(x,y)+1, & if\ H = 1\ and\ mod\ (D_i(x,y),2) = 0 \end{cases}$$

Step 7: Finally obtain the marked image M' through the inverse of sub-sampling with the unmodified S_{ref} and modified sub-sampled images S_i'.

5.4 Data extraction algorithm

Input: A grayscale marked image M' of size $m \times n$.

Output: A cover image C' and a binary secret image H'.

Step 1: Generate sub-sampled images S_i' of size $\frac{m}{\Delta u} \times \frac{n}{\Delta v}$ of the marked image M' using (1), where $i = 1,2, \dots, \Delta u \times \Delta v$.

Step 2: Take a reference sub-sampled image S_{ref}' from sub-sampled images S_i'. This sub-sampled image S_{ref}' is same which is used at used at the embedding side to conceal the secret data.

Step 3: Interpolate sub sampled image S_{ref}' by a factor of Δu and Δv, to generate interpolated image Ic'.

Step 4: Generate interpolated sub-sampled images IS_i' of size $\frac{m}{\Delta u} \times \frac{n}{\Delta v}$ of the interpolated image Ic' using (1), where i = 1, 2, ..$\Delta u \times \Delta v$.

Step 5: Create the difference images D_i' between the sub-sampled images S_i' and interpolated sub-sampled imagesIS_i', except the reference sub-sampled image S_{ref}' and its corresponding interpolated sub-sampled image, using the expression

$$D_i'(x,y) = S_i'(x,y) - IS_i'(x,y)$$

where$0 \le x \le \frac{m}{\Delta u}$ and $0 \le y \le \frac{n}{\Delta v}$

Step 6: (Data Extraction)

$$H' = \begin{cases} 0, & mod\left(D_i'((x,y),2)\right) == 0 \\ 1, & mod\left(D_i'((x,y),2)\right) == 1 \end{cases}$$

Step 7: Finally obtain the secret image H'.

5.5 Experimental results

Proposed technique is implemented in MATLAB software. Different 8 bits gray scale images namely as lena, barbara, baboon, boat and airplane, each of size 512×512 size were used in experiment. To extract the secret data, no cover image is required, so the proposed technique is blind. Embedding capacity in (bpp) measures the amount of data that can be hidden in a cover image. Effect of different embedding capacity on distortion is studied in proposed work.

Table 5.1 PSNR (in dB) of different images at different embedding capacity of proposed technique

Embedding Capacity	Lena	Barbara	Boat	Baboon	Airplane
1000	74.90	75.09	75.42	75.54	74.25
5000	67.97	68.10	68.38	68.35	67.42
10000	64.98	65.15	65.34	65.26	64.43
25000	60.97	61.18	61.32	61.30	60.46
50000	57.99	58.20	58.35	58.31	57.45
100000	54.97	55.19	55.35	55.31	54.45
150000	53.22	53.44	53.58	53.55	52.67
196608	52.04	52.28	52.40	52.39	51.49

From table 5.1, one can infer that as embedding capacity increases, distortion in the marked image increases. Maximum embedding capacity is 196609 bits. At maximum capacity, minimum PSNR is 51.48 which is acceptable by human visual system. Boat image gives highest PSNR value 52.40 with embedding capacity 196608 bits among all experiment images. For extract secret images, *SIM* is 1 as there is no data loss in extracted secret images.

Some of the cover images and their marked images at different embedding capacity are shown in Fig. 5.2.

(a) Lena image

(b) Marked lena image (embedding capacity : 10000 bits)

(c) Marked lena image (embedding capacity : 50000 bits)

(d) Marked lena image (embedding capacity : 100000 bits)

(e) Marked lena image (embedding capacity : 196608 bits)

(f) Barbara image

(g) Marked barbara image (embedding capacity : 10000 bits)

(h) Marked barbara image (embedding capacity : 50000 bits)

(i) Marked barbara image (embedding capacity : 100000 bits)

(j) Marked barbara image (embedding capacity : 196608 bits)

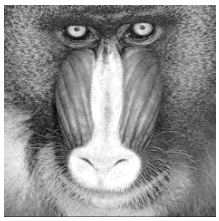
(k) Airplane image

(l) Marked airplane image (embedding capacity : 10000 bits)

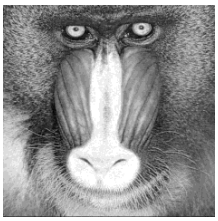
(m) Marked airplane image (embedding capacity : 50000 bits)

(n) Marked airplane image (embedding capacity : 100000 bits)

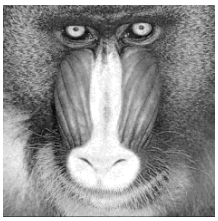
(o) Marked airplane image (embedding capacity : 196608 bits)



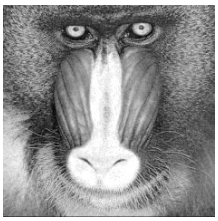
(p) Baboon image



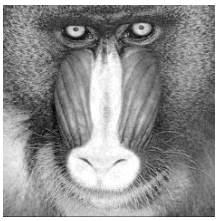
(q) Marked baboon image (embedding capacity : 10000 bits)



(r) Marked baboon image (embedding capacity : 50000 bits)



(s) Marked baboon image (embedding capacity : 100000 bits)



(t) Marked baboon image (embedding capacity : 196608 bits)

(u) irplane image

(v) Marked airplane image (embedding capacity : 10000 bits)

(w) Marked airplane image (embedding capacity : 50000 bits)

(x) Marked airplane image (embedding capacity : 100000 bits)

(y) Marked airplane image (embedding capacity : 196608 bits)

Fig. 5.2 Different cover images and their marked images different embedding capacity

Proposed technique is compared with the existing interpolation based data hiding techniques. For this comparison, Lena, Baboon, Airplane and Boat images of size 512×512 size are considered. In this comparison, PSNR and maximum embedding capacity of techniques are taken in consideration.

Table 5.2 Embedding capacity (in bits)/PSNR (in dB) comparison of the proposed technique with existing techniques

Embedding Technique	Lena Image	Baboon	Airplane
Yang *et al.*(2008)	10874/45.77	7706/41.46	9374/45.49
Jung *et al.*(2009)	200868/41.46	425199/35.46	378829/40.02
Luo *et al.*(2010)	71674/48.82	22696/48.36	84050/48.94
Abadi*et al.*(2010)	73207/48.78	45043/48.52	86964/48.92
Hong *et al.*(2011)	47549/49.98	13024/51.24	64923/50.31
Wang *et al.*(2013)	71191/48.80	24855/48.50	87301/48.94
Proposed Technique	196608/52.03	196608/52.39	196608/51.48

From this table, one can infer that proposed technique provides better PSNR than other existing techniques and hence less distortion in the marked images than the distortion of the other existing interpolation based techniques. Maximum embedding capacity of proposed technique is 1,96,608 bits for all four images while maximum embedding capacity of Jung *et al.*(2009) is 4,25,199 bits, but PSNR is Jung *et al.*(2009) technique is 35.46 dB which is very less than proposed technique's PSNR.

5.6 Conclusion

In this chapter, a data hiding technique based on interpolation of subsampled versions of a cover image is proposed. Comparisons with the existing interpolation based techniques show that proposed technique provides higher embedding capacity and better visual quality marked images. In addition, the performance of the proposed technique is more stable for different images.

CHAPTER 6
CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

In this dissertation, various data hiding techniques for digital images are proposed. First, a data hiding technique using histogram and modulus operator is proposed. The marked image obtained using this approach produces better visual quality as compared to various existing techniques. Further multilevel concept is used to hide the secret information in digital images to enhance the embedding capacity. This technique produces very high embedding capacity and better visual quality as compared to various existing techniques. In addition to this, blind data hiding technique using subsampling and interpolation is proposed. This technique produces better results as compared to various existing techniques. It can be concluded that by increasing embedding capacity, visual quality of an image is decreases. PSNR and SIM is the quality factor taken into consideration to analyze quality of marked image obtained after applying the proposed data hiding techniques.

6.2 Future scope

The future scope of this dissertation will focus on the further enhancement in embedding 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] Abadi M. A. M., Danyali H. and Helfroush M. S., "Reversible watermarking based on interpolation error histogram shifting", 5th International Symposium on Telecommunications, pp. 840-845, 2010.

[2] Alattar A. M., "Reversible watermark using the difference expansion of a generalized integer transform", IEEE Transactions on Image Processing, Vol.13, No. 8, pp. 1147–1156, 2004.

[3] Anderson R. J. and Petitcolas F. A. P., "On the limits of steganography". IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, pp 474–481, 1998.

[4] Artz D., "Digital Steganographic: hiding data within data", IEEE Internet Computing, Vol. 5, pp. 75-80, 2001.

[5] Bender W., Gruhl D., Morimoto N. and Lu A., "Techniques for data hiding", IBM System Journal Vol. 35, pp. 313–336, 1996.

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

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

[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, Vol. 6, No. 2, pp. 3100-3116, 2012.

[9] Chung K. L., Huang Y. H., Yan W. M. and Teng W. C., "Distortion reduction for histogram modification-based reversible data hiding", Applied Mathematics and Computation, Vol. 218 No. 9, pp. 5819-5826, 2012.

[10] Cox I. J., Miller M., Bloom J., Fridrich J. and Kalker T., "Digital Watermarking and

Steganography", Morgan Kaufmann Series in Multimedia Information and Systems, 2nd Ed., 2007.

[11] Fallahpour M. and Sedaaghi M.H., "High capacity lossless data hiding based on histogram modification", IEICE Electronics Express, Vol.4, No. 7,pp. 205-210,2007.

[12] Fridrich J., Goljan M., Du R., "Invertible authentication" In Proceedings of SPIE Security watermarking of multimedia contents, San Jose, pp. 197-208,2001.

[13] Fridrich J., Goljan, M. and Du, R., "Lossless data embedding—new paradigm in digital watermarking", EURASIP Journal on Advances in Signal Processing, No. 2 pp. 185-196,2002.

[14] Gonzalez R.C. and Woods R.E., "Digital Image Processing", 2nd Ed., Prentice Hall, NJ, 2002.

[15] Hong W. and Chen T. S., "Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism", Journal of Visual Communication and Image Representation, vol. 22 no. 2, pp. 131-140, 2011.

[16] Honsinger C. W., Jones P. W. Rabbani M. and Stoffel J. C., "Lossless recovery of an original image containing embedded data", US Patent, Patent No. US6278791B1, 2001.

[17] Hore, A. and Ziou D., "Image quality metric: PSNR vs. SSIM", In 20thInternationalconference on pattern recognition, pp.2366–2369, 2010.

[18] Huang H. C. and Chang F. C., "Hierarchy-based reversible data hiding", Expert Systems with Applications", Vol. 40, No. 1, pp. 34-43, 2013.

[19] Hwang J. H., Kim J. W. and Choi J.U., "A reversible watermarking based on histogram shifting", In IWDW, Lecture Notes in Computer Science, pp. 348-361. Springer Verlag, November 2006

[20] Jung K. H. and Yoo K. Y., "Data hiding method using image interpolation", Computer Standards and Interfaces, vol. 31, pp. 465-470, 2009.

[21] 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.

[22] 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 Forensic and Security, vol. 3, no. 3, pp. 456–465, 2008.

[23] Kim K. S., Lee M.J., Lee, H. Y. and Lee H. K., "Reversible data hiding exploiting spatial correlation between sub-sampled images", Pattern Recognition, Vol. 42, No. 11, pp. 3083–3096, 2009.

[24] Kuo W. C., Jiang D. J. and Huang Y. C., "A reversible data hiding scheme based on block division", In proceeding CISP, Vol. 1, pp. 365-369, 2008.

[25] Lee C.C., Wu H.C., Tsai C.S. and Chu Y.P., "Adaptive lossless steganographic scheme with centralized difference expansion", Pattern Recognization, Vol. 41 No. 6 pp. 2097–2106, 2008.

[26] Lee C.W. and Tsai W.H., "A lossless large volume data hiding method based on histogram shifting using an optimal hierarchical block division scheme", Journal of Information Science and Engineering , Vol. 27, pp.1265-1282,2007.

[27] Lee S. K., Suh Y. H. and Ho Y. S., "Reversiblee Image Authentication Based on Watermarking" In IEEE International Conference on Multimedia and Expo, pp. 1321-1324,2006.

[28] Lehmann T. M., Gonner C. and Spitzer K., "Survey : interpolation methods in medical imaging processing", IEEE Transaction on Medical Imaging, Vol. 18, No. 11, pp. 1049-1075, 1999.

[29] Li X., Li B., Yang B. and Zeng T., "General Framework to Histogram-Shifting-Based Reversible Data Hiding", IEEE Transaction on Image Processing, Vol. 22, No. 6, pp. 2181-2191, 2013.

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

[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, Vol. 181, No. 2, pp. 308-328, 2011.

[32] Luo L., Chen Z., Chen M., Zang X. and Xiong Z., "Reversible image watermarking using interpolation technique", IEEE Transactions on Information Forensics and Security, Vol. 5, No. 1, pp. 187-193,March 2010.

[33] Maeland E., "On the comparison interpolation method", IEEE Transaction on

Medical Imaging, Vol. 7, No. 3, pp. 213-217, 1988.

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

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

[36] Sencar H. T., Ramkumar M. and Akansu A. N., "Data hiding fundamentals and applications: Content security in digital multimedia", Elsevier Academic Press, July 2004.

[37] Thodi D. M. and Rodríguez J. J., "Expansion embedding techniques for reversible watermarking", IEEE Transactions on Image Processing, Vol. 16, No. 3, pp. 721-730, 2007.

[38] Tian J., "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits, Systems and Video Technology, Vol. 13, No. 8, pp. 890-896, 2003.

[39] Tsai P., Hu Y. C. and Yeh H. L., "Reversible image hiding scheme using predictive coding and histogram shifting", Signal Processing, Vol. 89, No. 6, pp.1129–43, 2009.

[40] Tseng H. W. and Chang C. C., "An extended difference expansion algorithm for reversible watermarking", Image and Vision Computing, Vol. 26, No. 8, pp. 1148-1153, 2008.

[41] Wang C. T. and Yu H. F., "High-capacity reversible data hiding based on multi-histogram modification", Multimedia Tools Appl, Vol. 61, pp. 299-319, 2012.

[42] 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, Vol. 23, pp. 569-577, 2013.

[43] Wang Z., Bovik A. C., Sheikh H. R. and Simoncelli E. P., "Image quality assessments: From error visibility to structural similarity", IEEE Transaction on Image Processing, Vol. 3, No. 4, pp. 600–612, 2004.

[44] Wang Z. H., Lee C. F. and Chang, C. Y., "Histogram-shifting-imitated reversible data hiding", Journal of Systems and Software, Vol. 86, No.2, pp. 315-323,2013.

[45] Yang C. H. T. and Chiu Y. P., "High capacity information hiding using interpolation technique", 3rd International conference on innovative computing information and

control, 2008.

[46] Zhao Z., Luo H., Lu Z. M. and Pan J. S., “Reversible data hiding based on multilevel histogram modification and sequential recovery”, AEU-International Journal of Electronics and Communications, Vol. 65 No. 10, pp. 814-826, 2011.