REVERSIBLE DATA HIDING BASED ON SLANTLET TRANSFORM/DISCRETE WAVELET TRANSFORM AND PIXEL PAIR MAPPING

A PROJECT REPORT

Submitted by

SHRIHARI.P

Register No: 13MAE14

in partial fulfillment for the requirement of award of the degree

of

MASTER OF ENGINEERING

in

APPLIED ELECTRONICS

Department of Electronics and Communication Engineering

KUMARAGURU COLLEGE OF TECHNOLOGY

(An autonomous institution affiliated to Anna University, Chennai)

COIMBATORE - 641 049

ANNA UNIVERSITY: CHENNAI 600 025

APRIL - 2015

BONAFIDE CERTIFICATE

Certified that this project report titled **"REVERSIBLE DATA HIDING BASED ON SLANTLET TRANSFORM/DISCRETE WAVELET TRANSFORM AND PIXEL PAIR MAPPING"** is the bonafide work of **SHRIHARI.P. [Reg. No. 13MAE14]** who carried out the research under my supervision. Certified further that, to the best of my knowledge the work reported herein does not form part of any other project or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE
Ms.A.Amsaveni,M.E.,(Ph.D)
PROJECT SUPERVISOR
Department of ECE,
Kumaraguru College of Technology,
COIMBATORE - 641049

SIGNATURE
Dr. Rajeswari Mariappan,Ph.D
HEAD OF THE DEPARTMENT
Department of ECE,
Kumaraguru College of Technology,
COIMBATORE - 641049

The candidate with university **Register No.13MAE14** is examined by us in the project viva-voce examination held on ----------

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

First, I would like to express my praise and gratitude to the Lord, who has showered his grace and blessings enabling me to complete this project in an excellent manner.

I express my sincere thanks to the management of Kumaraguru College of Technology and Joint Correspondent **Shri. Shankar Vanavarayar** for the kind support and for providing necessary facilities to carry out the work.

I would like to express my sincere thanks to our beloved Principal **Dr.R.S.Kumar Ph.D.,** Kumaraguru College of Technology, who encouraged me in each and every steps of the project.

I would like to thank **Dr.Rajeswari Mariappan Ph.D.,** Head of the Department, Electronics and Communication Engineering, for her kind support and for providing necessary facilities to carry out the project work.

In particular, I wish to thank with everlasting gratitude to the project coordinator **Ms.S.Sasikala M.E.,** Associate Professor, Department of Electronics and Communication Engineering ,for her expert counseling and guidance to make this project to a great deal of success.

I am greatly privileged to express my heartfelt thanks to my project guide **Ms.A.Amsaveni M.E.,** Associate Professor, Department of Electronics and Communication Engineering, throughout the course of this project work and i wish to convey my deep sense of gratitude to all teaching and non-teaching staffs of ECE Department for their help and cooperation.

Finally, I thank my parents and my family members for giving me the moral support and abundant blessings in all of my activities and my dear friends who helped me to endure my difficult times with their unfailing support and warm wishes.

ABSTRACT

Reversible data hiding is a technique used in the field of information security .Using this technique a secret data can be embedded inside a cover medium by the sender and the receiver can extract the secret data and cover medium without any distortion. The main benefit of this technique is that the cover medium used for embedding can also be recovered with high quality. Reversible data hiding has a wide range of applications such as medical image sharing, multimedia archive management, image transcoding, video error concealment and military application. This project proposes a novel robust reversible data hiding scheme based on Slantlet/Discrete wavelet transform and Pixel pair mapping. The Slantlet Transform matrix transforms small blocks of the original image and pixel pair mapping technique is used to embed data in each block. The pixel pair mapping concept is used to select the pixel randomly to embed the data in the image. The main objective of the task is to enhance robustness, imperceptibility and increased capacity. The original image can also be recovered from stego image after the hidden data is extracted from it. Similarly the data hiding technique was also done based on Discrete Wavelet Transform and finally PSNR, SSIM and BER values are compared.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

RDH	Reversible Data Hiding
MD5	Message-Digest algorithm 5
JPEG	Joint Picture Expert Group
LSB	Least Significant Bit
PSNR	Peak Signal To Noise Ratio
BER	Bit Error Rate
SSIM	Structural Similarity Index Measure
HS	Histogram
DCT	Discrete Cosine Transform
DE	Difference Expansion
SLT	Slantlet Transform
DWT	Discrete Wavelet Transform
CWT	Continuous Wavelet Transform
CDF	Cumulative Distribution Function
AES	Advanced Encryption Standard
MPEG	Moving Picture Experts Group
SDEM	Scramble Data Embedding in Mid-frequency range

CHAPTER 1
INTRODUCTION

In an information sharing environment, security of information plays an important role. Some information that is sensitive or confidential in nature must be kept private. With the introduction of computers, the need for automated tools for protecting files and other information stored in the computer become evident. Transmission of sensitive information via an open internet channel increases the risk of interception. There are many techniques proposed to deal with this issue. They are

1) Cryptography
2) Steganography
3) Watermarking
4) Reversible data hiding

1.1 CRYPTOGRAPHY

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries. This technique alters the form of the message at the sender and transmits it. At the receiver the original message is extracted. It mainly involves 2 operations

Encryption: It is the process of the conversion of information from a readable state to apparent nonsense with the usage of a key. It is done by the sender.

Decryption: It is the reverse process of encryption. That is, it is the process of converting scrambled message into the original one with the help of key. The key may be similar to the one which is used in encryption or it may be a different one. It is done at the receiver side.

The cryptography is characterized by 3 independent dimensions

1) The type of operations used for transforming plaintext to cipher text

All encryption algorithms are based on two general principles. They are substitution and transposition. Substitution is the one in which each element in the plain text is transformed into another element. Transposition is the one in which elements in the plain text are rearranged. The fundamental condition is that no information be lost.

2) The number of keys used

Based on this we can classify the techniques into two.

a) Symmetric-key cryptography: Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way).

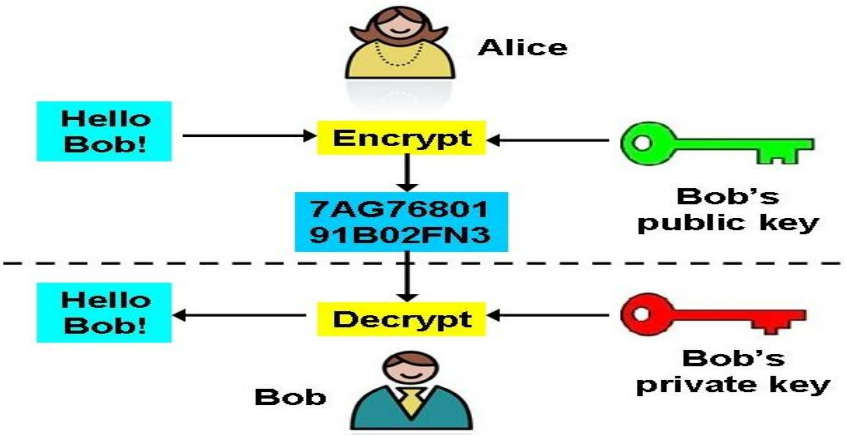


Fig 1.1 Symmetric-key cryptography

b) Public key cryptography: In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. In a public-key encryption system, the public key is used for encryption, while the private or secret key is used for decryption

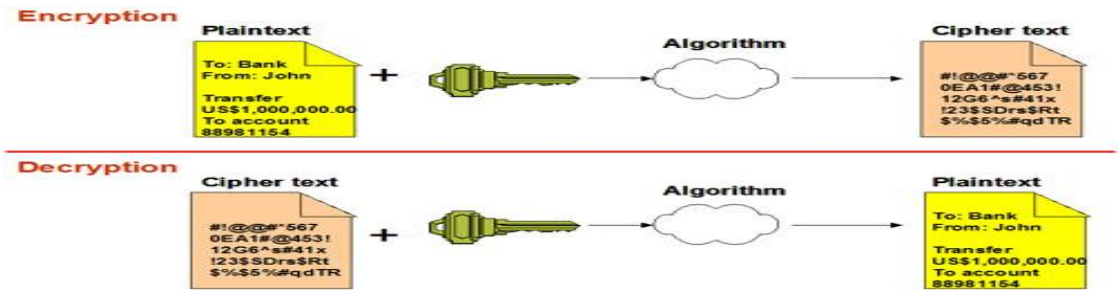


Fig 1.2 Public key cryptography

3) The way in which the plaintext is processed

There are 2 types

a) Block cipher: It processes the input one block of elements at a time, producing an output block for each input block

b) Stream cipher: It processes the input elements continuously, producing output one element at a time**,** as it goes along.

1.2 STEGANOGRAPHY

It is the art and science of encoding hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is a form of security through obscurity. Generally, the hidden messages will appear to be (or be part of) something else: images, articles, shopping lists or some other cover texts. Plainly visible encrypted messages no matter how unbreakable will arouse interest, and may in themselves be incriminating in countries where encryption is illegal. For example, the hidden message may be in invisible ink between the visible lines of a private letter. The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. So cryptography is the practice of protecting the contents of a message alone, steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size.

1.3 DIGITAL WATERMARKING

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity

of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Like traditional watermarks digital watermarks are only perceptible under certain conditions, i.e. after using some algorithm, and imperceptible anytime else. If a digital watermark distorts the carrier signal in a way that it becomes perceivable, it is of no use. Traditional Watermarks may be applied to visible media (like images or video), whereas in digital watermarking, the signal may be audio, pictures, video, texts or 3D models. A signal may carry several different watermarks at the same time. Unlike metadata that is added to the carrier signal, a digital watermark does not change the size of the carrier signal.

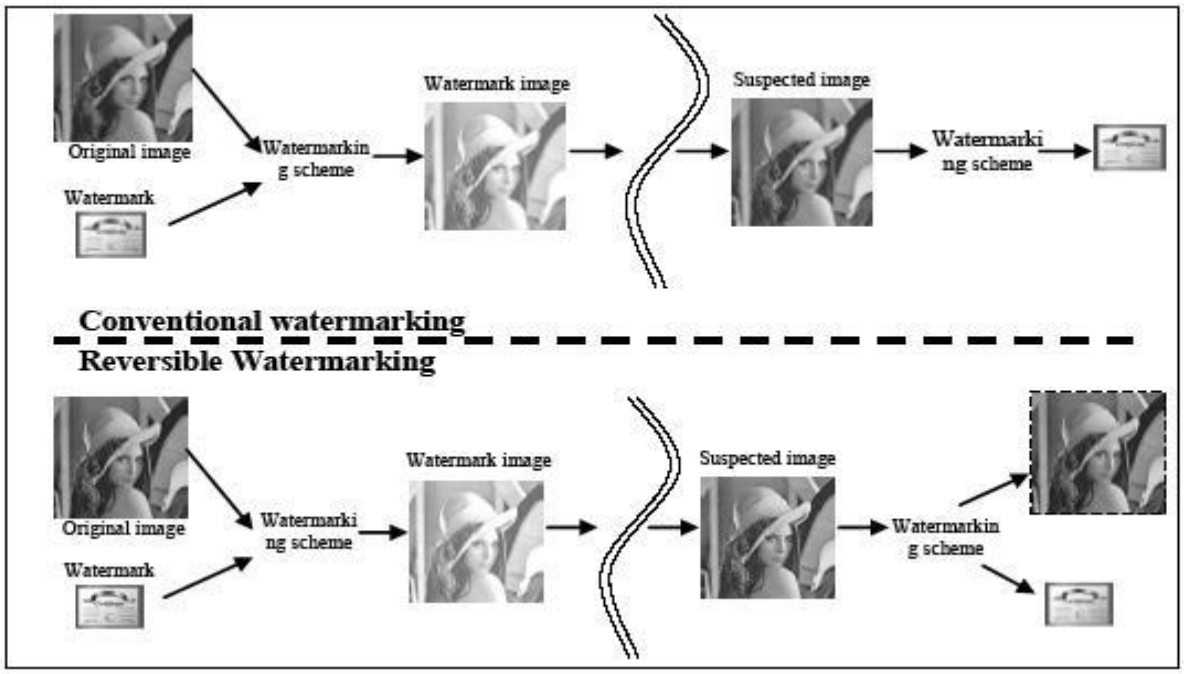


Fig 1.3 Digital watermarking

The needed properties of a digital watermark depend on the case in which it is applied. For marking media files with copyright information, a digital watermark has to be rather robust against modifications that can be applied to the carrier signal. Instead, if integrity has to be ensured, a fragile watermark would be applied. Both steganography and digital watermarking employ steganographic techniques to embed data covertly in noisy signals. But whereas steganography aims for imperceptibility to human senses,

digital watermarking tries to control the robustness as top priority. Since a digital copy of data is the same as the original, digital watermarking is a passive protection tool. It just marks data, but does not degrade it nor controls access to the data.

One application of digital watermarking is source tracking. A watermark is embedded into a digital signal at each point of distribution. If a copy of the work is found later, then the watermark may be retrieved from the copy and the source of the distribution is known. This technique reportedly has been used to detect the source of illegally copied movies.

1.4 REVERSIBLE DATA HIDING

The scheme is also known as lossless data embedding. Here the secret data can be embedded inside a cover image at the transmitter side and the hidden data as well as the cover image can be extracted without any degradation at the receiver side. The main characteristics of reversible data hiding scheme are

- Capacity: It refers to the amount of information that can be hidden in the cover medium
- Security: It refers the inability of the hacker to extract hidden information.
- Perceptibility: It means the inability to detect the hidden information.
- Robustness: It is the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.

1.5 DIFFERENT RDH TECHNIQUES

Reversible data hiding has been performed in three different domains. They are spatial domain, frequency domain, and compression domain. Spatial domain schemes directly change the pixel values to embed the data. Most spatial domain techniques are developed based on two principles, i.e., difference expansion and histogram shifting. Frequency domain involves calculation of coefficients of image using some transformation such as discrete wavelet transform, discrete cosine transform, slantlet transform, curvelet transform, etc.., Then the frequency coefficients are modified to embed the data. Compression domain schemes compress the image using compression

algorithm such as vector quantization, MPEG coding. According to the algorithm image is encoded to conceal the data.

1.5.1. LOSSLESS COMPRESSION

Space to hide data is found by compressing proper bit-plane that offers minimum redundancy to hold the hash (authentication information). Lowest bit-plane offering lossless compression can be used unless the image is not noisy. In completely noisy image some bit-planes exhibit strong correlation. These bit-planes can be used to find enough room to store the hash. Hash length is generally 128 bit using MD5 algorithm. The algorithm starts lossless compression from 5th bit-plane and calculates redundancy by subtracting compressed data size from number of pixels.

During embedding the algorithm first calculates the hash of the original image, finds the proper bit plane, and adds the hash with the compressed bit-plane data. Then it replaces selected bit-plane by concatenated data. For more security the concatenated hash with compressed data is encrypted using symmetric key encryption based on 2-dimensional chaotic maps. This algorithm takes variable sized blocks and gives the encrypted message as long as the original message, so no padding is needed. Other public or symmetric key algorithms can be used, but they require padding to embed the encrypted message and hence increase distortion. During decoding after key bit-plane selection the data is decrypted and hash is separated from the compressed original bit-plane data. The bit-plane is replaced by the decompressed data; hence the exact copy of the original image is found. The hash of the reconstructed image is calculated and compared with the extracted hash; if both are same the image in question is authentic.

Advantages

(i) High capacity

(ii) Security is equivalent to the security provided by cryptographic authentication

(iii) Can be applied for the authentication purposes of JPEG files, complex multimedia objects, audio files, digitized hologram, etc.

Disadvantages

(i) Noisy image forces the algorithm to embed information in higher bit-plane when the distortions are higher and easily visible

(ii) Single bit-plane in a small image does not offer enough space to hide hash after compression, so two or more bit-planes are required and the artifacts must be visible

(iii) Capacity is not high enough to embed large payload.

1.5.2. INTEGER TRANSFORM TECHNIQUE

In this scheme, an integer transform is used to embed 1-bit watermark into one pixel pair in a way that the sum of the pixel pair remains unchanged. Based on the invariability of sum values and the equality between the parities of sum values and difference values, the extraction of watermarks and the recovery of pixel pairs can be easily achieved.

Shaowei Weng *et al.* proposed an integer transform in which the forward transform is defined as

$$x' = x + d/2 + b \quad (1.1)$$

$$y' = y - d/2 - b \quad (1.2)$$

where b is used to denote one bit watermark, and d is the difference between the pixels x and y. Actually, x + y equals x' + y'. x + y and d have the same parity. x' and y' are the watermarked image pixels corresponding to x and y. On the decoding side, the sum of x' and y' is calculated first. Therefore x + y are determined. The difference value of x' and y' is calculated and denoted as d'. The actual difference d can be calculated as

$$d = (d' + LSB(d'))/2 - b \quad (1.3)$$

The value of d and the watermark bit b can be uniquely deduced because the parity of d is known and b is a binary number. For example, if x = 7, y = 5 and b = 0, then x' = 8, y'=4 after embedding. On the receiver side, (d' +LSB (d'))/2 is calculated as 2. The parity of d can be guaranteed to be the same as d'. The parity of d' is odd parity. The parity of d is odd if and only if b = 0. As a result, watermark bit b is correctly extracted and the value of d is obtained.

Once d and x + y are obtained then the original pixel values x and y are calculated as

$$x = (x + y + d)/2 \quad (1.4)$$

$$y = (x + y – d)/2 \quad (1.5)$$

Advantages

(i) High capacity

(ii) Use of secret key during embedding increases security. The

Disadvantages

(i) Often multiple bit-planes are required to have enough space when the artifacts become visible

(ii) Gray scale mapping

1.5.3. DIFFERENCE EXPANSION TECHNIQUE

Tian proposes a high quality reversible watermarking method with high capacity based on difference expansion. Pixel differences are used to embed data; this is because of high redundancies among the neighboring pixel values in natural images.

Embedding

(i) Differences of neighboring pixel values are calculated

(ii) Changeable bits in that differences are determined

(iii) Some differences are chosen to be expandable by 1-bit, so changeable bits increases

(iv) Concatenated bit-stream of compressed original changeable bits, the location of expanded difference numbers (location map), and the hash of original image (payload) is embedded into the changeable bits of difference numbers in a pseudorandom order

(v) Use the inverse transform to have the watermarked pixels from resultant differences.

Extraction

(i) Differences of neighboring pixel values are calculated

(ii) Changeable bits in that differences are determined

(iii) Extract the changeable bit-stream ordered by the same pseudo random order as embedding

(iv) Separate the compressed original changeable bit-stream, the compressed bit-stream of locations of expanded difference numbers (location map), and the hash of original image (payload) from extracted bit-stream

(v) Decompress the compressed separated bit-streams and reconstruct the original image replacing the changeable bits

(vi) Calculate the hash of reconstructed image and compare with extracted hash.

Advantages

(i) No loss of data due to compression-decompression

(ii) Also applicable to audio and video data

(iii) Encryption of compressed location map and changeable bit-stream of different numbers increases the security.

Disadvantages

(i) There may be some round off errors (division by 2), though very little

(ii) Largely depends on the smoothness of natural image; so cannot be applied to textured image where the capacity will be zero or very low

(iii) There is significant degradation of visual quality due to bit-replacements of gray scale pixels

1.5.4. HISTOGRAM MODIFICATION TECHNIQUE

Ni et al. utilizes zero or minimum point of histogram. If the peak is lower than the zero or minimum point in the histogram, it increases pixel values by one from higher than the peak to lower than the zero or minimum point in the histogram. While embedding, the whole image is searched. Once a peak-pixel value is encountered, if the bit to be embedded is '1' the pixel is added by 1, else it is kept intact. Alternatively, if the peak is higher than the zero or minimum point in the histogram, the algorithm decreases pixel values by one from lower than the peak to higher than the zero or minimum point in the

histogram, and to embed bit '1' the encountered peak-pixel value is subtracted by 1.The decoding process is quiet simple and opposite of the embedding process.

Advantages

(i) It is simple

(ii) It always offers a constant PSNR 48.0dB

(iii) Distortions are quite invisible

(iv) Capacity is high

Disadvantages

(i) Capacity is limited by the frequency of peak-pixel value in the histogram

(ii) It searches the image several times, so the algorithm is time consuming.

1.5.5 INTERPOLATION TECHNIQUE

In this technique, the difference between interpolation value and corresponding pixel value is used to embed bit "1" or "0" by expanding it additively or leaving it unchanged. It is different from most differential expansion approaches in two important aspects:

1) It uses interpolation-error; instead of inter pixel difference or prediction- error, to embed data.

2) It expands difference, which is interpolation-error here, by addition instead of bit-shifting.

First, interpolation values of pixels are calculated using interpolation technique, which works by guessing a pixel value from its surrounding pixels. Then interpolation-errors are obtained by

$$e = x - x' \tag{1.14}$$

Where x' are the interpolation values of pixels x.

The secret bit b is embedded by additively expanding the interpolation error values. The additive interpolation-error expansion is formulated as

$$e' = \begin{cases} e + sign(e) \times b, & e = LM \text{ or } RM \\ e + sign(e) \times 1, & e \in (LN,LM) \cup (RM,RN) \\ e, & \text{otherwise} \end{cases} \tag{1.15}$$

Where LM and RM denote the corresponding values of the two highest points of interpolation errors histogram and LN and RN denote the corresponding values of the two lowest points of interpolation-errors histogram. The watermarked pixels x'' becomes

$$x'' = x' + e' \tag{1.16}$$

During the extracting process, the interpolation value x' is computed with the same interpolation algorithm and the corresponding interpolation-errors are obtained. Once the interpolation errors, LM, RM, LN and RN are known, the embedded secret data can be extracted. Then the inverse function of additive interpolation-error expansion is applied to recover the original interpolation-errors. Finally, we can restore the original pixels x by adding interpolation value x'and the interpolation error e.

After secret messages are embedded, some overhead information is needed to extract the covert information and restore the original image. The overhead information is the information to identify those pixels containing embedded bit (LM, LN, RM and RN) and the information to solve the overflow/underflow problem.

CHAPTER 2

LITERATURE SURVEY

1) Rasha Thabit, Bee Ee Khoo "Robust reversible watermarking scheme using Slantlet transform matrix" The Journal of Systems and Software (2013).

This paper presents a novel robust reversible watermarking scheme based on using the Slantlet transform matrix to transform small blocks of the original image and hiding the watermark bits by modifying the mean values of the carrier sub bands. The problem of overflow/underflow has been avoided by using histogram modification process. The proposed scheme has robustness against different kinds of attacks and the results prove that it is completely reversible with improved capacity, robustness, and invisibility in comparison with the previous methods.

By applying the SLT using matrix multiplication a small block from Lena image (size16 × 16) has been cut and this block is transformed using the SLT matrix (size 16 × 16). Then the inverse SLT transform is applied to recover the original block. The error between the original block and the recovered block is very small, but this error is not acceptable in the reversible methods. To make the recovered block exactly as the original block we rounded the values of the recovered block to their integer values and thus the error between the original block and the recovered block becomes zero. In order to avoid the problem of overflow and/or underflow, the histogram modification process will be applied. Histogram modification process is that to increase the visual quality of the watermarked image and to apply the pixel adjustment only when it is required. The purpose of the proposed method is to ensure the reversibility and to improve the robustness, capacity, and invisibility.

Advantages

(i) Robustness is high.

(ii) Data hiding has higher capacity.

(iii) Better image quality.

2) Sushil Kumar, S.K. Muttoo "Distortionless Data Hiding based on Slantlet Transform" International Conference on Multimedia Information Networking and Security (2009).

This paper presents a distortionless data hiding technique based on wavelet-like transform, known as Slantlet Transform (SLT). The proposed algorithm first encodes the original message using the encoder, T-codes. T-codes have shown to be more robust than the best known variable-length codes, Huffman codes. T-codes have a well explained resynchronization mechanism which leads to fast and reliable resynchronization. The secret data is then embedded in the high frequency sub-bands, viz., HH, HL and LH which are obtained by applying Slantlet transform to the cover-image. We use two steganography algorithms, viz., LSB algorithm and thresholding algorithm for embedding data in the image. We show further that the original image can also be recovered from stego-image after the hidden data is extracted from it. It is known that SLT is a better candidate for signal compression compared to the DWT based scheme and it can provide better time localization. The proposed algorithm yields better imperceptibility for the stego-images than the conventional DWT based scheme in case of low embedding rate and yields acceptable results for high embedding rate as well.

Advantages

(i) There is no artifact in the stego-image, the original image can be distortionlessly recovered from the stego-image after the hidden data has been been extracted.

(ii) Better image quality when compared to wavelet (CDF) transforms.

3) Ivan W. Selesnick, The Slantlet Transform, IEEE transactions on signal processing, vol. 47, no. 5, may 1999.

The discrete wavelet transform (DWT) is usually carried out by filter bank iteration; however, for a fixed number of zero moments, this does not yield a discrete time basis that is optimal with respect to time localization. This paper discusses the implementation and properties of an orthogonal DWT, with two zero moments and with improved time localization. The basis is not based on filter bank iteration; instead, different filters are used for each scale. For coarse scales, the support of the discrete-time basis functions approaches two thirds that of the corresponding functions obtained by filter bank iteration. It retains the octave-band characteristic and is piecewise linear (but discontinuous).

The smoothing of data while preserving edges relatively well is an essential advantage of wavelets in denoising, and it depends in part on both the short support of the basis functions with respect to their scale and their number of vanishing moments. In addition, in the application of wavelet bases to image compression, the time localization and the number of zero moments of the basis are both important. Good time localization properties lead to good representation of edges. Approximation order is important for sparse representation (compression) of smooth regions. However, short support and zero moments are competing criteria in the construction of wavelet filter banks.

Although not based on an iterated filterbank tree, the filterbank described in this paper retains the main desirable characteristics of the usual DWT filterbank, namely, orthogonality, an octave-band characteristic, a scale-dilation factor of 2, and an efficient implementation. A transform for finite length signals based on this filterbank is particularly clean due to the filter lengths being exact powers of two. The basis appears particularly well suited for piecewise linear signals, as does the Haar basis for piecewise constant signals.

4) S. Kurshid Jinna, Dr. L. Ganesan, Reversible Image Watermarking using Bit Plane Coding and Lifting Wavelet Transform, IJCSNS International Journal of Computer Science and Network Security, vol. 9 no.11, November 2009.

This paper proposes a distortionless image data hiding algorithm based on integer wavelet transform that can hide data into the original image .The data can be retrieved and the original image can be recovered without any distortion after the hidden data are extracted. This algorithm hides data into one or more middle bit-plane(s) of the integer wavelet transform coefficients in the LH, HL and HH frequency sub bands. It can embed more data into the bit planes and also has the necessary imperceptibility requirement. The image histogram modification may be used to prevent grayscales from possible overflow or underflow.

The original image is preprocessed by performing lifting scheme. Now integer to integer wavelet transform is performed to decompose the image into its components namely, Approximate coefficients, horizontal, vertical coefficients and diagonal coefficients. We use the horizontal vertical as well as the diagonal detailed bands to embed the watermark. We chose a bit plane of the detailed bands. The original bits in the selected plane are compressed losslessely to create space for embedding the payload bits. The compression exploits the fact that '0'sand '1's are nonuniformly distributed as we move from least significant bit plane to higher ones. After compression necessary headers are generated reflecting the original bit distribution in the chosen plane of the quadrants.

Advantages

(i) Arithmetic coding used for compression guarantees complete reversibility

5) Mamata J, Poornima G, Comparative Analysis of Embedding Data in Image using DCT and DWT Techniques, International Journal of Science and Research

This paper deals with hiding credit card numbers in an image file (bank logo) using, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based Steganography. It is a novel Lossless Secure data embedding algorithm in which the vital information can be embedded into the cover image while preserving the quality of cover image and maintaining the security of the data. The security of the data embedded and cover image quality are two main issues that need to be considered during the process of the data embedding. SDEM-DCT and SDEM-DWT (Scramble Data Embedding in Mid-frequency range of DCT and DWT) Algorithm consists of three major security levels that can be used to hide Credit Card Numbers of customers inside the bank LOGO.

The paper proposes a high capacity data hiding method is used to embed the Credit card numbers into the images but it cannot be done in a direct manner. To have a more Security levels for data embedding a robust Scramble and Descramble Data embedding algorithm is introduced which consist of MK randomize key Generator. In this method, three levels of security are used, first in Scrambling original data, second Exclusive OR the Scramble original data with Generated keys by M-K randomize key generator and third the place of DCT coefficients to embedding. In DWT Based Steganography, coefficients in the low frequency sub-band could be preserved unaltered for improving the image quality. This is because of different characteristics of DWT coefficients in different sub-bands. Since the most essential portion (the low frequency part) remain unchanged, when the secret messages are embedded in the high frequency sub-bands corresponding to the edges portion of the original image, PSNR will be being recommended. The proposed Method is very practical for most transferable Banks transactions on the internet.

6) Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang , Reversible Data Hiding in Encrypted JPEG Bitstream, IEEE transactions on multimedia, vol. 16, no. 5, August 2014.

This paper proposes a framework of reversible data hiding (RDH) in an encrypted JPEG bit stream. Unlike existing RDH methods for encrypted spatial-domain images, the proposed method aims at encrypting a JPEG bit stream into a properly organized structure, and embedding a secret message into the encrypted bit stream by slightly modifying the JPEG stream. We identify usable bits suitable for data hiding so that the encrypted bit stream carrying secret data can be correctly decoded. The secret message bits are encoded with error correction codes to achieve a perfect data extraction and image recovery. The encryption and embedding are controlled by encryption and embedding keys respectively. If a receiver has both keys, the secret bits can be extracted by analyzing the blocking artifacts of the neighboring blocks, and the original bit stream perfectly recovered. In case the receiver only has the encryption key, he/she can still decode the bit stream to obtain the image with good quality without extracting the hidden data.

The general framework of the proposed scheme is content owner, data hider, and receiver. The original JPEG bit stream is properly encrypted to hide the image content with the bit stream structure preserved. The secret message bits are encoded with error correction codes (ECC) and embedded into the encrypted bit stream by modifying the appended bits corresponding to the AC coefficients. By using the encryption and embedding keys, the receiver can extract the embedded data and perfectly restore the original image. When the embedding key is absent, the original image can be approximately recovered with satisfactory quality without extracting the hidden data. The proposed framework is also applicable to JPEG-LS and JPEG 2000 with slight modification of the encryption and embedding schemes according to the respective coding-decoding algorithms.

7) Pallavi Patil, D.S Bormane, DWT Based Invisible Watermarking Technique for Digital Images, International Journal of Engineering and Advanced Technology (IJEAT), Volume-2, Issue-4, April 2013

A lossless data hiding scheme is presented based on quantized coefficients of discrete wavelet transform (DWT) in the frequency domain to embed secret message. Using the quantized DWT based method; This method embed secret data into the successive zero coefficients of the medium-high frequency components in each reconstructed block for 3-level 2-D DWT of cover image. The procedures of the proposed system mainly include embedding & extracting. The original image can be recovered losslessly when the secret data had been extracted from stego-image.

The proposed method embeds secret message into DWT coefficients in medium high frequency components and restores the original image coefficients after the secret messages have been extracted. Wavelet transform is used to converts an image from time or spatial domain to frequency domain. Decomposition of digital image will be pair of waveform with high frequency corresponds to detailed parts of an image & low frequency to smooth parts of image. The digital message will be embedding in medium-high frequency components & the image will be reconstructed to get cover image with digital message hidden. Embedded image decomposed into inverse discrete wavelet transform. Inverse wavelet transform is used to convert frequency domain to spatial domain. Hence it is frequency-time representation. Embedded image will be extracted in to sub-band frequencies using dwt method. The digital data will be taken from the medium high frequency components & the extracted digital data will be compared with original message.

8) Weiming Zhang , KedeMa, NenghaiYu, Reversibility improved data hiding in encrypted images, School of Information Science and Technology

A novel reversible data hiding technique in encrypted images is presented in this paper. Instead of embedding data in encrypted images directly, some pixels are estimated before encryption so that additional data can be embedded in the estimating errors. A bench mark encryption algorithm (e.g. AES) is applied to the rest pixels of the image and a special encryption scheme is designed to encrypt the estimating errors. Without the encryption key, one cannot get access to the original image. However, provided with the data hiding key only, he can embed in or extract from the encrypted image additional data without knowledge about the original image. Moreover, the data extraction and image recovery are free of errors for all images. Experiments demonstrate the feasibility and efficiency of the proposed method, especially in aspect of embedding rate versus Peak Signal-to-Noise Ratio (PSNR).

The paper proposes a novel method to significantly improve the performance by reversing the order of encryption and vacating room. In the light of this idea, we empty out room prior to image encryption by shifting the histogram of estimating errors of some pixels and the emptied out room will be used for data hiding. The proposed method is composed of four primary steps: vacating room and encrypting image, data hiding in the encrypted image, data extraction and image recovery. Two different schemes, extraction before decryption and decryption before extraction, are raised to cope with different applications.

Advantages

(i) Achieves excellent performance in three aspects: complete reversibility, PSNR under given embedding rate, separability between data higher extraction and image decryption.

CHAPTER 3

PROPOSED METHODOLOGY

The proposed data hiding scheme aims at the security of the hidden data and also more embedding capacity of data into the cover image. Here the cover image is transformed from temporal domain to frequency domain by using slantlet transform. The data to be embedded is converted into ASCII code and is embedded into slantlet coefficients using pixel pair mapping method. After embedding the data the inverse slantlet transform is applied, the hidden data can be extracted from the cover image accurately with the help of location map and the cover image can also be extracted.

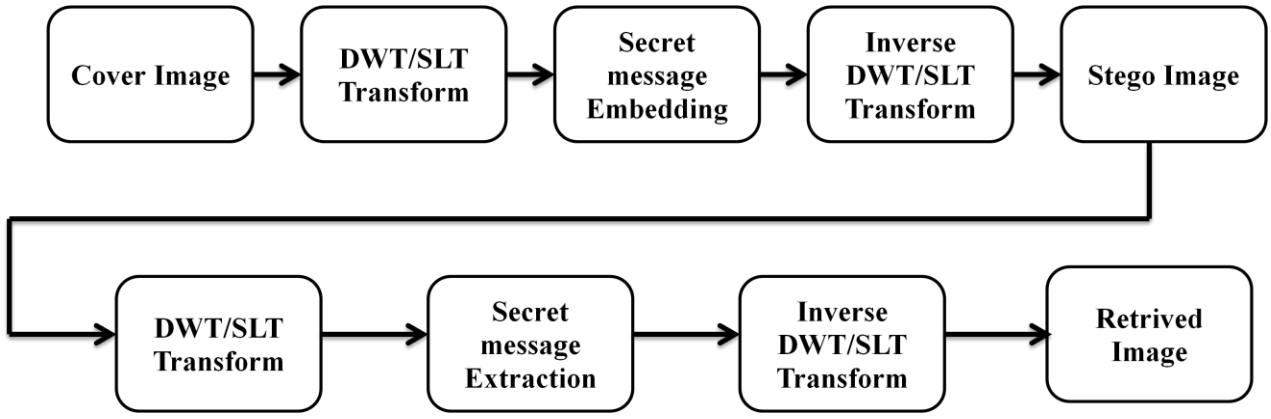


Fig 3.1 Work Flow Diagram

3.1 DISCRETE WAVELET TRANSFORM

Wavelet domain techniques are becoming very popular because of the developments in the wavelet stream in the recent years. Wavelet transform is used to transform the image into frequency domain. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis. A continuous wavelet transform (CWT) is used to divide a continuous-time function into wavelets and it is written as

$$\gamma(s,\tau) = \int f(t)\psi^{*}_{s,\tau} tdt \qquad (3.1)$$

Where * denotes complex conjugation. This equation shows how a function f(t) is

decomposed into a set of basis functions $\psi^t\, s, \tau$ called the wavelets. The variables s and τ, scale and translation, are the new dimensions after the wavelet transform. The wavelets are generated from a single basic wavelet ψ^t the so-called mother wavelet, by scaling and translation

$$\psi_{s,\tau}(t) = \frac{1}{\sqrt{s}}\psi(\frac{t-\tau}{s}) \tag{3.2}$$

As CWT maps a one-dimensional signal to a two-dimensional time-scale joint representation that is highly redundant. The time-bandwidth product of the CWT is the square of the signal and for most applications, which seek a signal description with as few components as possible, this is not efficient. To overcome this problem discrete wavelets have been introduced. Discrete wavelets are not continuously scalable and translatable but can only be scaled and translated in discrete steps. This is achieved by modifying the wavelet representation in equation (3.2)

$$\psi_{j,k}(t) = \frac{1}{\sqrt{s_0^j}}\psi(\frac{t-k\tau_0 s_0^j}{s_0^j}) \tag{3.3}$$

Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. A one dimensional DWT is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter. The result of latter convolution is smoothed version of the input, while the high frequency part is captured by the first convolution. The reconstruction involves a convolution with the synthesis filter and the results of this convolution are added. In two dimensional transform, first apply one step of the one dimensional transform to all rows and then repeat to all columns. This decomposition results into four classes or band coefficients. The Haar Wavelet Transform is the simplest of all wavelet transform. In this the low frequency wavelet coefficient are generated by averaging the two pixel values and high frequency coefficients are generated by taking half of the difference of the same two pixels. The four bands obtained are approximate band (LL), Vertical Band (LH), Horizontal band (HL), and diagonal detail band (HH). The approximation band consists of low frequency

wavelet coefficients, which contain significant part of the spatial domain image. The other bands also called as detail bands consists of high frequency coefficients, which contain the edge details of the spatial domain image. This DWT decomposition of the signal continues until the desired scale is achieved .Two-dimensional signals, such as images, are transformed using the two-dimensional DWT. The two-dimensional DWT operates in a similar manner, with only slight variations from the one-dimensional transform. Given a two-dimensional array of samples, the rows of the array are processed first with only one level of decomposition. This essentially divides the array into two vertical halves, with the first half storing the average coefficients, while the second vertical half stores the detail coefficients. This process is repeated again with the columns, resulting in four sub bands within the array defined by filter output. Fig 3.1.1 shows a one level decomposition using the two-dimensional DWT. Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective.

In the figure 3.2 LPF1 Represents low-pass filtering of the image rows, HPF1 represents high pass filtering of Image rows, LPF2 represents low-pass filtering of image columns, and HPF2 represents high-pass filtering of image columns.

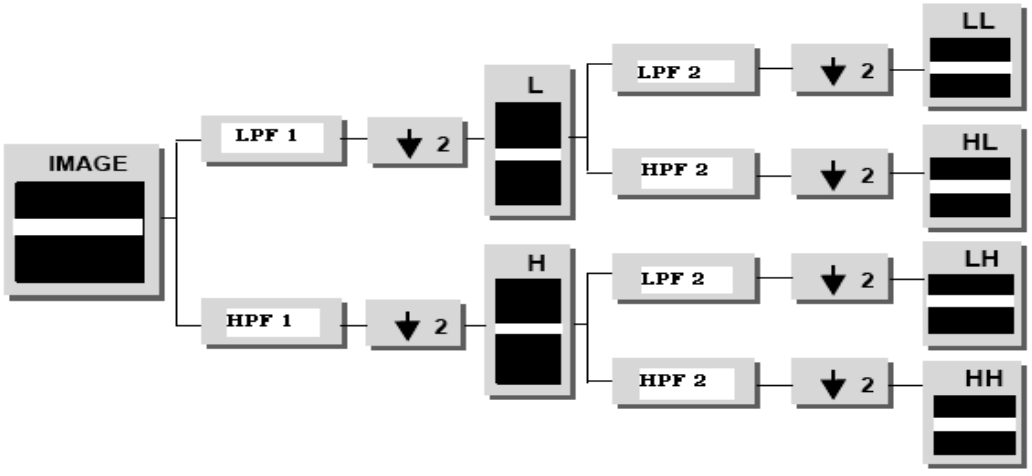
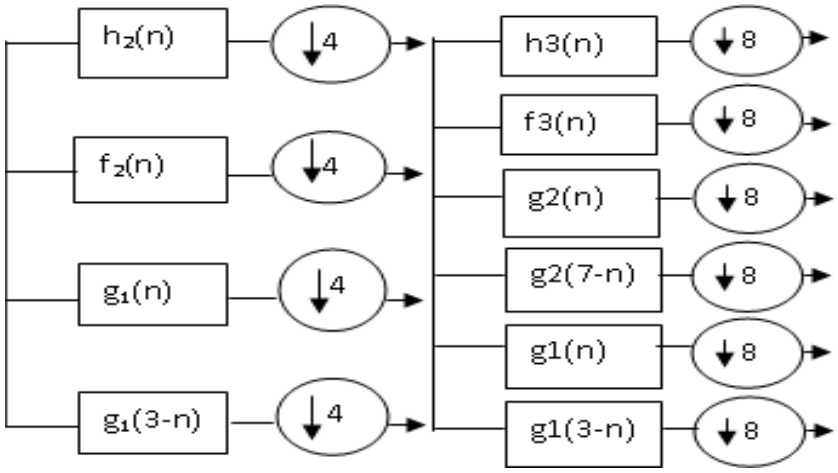


Fig 3.2 One-level decomposition using the two-dimensional DWT.

3.2 SLANTLET TRANSFORM

Slantlet transform (SLT) is an equivalent form of the DWT implementation but provides better time-localization due to the shorter supports of component filters. The SLT filters are essentially piecewise linear filters, have desirable properties of orthogonality and two vanishing moments, have an octave-band characteristic, can exactly provide a scale dilation factor of 2, provides a multi-resolution decomposition. The SLT filter bank can be implemented using a parallel structure with different filters for each scale instead of the iteration of filters for each level. The structures of the SLT filter bank for 2-scale and 3-scale are given.



(a) (b)

Fig. 3.3 (a) 2-scale SLT filter bank (b) 3-scale SLT filter bank

The filters used to construct the Slantlet matrix are $g_i(n)$, $f_i(n)$ and $h_i(n)$. The L scale filter bank has 2L channels.

$$g_i(n) = \begin{cases} a_{0,0} + a_{0,1}n & \text{for} \quad n = 0,...2^i - 1 \\ a_{1,0} + a_{1,1}(n - 2^i) & \text{for} \quad n = 2^i,...2^{i+1} - 1 \end{cases} \tag{3.4}$$

Where the parameters of the filters are obtained as,

$$a_{0,0} = \frac{s_0 + t_0}{2} \tag{3.5}$$

$$a_{1,0} = \frac{s_0 - t_0}{2} \tag{3.6}$$

$$a_{0,1} = \frac{s_1 + t_1}{2} \tag{3.7}$$

$$a_{1,1} = \frac{s_1 - t_1}{2} \tag{3.8}$$

$$s_0 = -s_1 \cdot \left(\frac{m-1}{2} \right) \tag{3.9}$$

$$t_0 = \frac{(m+1)s_1}{3 - mt_1} \; \frac{m-1}{2m} \tag{3.10}$$

$$s_1 = 6\sqrt{\frac{m}{(m^2-1)(4m^2-1)}} \tag{3.11}$$

$$t_1 = 2\sqrt{\frac{3}{m(m^2-1)}} \tag{3.12}$$

$$m = 2^i \tag{3.13}$$

The filters $h_i(n)$ and $f_i(n)$ are obtained as follows

$$h_i(n) = \begin{cases} b_{0,0} + b_{0,1}n & \text{for} \quad n = 0,...2^i - 1 \\ b_{1,0} + b_{1,1}(n - 2^i) & \text{for} \quad n = 2^i,...2^{i+1} - 1 \end{cases} \tag{3.14}$$

$$f_i(n) = \begin{cases} c_{0,0} + c_{0,1}n & \text{for} \quad n = 0,..2^i - 1 \\ c_{1,0} + c_{1,1}(n - 2^i) & \text{for} \quad n = 2^i,..2^{i+1} - 1 \end{cases} \tag{3.15}$$

Where the parameters b and c are obtained as follows,

$$b_{0,0} = u \cdot \frac{v+1}{2m} \tag{3.16}$$

$$b_{0,1} = \frac{u}{m} \tag{3.17}$$

$$b_{1,0} = u - b_{0,0} \tag{3.18}$$

$$b_{1,1} = -b_{0,1} \tag{3.19}$$

$$c_{0,1} = q \cdot (v - m) \tag{3.20}$$

$$c_{1,1} = -q \cdot (v + m) \tag{3.21}$$

$$c_{1,0} = c_{1,1} \cdot \frac{v + 1 - 2m}{2} \tag{3.22}$$

$$c_{1,1} = c_{0,1} \cdot \frac{v + 1}{2} \tag{3.23}$$

Where u, v and q are given by

$$u = \frac{1}{\sqrt{m}} \tag{3.24}$$

$$v = \sqrt{\frac{2.m^2 + 1}{3}} \tag{3.25}$$

$$q = \sqrt{\frac{3}{m \cdot (m^2 - 1)/m}} \tag{3.26}$$

The Slantlet matrix is formed by using the parameters of the filters. The Slantlet transform is given by the equation

$$S = SLT_N \, s \, SLT_N^T \tag{3.27}$$

Where s is the two-dimensional signal, SLT_N is an N*N Slantlet matrix, SLT_N^T is transposed Slantlet matrix of size N*N. The coefficient matrix obtained after applying Slantlet transform is represented as

$$S = \begin{bmatrix} S0,0 & S0,1 & \dots & S0,N-1 \\ S1,0 & S1,1 & \dots & S1,N-1 \\ \vdots & \vdots & \ddots & \vdots \\ SN-1,0 & SN-1,1.... & & SN-1,N-1 \end{bmatrix} \tag{3.28}$$

3.3 EMBEDDING CAPACITY

The figure 3.3.1 represents the migration of the secret data that has to be embedded in the cover image. The data relevant to the image is first migrated by certain limit. Since

it is pointed out that an Embedding Capacity of 3,500 bits is enough for the applications of RDH in military application, medical image sharing etc., so the threshold value for optimization is set as 1,000 Characters (7,000 bits).

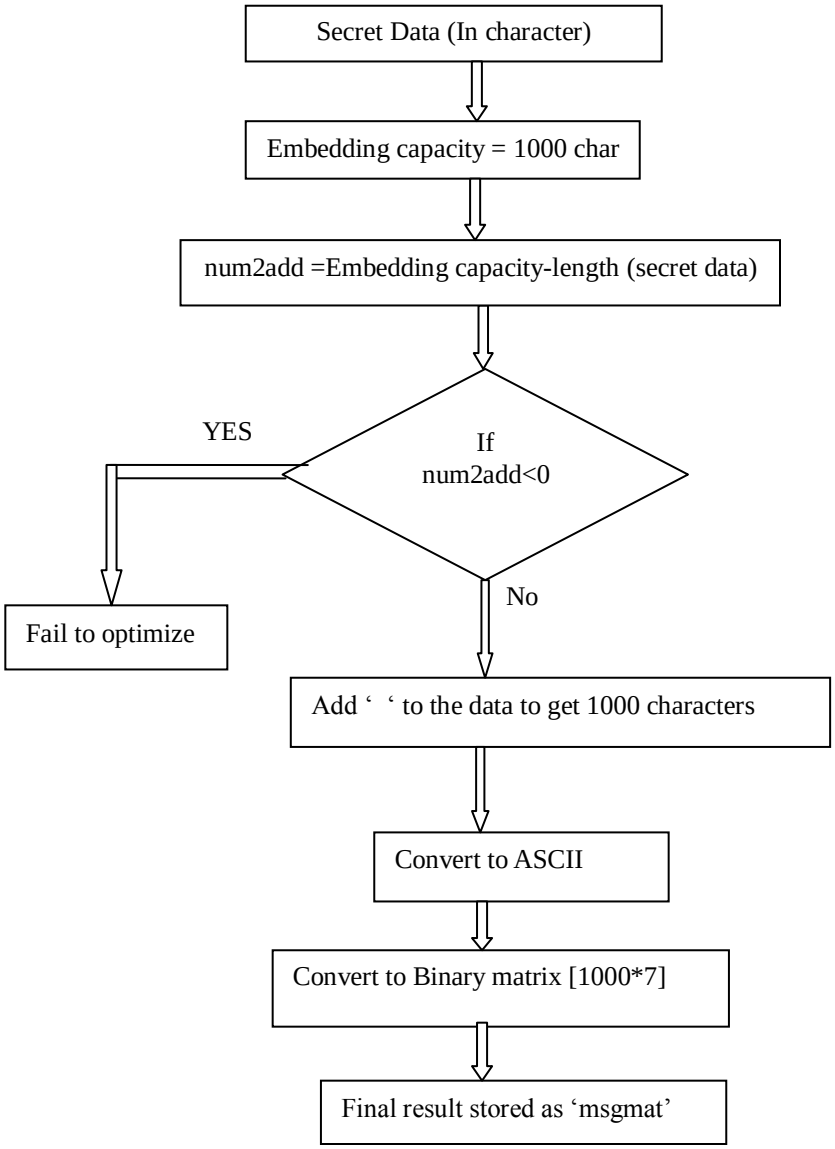


Fig 3.4 Migration of Embedding Capacity

If the length of character is above the threshold value, the embedding process will be failed. The migration is done by padding the null character to the payload which has the length less than the threshold value. Further the processing is initialized by converting the character to its corresponding ASCII values which has exactly 1000 values. In MATLAB,

whatever the data (character, audio, image, video, etc.,) may be, it can be processed in matrix format. So it is then converted to the matrix form which has the value 1 and 0.

$$\begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ & & & \vdots & & & \\ & & & \vdots & & & \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}_{1000\times 7}$$

3.4 PIXEL PAIR MAPPING ALGORITHM

Randomized Pixel Variation also known as pixel pair mapping technique is based on the biological process of pigment cell named as melanocyte controlling the color of epithelial tissue. This technique is used to select the pixel randomly to hide the data bit. The objective is to assure robustness, imperceptibility and high capacity. The technique here is to preprocess the original image to obtain gray scale image whose pixel intensity value ranges from 0 to 255.

The first step is to determine the size of location map. The size of image is calculated and the number of rows and columns are found.

$$\text{dim1} = \text{piclngth} - m \tag{3.29}$$

$$\text{dim2} = \text{pichght} - n \tag{3.30}$$

Here dim1 and dim2 determine the size of location map. Piclngth and pichght are the number of rows and columns of the pixels in the cover image. The values of m and n are taken smaller so that the size of the location map is smaller compared to the size of the original image. The key is used to find out the points in the location map for both embedding and extracting the data bit. Zero matrix of the size of location map is taken, the algorithm iterates 7000 times to find 7000 positions in the location map. These positions are the locations where the secret data is hidden.

The algorithm developed to determine the pixel pair mapping is shown in the fig.3.6. It can also be termed as the mask pattern which is analogous to the biological process. This is a matrix for finding the points to hide the message.

The input of this algorithm is rows, columns, dim1, dim2, and key. The rows and column are used to indicate the exact point of the location map. The dim1 and dim2 are used to determine the size of the mask pattern. Initially the zero matrix A is defined which is nothing but the mask pattern. The iteration of this algorithm will be repeated for 7,000 times to get 7,000 points in the location map. The variables row and column are used for two purposes: one for robustness (i.e.) to transmit the data bit securely and another one is to make decision on the mapping of the point in the location map.

For simplicity, the zero matrix of size 10×10 is selected as the mask pattern and algorithm is performed to get the resultant matrix at the right side of fig 3.5 The white block, which represents the position where the data bit going to be embed in the corresponding position of the cover image.

After secret messages are embedded, some overhead information is needed to extract the covert information and restore the original image. Generally, the overhead information contains the following:

- The information to identify those pixels containing embedded bits.
- The information to solve the overflow/underflow problem. In our proposed scheme, we use four keys to identify the pixels containing embedded bits, and exploit a boundary map, to record information on solving the overflow/underflow problem.

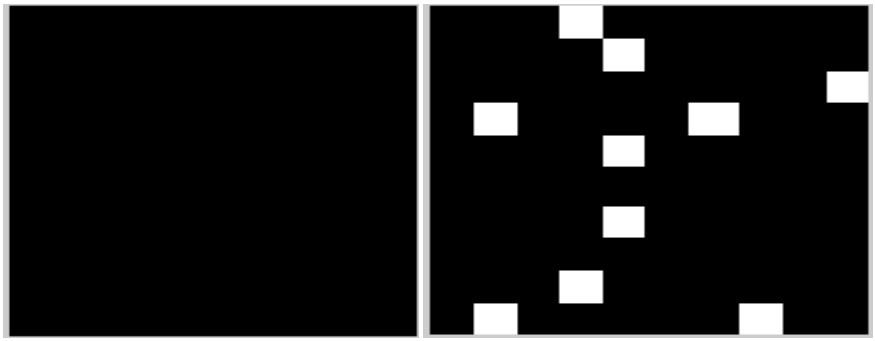


Fig 3.5 A zero matrix of size 10×10 and the resultant matrix to hide the data

When a boundary pixel is encountered during the extracting process, it is originally either a boundary pixel or a pseudo boundary pixel. Therefore, to find the original boundary pixels, boundary map is the right judge to distinguish between genuine and pseudo. It is a

binary array with its every element corresponding to a boundary pixel in the stego-image, 0 for genuine and 1 for pseudo.

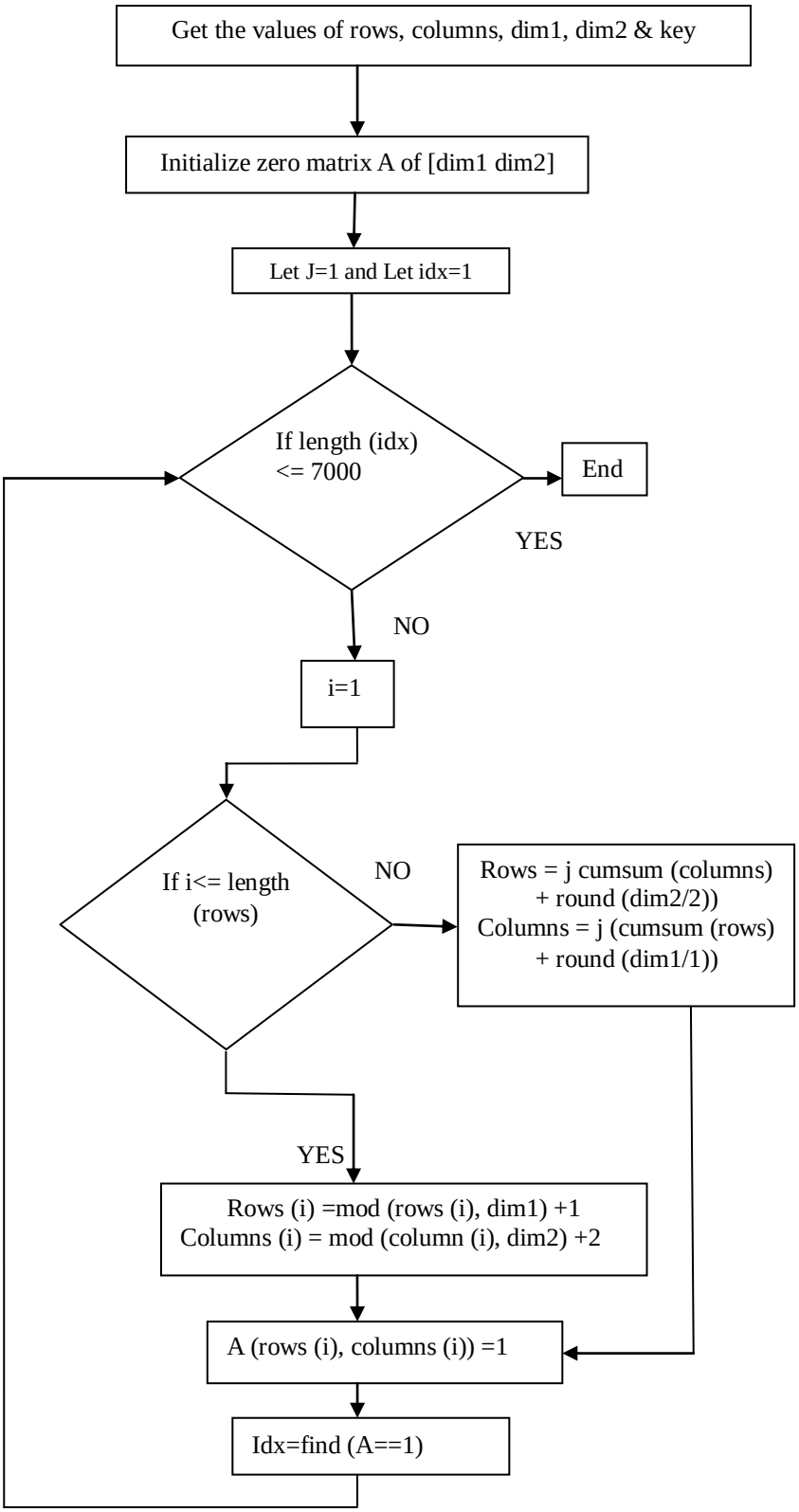


Fig 3.6 Flowchart of the pixel pair mapping algorithm

3.5 PROPOSED ALGORITHM

Step1: Slantlet transform/DWT is applied on cover image. It splits the image into LL, LH, HL and HH sub bands.

Step2: Choose one of the sub bands other than the LL to hide the data.

Step3: The secret data is converted into 7bit ASCII code. The secret data is in the matrix form of 1000*7 of 1's and 0's.

Step4: The selected sub band should be of size sufficient to hide 7000 bits.

Step5: Embedding process: The location map is selected according to the equations (3.29) and (3.30)

Here dim1 and dim2 determine the size of location map. Piclngth and pichght are the number of rows and columns of the pixels in the cover image. m and n are small integer values.

a. Initialize zero matrixes A of size dim1 and dim2 are taken. Generate 7000 1's using pixel pair mapping method.

b. In the location map if the bit corresponding to any row and column is zero, the pixel of the cover image is taken as itself. If the bit corresponding to the row and column is one,

- The remainder of division by 2 of the pixel value in the cover image is taken, if it is zero and the embedded bit is one, then the pixel value is incremented by one.
- The remainder of division by 2 of the pixel value in the cover image is taken, if it is one and the embedded bit is zero, then the pixel value is decremented by one.

Step6: After the Embedding process, the inverse of the Slantlet transform/DWT is taken and the Stego image is obtained.

Step7: The Stego image is sent to the receiver. Again the Slantlet transform/DWT is found

Step8: Extraction process: The extraction process requires the location map. In the

extraction phase 1000* 7 zero matrixes is initialized. Using the even pixel values pointed by index value in the cover image 1's are retrieved and the secret data is extracted.

Step9: The inverse wavelet transform is taken to retrieve the original image.

CHAPTER 4

RESULTS AND DISCUSSIONS

The performance metrics of the proposed method have been evaluated and compared the results of DWT and Slantlet transform method.

The various performance metrics are

(i) Peak Signal to Noise Ratio (PSNR)

(ii) Bit Error Rate (BER)

(iii) Structural Similarity index (SSIM)

Peak Signal to Noise Ratio (PSNR) is defined as:

$$\text{PSNR} = 10 * \log_{10} \left\{ \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} (255)^2}{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \left[I(i,j) - I'(i,j) \right]^2} \right\} \quad (4.1)$$

Where I(i, j) and I'(i, j) are the corresponding cover image and Stego image pixel intensities.

The Bit Error Rate (BER) is the number of bit errors per unit time. The bit error ratio (also BER) is the number of bit errors divided by the total number of transferred bits during a studied time interval.BER is a unitless performance measure, often expressed as a percentage.

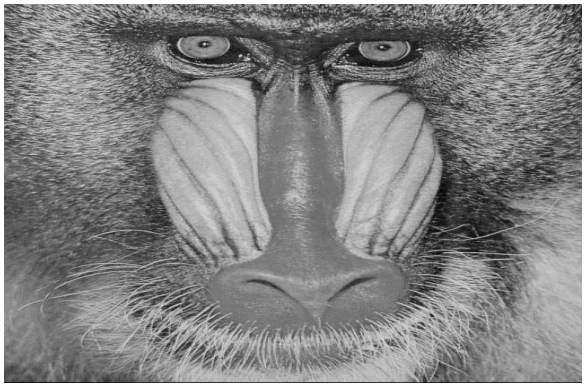
$$\text{Bit Error Rate (BER)} = \frac{\text{Number of Errors}}{\text{Total Transmitted Bits}} \quad (4.2)$$

The Structural Similarity (SSIM) index is a method for measuring the similarity between two images. The SSIM index can be viewed as a quality measure of one of the images being compared provided the other image is regarded as of perfect quality.

$$\text{SSIM} = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu^2{}_x + \mu^2{}_y + c_1)(\sigma^2{}_x + \sigma^2{}_y + c_2)} \quad (4.3)$$

are the average of x and y. $\sigma^2{}_x$, $\sigma^2{}_y$ are the variance of x and y. σ_{xy} is the covariance of x and y. c1 and c2 are the variables to stabilize the division.

(a)



(b)

(c)

(d)

(e)

Fig 4.1 Cover Images (a) Barbara, (b) Baboon, (c) Gold Hill, (d) Boat, and (e) Lena.

Tables 4.1, 4.2 and 4.3 list the comparative PSNR, BER and SSIM values respectively between cover and stego images for various wavelets. In the proposed method, the PSNR values and SSIM are likely similar for various wavelets. Bit Error Rate (BER) increases for various wavelets.

IMAGES	PSNR(dB)				
	db1	db2	db3	db10	db12
BARBARA.gif	61.8679	62.8923	62.8897	63.0049	62.9599
BABOON.gif	61.8493	62.8356	62.8301	62.8709	62.9057
GOLD HILL.gif	61.8025	62.9015	62.8601	62.9374	62.9514
BOAT.gif	61.8753	62.9529	62.9372	63.0800	63.0292
LENA.gif	61.8958	62.9526	62.9500	63.0062	63.0564

Table 4.1 PSNR in dB after embedding the secret data in different cover images.

IMAGES	BER				
	db1	db2	db3	db10	db12
BARBARA.gif	0	0.0056	0.0071	0.0321	0.0403
BABOON.gif	0	0.0050	0.0067	0.0349	0.0403
GOLD HILL.gif	0	0.0054	0.0069	0.0309	0.0407
BOAT.gif	0	0.0047	0.0080	0.0304	0.0379
LENA.gif	0	0.0047	0.0074	0.0304	0.0406

Table 4.2 BER after embedding the secret data in different cover images.

IMAGES	SSIM				
	db1	db2	db3	db10	db12
BARBARA.gif	0.9959	0.9968	0.9966	0.9971	0.9969
BABOON.gif	0.9976	0.9978	0.9976	0.9982	0.9983
GOLD HILL.gif	0.9952	0.9966	0.9966	0.9969	0.9966
BOAT.gif	0.9952	0.0064	0.9965	0.9965	0.9961
LENA.gif	0.9959	0.9967	0.9966	0.9956	0.9970

Table 4.3 SSIM after embedding the secret data in different cover images.

Table 4.4 list the comparative PSNR values respectively between cover and stego images based on Slantlet Transform for various payload.

IMAGES	PAYLOAD(CHARACTERS)									
	100	200	300	400	500	600	700	800	900	1000
LENA.gif	58.3124	58.3063	58.3050	58.3018	58.2994	58.2990	58.2985	58.2926	58.2866	56.2809
BARBARA.gif	58.2942	58.2934	58.2895	58.2893	58.2885	58.2880	58.2874	58.2871	58.2867	58.2863
BABOON.gif	58.2792	58.2783	58.2752	58.2716	58.2698	58.2696	58.2689	58.2684	58.2675	58.2661
GOLDHILL.gif	58.2870	58.2826	58.2787	58.2761	58.2703	58.2659	58.2645	58.2547	58.2531	58.2496
BOAT.gif	58.2653	58.2642	58.2635	58.2602	58.2599	58.2590	58.2526	58.2465	58.2443	58.2438

Table 4.4 PSNR in dB after embedding the secret data in different cover images.

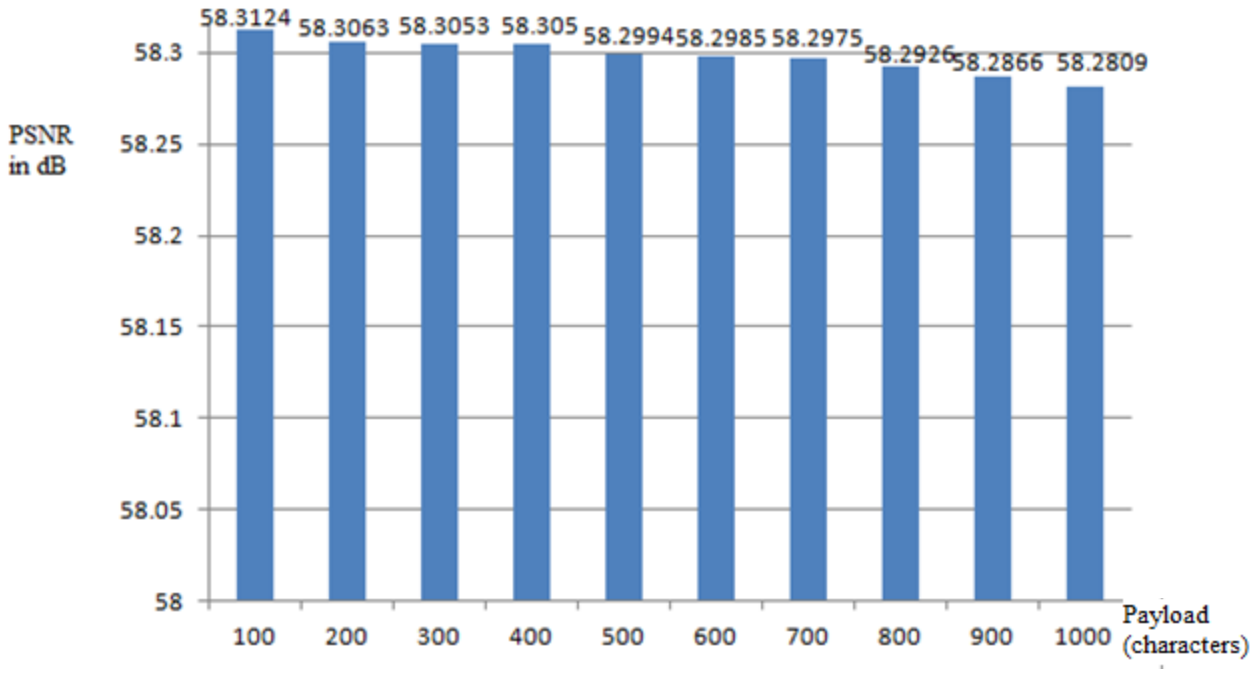


Fig 4.2 PSNR Vs Payload of the proposed method.

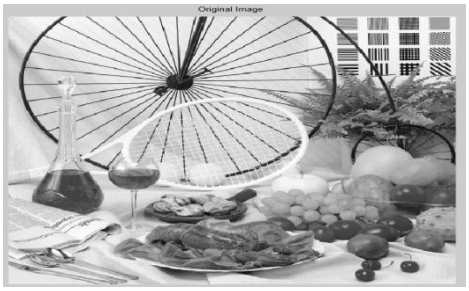
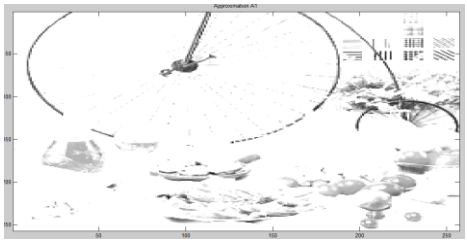
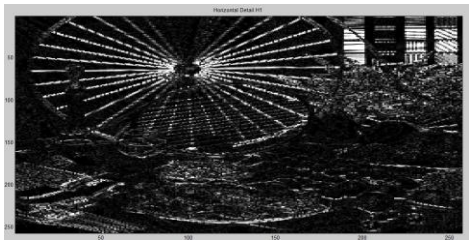


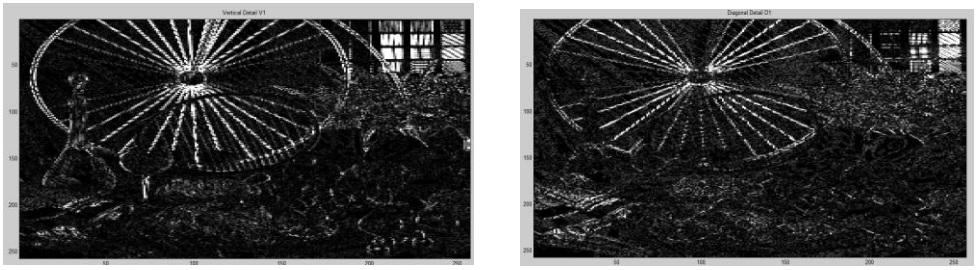
Fig 4.3 Cover Image



(a)



(b)



(c) **(d)**

Fig 4.4 DWT Image (a) Approximation (b) Horizontal (c) Vertical (d) Diagonal bands

(a) **(b)**

Fig 4.5 (a) Stego Image (b) Inverse DWT Image

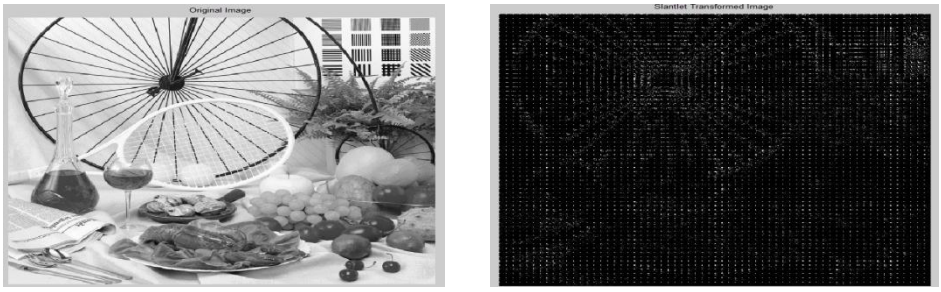
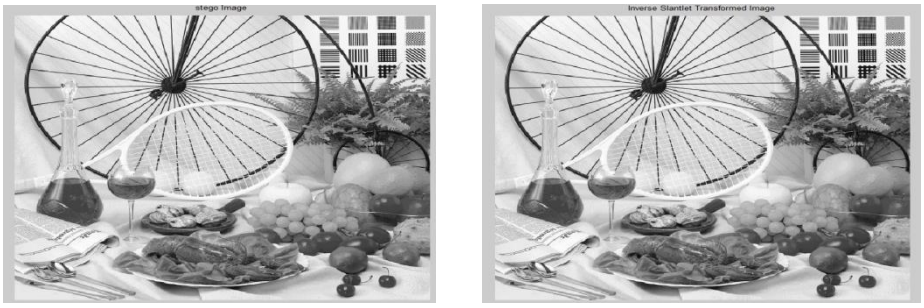


Fig 4.6 Cover Image **Fig 4.7 Slantlet Transformed Image**



(a) **(b)**

Fig 4.8 (a) Stego Image (b) Inverse Slantlet Transformed Image

CHAPTER 5

CONCLUSION AND FUTUREWORK

5.1 CONCLUSION

In this proposed work the Slantlet Transform/DWT and Pixel pair mapping method is used. This proposed scheme ensures the data security with higher success rates and provides high data embedding capacity. The cover image is converted to frequency domain using Slantlet Transform and the Pixel pair mapping method is implemented to embed the data into the cover image to get better results. Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM) have been used to measure the stego image quality and Bit Error Rate (BER) is used to measure the quality of the extracted secret image. The Reversible Data hiding is one of the feasible methodology to protect the important information with authentication, fingerprinting, copy control and covert communication as well as it recovers the cover image exactly.

5.2 FUTURE WORK

This project can be extended by using neural networks algorithm to get more accuracy and embedding capacity. The algorithm can also be implemented for hiding data in audio and video files.

REFERENCES

[1] Guorong Xuan, Yun Q. Shi, Zhicheng Ni, Peiqi Chai, Xia Cui, and Xuefeng Tong, "Reversible Data Hiding for JPEG Images Based on Histogram Pairs" 2007

[2] Hengfu YANG, Xingming SUN, Guang SUN "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution" The Journal of Radio Engineering, Vol. 18, No. 4

[3] Ivan W. Selesnick "The Slantlet Transform" IEEE transactions on signal processing, Vol. 47, No. 5, May 1999

[4] Jun Tian "Reversible Data Embedding Using a Difference Expansion" 890 IEEE transactions on circuits and systems for video technology, VOL. 13, NO. 8, AUGUST 2003

[5] Jun Tian, "Reversible watermarking by difference expansion", Multimedia and Security workshop at ACM multimedia '02, Dec 2002

[6] M. Fallahpour and M.H. Sedaagi, "High capacity lossless data hiding based on histogram modification", IEICE Elecronics Epress, Vol.4, No.7, 205-210

[7] Marghny Mohamed, Fadwa Al-Afari and Mohamed Bamatraf, "Data hiding by LSB sustitution using optimal key-permutation", International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011

[8] Masoud Nosrati , Ronak Karimi and Mehdi Hariri, "Reversible data hiding: principles, techniques and recent studies", World Applied Programming, Vol. 2, Issue (5), May 2012. 349-353

[9] Md. Rashedul Islam, Ayasha Siddiqa, Md. Palash Uddin, Ashis Kumar Mandal and Md. Delowar Hossain, "An efficient filtering based apporoach improving LSB image seganography using status bit along with AES crypography", 3rd International Conference On Informatics, Electronics & Vision 2014

[10] Mehdi Hussain and Mureed Hussaun, "A survey of image seganography techniques", International Journal of Advanced Science and Technology, Vol. 54, May, 2013

[11] Parisa Gerami, Subariah Irahim and Morteza ashardoost, "Least significant bit image steganography using paricle swarm optimization ", International Journal of Computer Applications (0975-8887), Vol. 55, October, 2012

[12] Punam Bedi, Roli Bansal and Priti Sehgal, "Using PSO in a spatial domain based image hiding scheme with disortion tolerance", Computers and Electrical Engineering 39 (2013) 640–654, 2013

[13] Rasha Thabit, Bee Ee Khoo "Robust reversible watermarking scheme using Slantlet transform matrix" The Journal of Systems and Software, 2013

[14] Sushil Kumar, S.K. Muttoo "Distortionless Data Hiding based on Slantlet Transform" International Conference on Multimedia Information Networking and Security, 2009

[15] Vidyasagar M. Potdar, Song Han and Elizabeth Chang, "A survey of digital image watermarking techniques", 3rd IEEE International Conference on Industrial Informatics (INDIN), 2005

[16] Wen-Chung Kuo, Dong-Jin Jiang and Yu-Chih Huang, "A reversible data hiding scheme based on block division", 2008 Congress on Image and Signal Processing

[17] Xiaolong Li, Bin Li, Bin Yang, and Tieyong Zeng, "General framework to histogram-shifting-based reversible data hiding", IEEE Transactions On Image Processing, Vol. 22, No. 6, June 2013

[18] Xiaoxia Li and Jianjun Wang, "A seganographic method based upon JPEG and paricle swarm optimization algorithm", Information Sciences 177 (2007) 3099–3109, Feb 2007

[19] Yongjian Hu, Heung-Kyu Lee, and Jianwei Li, "DE-based reversile data hiding with improved overflow location map", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 19, No. 2, February 2009

[20] Yun Q. Shi, "Reversible data hiding", Third International Workshop, IWDW 2004, Seoul, South Korea, October 30 - November 1, 2004

[21] Weiming Zhang , KedeMa, NenghaiYu "Reversibility improved data hiding in encrypted images" School of Information Science and Technology, June 2013

[22] Zhenxing Qian, Xinpeng Zhang, and Shuozhong Wang , "Reversible Data Hiding in Encrypted JPEG Bitstream" IEEE transactions on multimedia, vol. 16, no. 5, August 2014

[23] Zhi-Hui Wang, Chin-Feng Lee, Ching-Yun Chang "Histogram-shifting-imitated reversible data hiding" The Journal of Systems and Software 86 (2013) 315– 323, 2013

CONFERENCE PUBLICATION

The paper presented on **Reverible Data hiding based on DWT and Slantlet Transform** in international conference ICKCE 2015 at **Kathir College of Engineering.**