AN EFFICIENT DATA HIDING SCHEME USING FRACTIONAL FOURIER TRANSFORM AND FIREFLY ALGORITHM

A PROJECT REPORT

Submitted by

ARUNKUMAR.C

Register No: 13MCO03

in partial fulfillment for the requirement of award of the degree

of

MASTER OF ENGINEERING

in

COMMUNICATION SYSTEMS

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 "**AN EFFICIENT DATA HIDING SCHEME USING FRACTIONAL FOURIER TRANSFORM AND FIREFLY ALGORITHM**" is the bonafide work of **ARUNKUMAR.C. [Reg. No. 13MCO03]** 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
PROJECT SUPERVISOR
Department of ECE,
Kumaraguru College of Technology,
COIMBATORE - 641049

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

The candidates with university **Register No.13MCO03** 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 us with his valuable thoughts.

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.R.Hemalatha M.E., (Ph.D).,** 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., (Ph.D).,** 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 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. According to the problems of steganography, the main effort is to provide a better imperceptibility of stego-image that can be done by decreasing distortion of image.

The proposed method provides a reversible data hiding technique based on Fractional Fourier Transform (FRFT) and Firefly algorithm (FA). The host image is divided into a number of blocks and converted into transform domain using Fractional Fourier Transform (FRFT). Finding the best location to hide the secret data is an important task so that it will conceal the existence of the message. The optimal location to hide the secret data will be found by Firefly Algorithm (FA). The objective function for FA is defined in such a way that both quality and robustness of the stego image are acceptable. This results in a stego image which is not only good in quality but is also able to sustain certain noise. After embedding the secret data into cover medium the inverse Fractional Fourier Transform is applied to convert the cover medium into original form. The histogram shifting technique is used to embed the secret data in the cover image. Histogram Techniques have attracted increasing interests due to their low computational complexity, high visual quality and can achieve good performance in terms of PSNR values. This proposed method ensures the four essential parameters, which are commonly used to determine quality of data hiding scheme. They are robustness, imperceptibility, payload, and security.

The performance metrics like Peak Signal to Noise Ratio (PSNR), Mean Structural Similarity Index (MSSIM), Average difference, Structural Content (SC), Image Fidelity and Normalized Correlation Coefficient have been evaluated and compared the results with other techniques such as LSB substitution, difference expansion and other existing techniques. The comparison with some recent data hiding techniques shows better stego image quality.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

3D	3 Dimensional
BER	Bit Error Rate
BSQ	Block Satistical Quantity
DCT	Discrete Cosine Transform
DWT	Discrete Wavelet Transform
EPR	Electronic Patient Record
FA	Firefly Algorithm
FRFT	Fractional Fourier Transform
GAP	Gradient Adjusted Prediction
HS	Histogram Shifting
JPEG	Joint Photographic Experts Group
LBG	Linde Buzo Gray
LSB	Least Significant Bit
MSSIM	Mean Structural Similarity Index
PSNR	Peak Signal to Noise Ratio
PSO	Particle Swarm Optimization
RDH	Reversible Data Hiding
SC	Structural Content
SSIM	Structural Similarity Index
VQ	Vector Quantization

CHAPTER 1

INTRODUCTION

As the popularity of the Internet and the bandwidth increase rapidly, they offer a great convenience to the transmission of a large amount of various digital multimedia over the Internet day by day. Some of them may be secret information which is candidate to unauthorized access. Therefore, providing the digital multimedia security becomes more important every day. Many techniques have been proposed to deal with this issue. They are

1) Cryptography

2) Steganography

3) Watermarking

4) Reversible data hiding

1.1 CRYPTOGRAPHY

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling plaintext into ciphertext, then back again. The process of the conversion of information from a readable state to apparent nonsense with the usage of a key is called encryption. The process of converting false message into the original one with the help of key is called decryption.

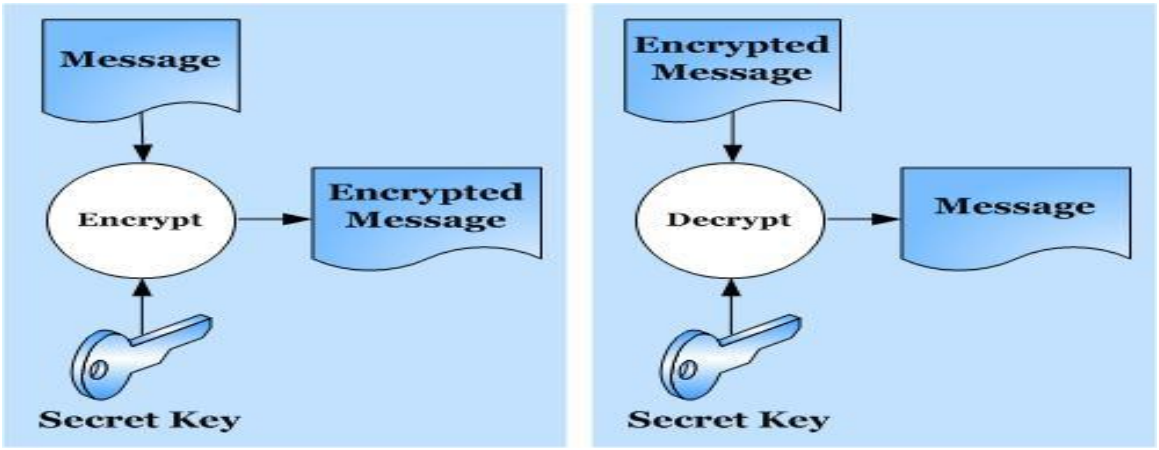


Fig 1.1 cryptography

Modern cryptography concerns itself with the following four objectives:

1) **Confidentiality**: The information cannot be understood by anyone for whom it was unintended.

2) **Integrity:** The information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3) **Non-repudiation**: The creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4) **Authentication**: The sender and receiver can confirm each other's identity and the origin/destination of the information.

1.1.1 Types of cryptography

1) The way in which the plaintext is processed

i) Stream cipher

A stream cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to each binary digit in a data stream, one bit at a time.

ii) Block cipher

A block cipher is a method of encrypting text (to produce ciphertext) in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.

2) Types of operation

i) Substitution cipher

In cryptography, a substitution cipher is a method of encoding by which units of plaintext are replaced with ciphertext, according to a regular system; the "units" may be single letters , pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic. A monoalphabetic cipher uses fixed substitution over the entire message, whereas a polyalphabetic cipher uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa.

ii) Transposition cipher

In cryptography, a transposition cipher is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed.

Eg: Rail Fence cipher, Route cipher

3) Number of keys used

i) Symmetric key cryptography or Secret key Cryptography

In a symmetric cipher, both parties must use the same key for encryption and decryption. This means that the encryption key must be shared between the two parties before any message can be decrypted. Symmetric systems are also known as shared secret systems or private key systems.

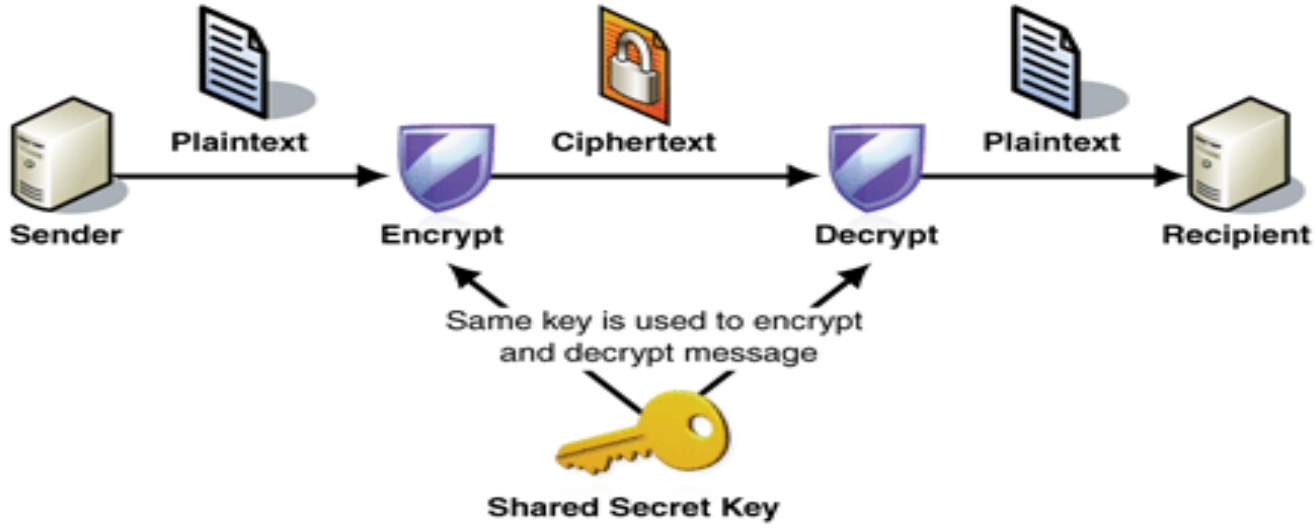


Fig 1.2 Symmetric key cryptography

ii) Asymmetric key cryptography or public key Cryptography

In asymmetric cipher, the encryption key and the decryption key are separate. In asymmetric system, each person has two keys. One key, the public key, is shared publicly. The second key, the private key, should never be shared with anyone. The message is encrypted using private key or public key. Then the decryption is performed using public key or private key. That is why the system is called asymmetric.

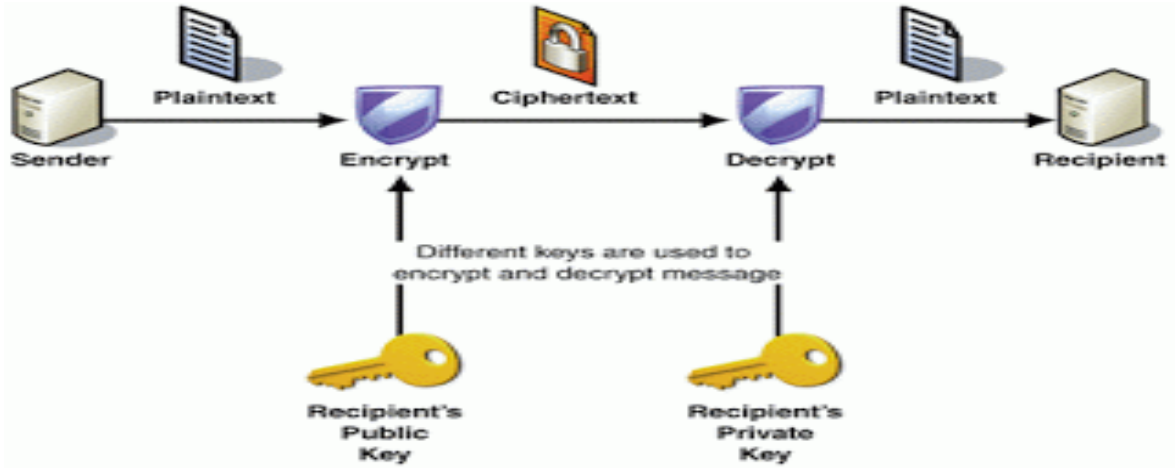


Fig 1.3 Asymmetric key cryptography

1.2 STEGANOGRAPHY

Steganography is the art or practice of concealing a file, message, image, or video within another file, message, image, or video. In modern digital steganography, data is first encrypted by the usual means and then inserted, using a special algorithm, into redundant (that is, provided but unneeded) data that is part of a particular file format such as a JPEG image. Think of all the bits that represent the same color pixels repeated in a row. By applying the encrypted data to this redundant data in some random or nonconspicuous way, the result will be data that appears to have the "noise" patterns of regular, unencrypted data. 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.

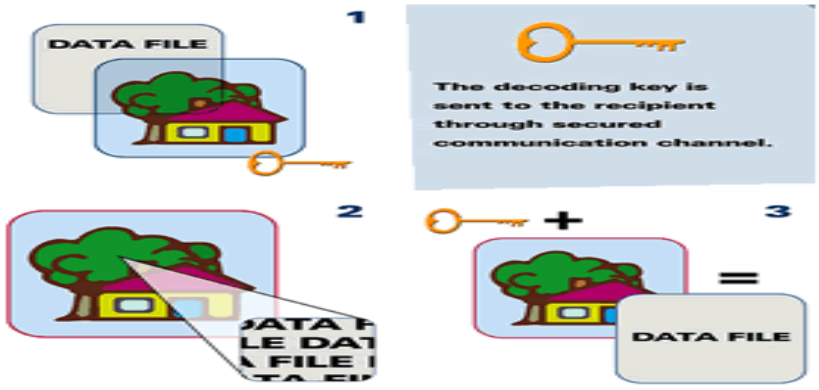


Fig 1.4 Steganography

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.

The needed properties of a digital watermark depend on the use 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.

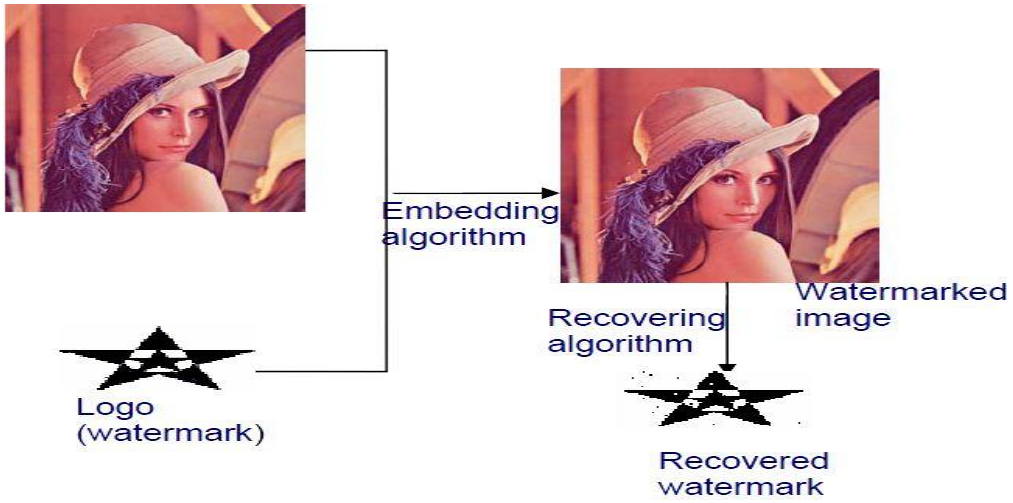


Fig 1.5 Digital watermarking

1.4 REVERSIBLE DATA HIDING (RDH)

Data hiding is a process of embedding useful data into another media called cover media. In the fields like medical, military, remote sensing and judicial, the cover media also needs to be recovered back without distortion after the extraction of the secret data. This type of data hiding is called as Reversible Data Hiding. The main characteristics of reversible data hiding scheme are as follows,

- 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 sifting. 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. DIFFERENCE EXPANSION TECHNIQUE

Tian proposed 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

1.5.2 HISTOGRAM SHIFTING

Ni et al. utilize 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.

1.5.3 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

$$e = x - x' \tag{1.1}$$

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

$$e' = \begin{cases} e + sign(e) \times b, & e = LM \text{ or } RM \\ e + sign(e) \times 1, & e \in (LN,LM) \cup (RM,RN) \\ e, & \text{otherwise} \end{cases} \tag{1.2}$$

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

$$x'' = x' + e' \quad (1.3)$$

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 are the information to identify those pixels containing embedded bit (LM, LN, RM and RN) and the information to solve the overflow/underflow problem.

1.5.4 DCT-BASED DATA HIDING TECHNIQUE

B. Yang et al. proposed DCT based data hiding technique scheme, in this method they choose AC coefficients in the integer DCT domain for the bit-shift operation, and therefore the capacity and the quality of the watermarked image can be adjusted by selecting different numbers of coefficients of different frequencies. To prevent overflows and underflows in the spatial domain caused by modification of the DCT coefficients, they design a block discrimination structure to find suitable blocks that can be used for embedding without overflow or underflow problems.

They also use this block discrimination structure to embed an overhead of location information of all blocks suitable for embedding. With this scheme, secret data bits can be embedded in the saved LSBs of coefficient blocks, and retrieved correctly during extraction, while the original image can be restored perfectly.

1.5.5 VQ-BASED DATA HIDING TECHNIQUE

VQ involves codebook construction from a set of training images; the training images are partitioned into non-overlapping blocks and the most representative blocks are selected to form codebook, in which the elements in the codebook are called codewords. In general, the LBG algorithm is employed to produce the desired codebook. With the generated codebook, each block in an image is encoded with the index of the nearest codeword, such that the total storage space for an image is minimized.

1.5.6 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

$$x' = x + d/2 + b \tag{1.4}$$

$$y' = y - d/2 - b \tag{1.5}$$

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

$$d = (d' + LSB(d'))/2 - b \tag{1.6}$$

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

$$x = (x + y + d)/2 \tag{1.7}$$

$$y = (x + y - d)/2 \tag{1.8}$$

Advantages

(i) High capacity

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

disadvantages

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

(ii) Gray scale mapping

1.5.7 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.

CHAPTER 2

LITERATURE SURVEY

1) Zhicheng Ni, Yun *Q*. Shi, Nirwan Ansari and Wei Su, "Reversible data hiding", ISCAS '03 IEEE Transactions On Circuits And Systems, Vol. 2, May 2003

Ni et al. proposed a novel reversible data biding algorithm, which can recover the original image without distortion from the marked image after the hidden data have been extracted. This algorithm utilizes the zero or the minimum point of the histogram and slightly modifies the pixel values to embed data. It can embed more data as compared to most of the existing reversible data hiding algorithms. A theoretical proof and numerous experiments show that the PSNR of the marked image generated by this method is always above 48 dB, which is much higher than other reversible data hiding algorithms. The algorithm has been applied to a wide range of different images successfully.

In the histogram, a zero point, e.g. 255, (number of pixel assumes the gray value of 255) a peak point, e.g. 154, (a maximum number of pixels assume the gray value of 154) will be choosen. The capacity of this algorithm equals to the maximum number of pixels obtained. In very rare cases, finding the zero point in a histogram is difficult. In this cases minimum point will be used instead of the zero point. If there are multiple pairs of zero points and peak poinrs, obviously, it is possible to further increase the payload by adding complexity to this algorithm. The gray value of the zero point and the peak point will he treated as side information that needs to the transmitted tu the receiving side for data retrieval.

The proposed reversible data hiding scheme is able to embed about 5-60kb its into grayscale image of size 512 x 512. The performance is hence better than most exisiting reversible data hiding algorithms.

Advantages

(i) The PSNR is proven to be above 48dB

(ii) Capacity of embedded data is quite large

(iii) This algorithm can be applied to virtually all type of images

(iv) This algorithm is very simple

(v) The execution time is very short

2) Dae-Soo Kim, Gil-Je Lee, Kee-Young Yoo* "Reversible Image Hiding Scheme for High Quality based on Histogram Shifting" 10th International Conference on Information Technology: New Generations-2013

Ni et al. proposed reversible image hiding scheme using histogram shifting. Their scheme modified the pixel values of the cover-image between the peak point and the zero point in the histogram. PSNR of almost every histogram shifting based methods was about 48dB because many pixels that don't hide the secret data was modified. In this paper, to the higher hiding capacity and image quality improved Ni et al.'s scheme using Gradient-adjusted prediction (GAP) and modulo operation. In experimental results, the hiding capacity of the proposed scheme is superior to Ni et al.'s scheme. Also the image quality of the proposed scheme is increased by about 7 dB than Ni et al.'s scheme.

The goal of the proposed scheme provides the higher hiding capacity and quality than Ni et al.'s scheme by using the gradient-adjusted prediction (GAP) and the modulo operation. The GAP is used to compute the prediction error value between the pixel value of cover image and the prediction value for the increasing hiding capacity. On the other hand, the modulo operation is used to the higher quality than Ni et al.'s scheme. As the GAP is used to the gradient variation of the neighboring pixels, peak point height of the prediction error value is high. It is effective to increase hiding capacity. As numbers wrap around upon reaching a given fixed quantity, the histogram of residue value is directly shifted to the zero point from the peak point. As the result, it provides a high image quality.

The proposed scheme can be prevented to underflow and overflow by simple pre-processing work. In pre-processing stage, when the pixel value is 255, it modify to 254. Likewise, when the pixel value is 0, it modifies to 1. The hiding capacity of Ni et al.'s scheme and the proposed scheme were 5,414 bits and 53,883 bits in Lena image. The hiding capacity of the proposed scheme was increased by almost quadruple.

Advantages

(i) The proposed scheme can achieve good imperceptibility

(ii) Data hiding has higher capacity

(iii) The image quality of the proposed scheme is 56.27dB that is increased by 7.3 dB more than general histogram shifting technique

3)Lingling An, Xinbo Gao, Cheng Deng, and Feng Ji, "Reversible watermarking based on staistical quantity histogram", IEEE Transactions on Image Processing, Vol 21, Mar 2012 Conference on Information Technology: New Generations-2013

Cheng et al. develop a novel histogram shifting based method by introducing a block statistical quantity (BSQ). The similarity of BSQ distributions for different images reduces the diversity of grayscale histograms and guarantees the stable performance of the proposed method. They also adopt different embedding schemes to prevent the issues of overflow and underflow. Moreover, by selecting the block size, the capacity of the proposed watermarking scheme becomes adjustable. the BSQ histograms have a similar shape for different images, the diversity of grayscale histograms can be reduced effectively and thus reliable selection of maximum and minimum points and stable performance will be achieved. Moreover, the block-wise scheme makes the capacity adjusted by the block size. To prevent the issues of overflow and underflow, they classify blocks into regular or singular ones and adopt different embedding strategies.

Advantages

(i) Achieve high PSNR with considerable embedding capacity

(ii) Data hiding has higher capacity

Disadvantages

(i) Proposed method is that additional information is embedded into the image, which decreases the capacity to some extent

4) 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

In order to enhance the data hiding capacity, we use the block division method and one bit to record the change of the selected minimum point to replace the record data method using in Hwang, *et al.*. According to their proposed method and experience analysis, this reversible data hiding scheme is not only to improve the original data hiding capacity but also to reach the goal of data recovering.

In this chung et al. method the cover image is divided to several equal blocks. Then, the maximum point and the two minimum points in this block will be found. Simultaneously, the embedding space is generated by shifting the both side of maximum point to right and left one point, respectively. A location map is proposed to store location information of the pixels (such as maximum point, left minimum point, and right minimum point in each block).

Finally the secret data will be embedded into cover image. They can utilize the block division method to improve the materials amount of displacement effectively and can increase the hidden materials amount. The hiding capacity of HKC scheme is just only 4,304 bits. Comparing with HKC scheme, the embedding capacity is 12,704 bits by using this proposed scheme.

Advantages

(i) Proposed scheme are able to improve the fact embedding capacity by using block division method

(ii) They use one bit to record the change of the selected minimum point to achieve not only higher data hiding capacity but also the reversible effect

5) Che-Wei Lee and Wen-Hsiang Tsai, "A lossless large-volume data hiding method based on histogram shifting using an optimal hierarchical block division scheme", Journal Of Information Science And Engineering XX

A lossless large-volume data hiding method based on histogram shifting is proposed. The method is based on a scheme of hierarchically dividing a cover image into smaller blocks for data embedding using the histogram shifting technique, which yields a large data hiding capacity and results in a high stego-image quality. A technique for recursive looking-ahead estimation of the maximum data hiding volume at the lowest level of the block-division tree structure is proposed to yield an optimal data hiding result. The technique is shown to break a bottleneck of data-hiding-rate increasing at the image block size of 8x8, which is found to exist in other histogram-shifting methods. Four ways of block divisions are used, and one of them is selected optimally in each tree level of block divisions. A good property of the proposed method is, the data hiding rate yielded by the proposed method increases without degrading the stego-image quality.

They divided the cover image into equal-sized sub-blocks from size 256x256 down to 2x2. The data-hiding rate increases from the size of 256x256 through 8x8, and then turns to decrease from 4x4 to 2x2. Additionally, the PSNR values keep increasing from the size of 256x256 all way down to 2x2, contrary to the intuition that hiding more data will result in worsening the stego-image quality. From the above observation, the block size of 8x8 is seen to be the best choice for maximizing the data hiding capacity while minimizing the image distortion. However, this size may as well be regarded as a bottleneck in the trend of data-hiding-rate increasing. To enhance the level of security, proposed methods make use of keys to control the data extraction process. In general, data are embedded into the cover medium in a specific order which is determined by the key. A key is usually constructed by meaningless numbers, and serves as a seed for a random number generator which produces a series of numbers to specify the data embedding order.

6) Jiajia Zhang, Shuli Zheng , Donghui Hu, Yunling Zhang, " Improving histogram shifting reversible data hiding by pixel pair's average predictions" Ninth International Conference on Computational Intelligence and Security-2013

Based on histogram shifting and histogram modification of difference images, this paper proposed a method of histogram shifting reversible data hiding by pixel pair's average predictions on gray images. Under the premise that the average remains changeless after each operation, embedding and extracting operations are completed, utilizing the difference histogram theory. Experimental results demonstrate that the proposed method can keep high image quality and high embedding capacity, and produce little auxiliary information. It is better than the comparative method with good performance.

This proposed method is divided into M×N/2 group of pixels pairs in the size of M×N image. The average of each original pixel pair is calculated and then the prediction errors between the original value and the average are obtained composing a difference matrix. Next, we can find out the peak point and the zero point, and the secret information is embedded according to difference histogram theory. According to the rules that are proposed and the peak point and the zero point, the secret information are extracted and the image is recovered during the extraction process.

In our proposed method, we use the literature way to prevent overflow and underflow. That way is mainly through the boundary pixels plus or minus k, marking with a flag bit. For example, suppose that k=1, if the value of pixel is 0, and then plus 1 to become 1, the flag bit become 1.If the original pixel value is 1, the flag bit become 0. If the pixel value is 255, and then minus 1 to become 254, the flag bit become 1, and another condition is that the flag bit is 0 when the original pixel value is 254. So the original pixel value is determined by the flag bit. The total size of these flag bits is based on the number of occurrences of the pixel value: 0, 1, 254, 255. Namely, the sum of the number of occurrences of these pixel values is multiplied by 1 in bits. Finally, these flag bits can be used as auxiliary information transmitted to the recipients, or as an embedded part of the secret information to embed into the original

Advantages

(i) The embedding capacity is improved

(ii) The image quality is guaranteed

7) Xinlu Gui, Xiaolong Li and Bin Yan, "Efficient Reversible Data Hiding Based On Two-Dimensional Pixel-Intensity-Histogram Modification", IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP)

In this paper, referred to the general framework of histogram shifting- based reversible data hiding, some valuable related works based on two-dimensional pixel-intensity-histogram modification are first introduced. In these schemes, all pixels are classified into two categories, which are embedded with data or shifted for reversibility, respectively. From this point of view, novel embedding schemes are proposed with more applicable pixel partition and more redundant information utilized. Moreover, pixel selection is conducted such that smooth pixels are priority embedded to further exploit the image redundancy. The experimental results show the superiority of the proposed methods over some state-of-the-art works in terms of capacity-distortion performance.

The two novel RDH schemes based on two-dimensional pixel-intensity-histogram are proposed, which outperform some previous HS-based methods in the capacity-distortion performance. The first one adaptively embeds data into high frequency pixel pairs to improve the capacity without distortion increment. The other one guarantees that for a desired capacity, the payload is chosen to keep more pixel pairs unchanged after embedding.

Advantages

(i) Improve the capacity without distortion increment

8)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

This paper proposed a novel reversible data hiding scheme based on the histogram-shifting-imitated approach. Instead of utilizing the peak point of an image histogram, the proposed scheme manipulates the peak points of segments based on image intensity. The secret data can be embedded into the cover image by changing the peak point pixel value into other pixel value in the same segment. The proposed method uses a location map to guarantee the correct extraction of the secret data.

Since the modification of the pixel value is limited within each segment, the quality of the stego image is only related to the size of the segmentation, which means after embedding data into the cover image, it can be reused to do the multi-layer data embedding while maintaining the high quality of the final stego image. The experimental results of comparison with other existing schemes demonstrate the performance of the proposed scheme is superior to the others.

Advantages

(i) It is a lossless process with respect to the image, which allows an authorized party to decode the embedded data and completely restore the original state

(ii) This scheme achieved at stego-image that has high visual quality. A smaller segment size can yield a stego-image with even better visual quality because both the cover pixel and its corresponding stego-pixel fall within the same segment. PSNR above 40 dB is achieved

(iii) It is effective for multiple-layer embedding without loss in image fidelity, because the segment confines the degree of pixel modification. No matter how many layers of message embedding are used, image distortion can only occur to a very limited extent

(iv) It used a simple function, i.e., pixel-shifting mapping with a private key, to perform the embedding and extracting processes, which takes a small amount of time and is secure

9)Sayan Chakraborty, Sourav Samanta, Debalina Biswas, Nilanjan Dey, and Sheli Sinha Chaudhuri, "Particle swarm optimization based parameter optimization technique in medicalinformation hiding", IEEE International Conference on Computational Intelligence and Computing Research, 2013

In this paper, a Discrete Wavelet Transformation (DWT) based method is proposed for embedding a Hospital Logo or Electronic Patient Record (EPR), where the embedding factors/scaling factors is optimized by Particle Swarm Optimization (PSO). In this proposed method, they are using particle swarm optimization for embedding factors, as PSO. At first PSO randomly generates a no. of particles, which forms the initial swarm. Each swarm has their own individual values of embedding factors. By using these values, a watermark image is embedded and the PSNR value of watermarked biomedical image is calculated.

After secret image embedding process, the similarity between the original image x and modified image x' is measured by the standard correlation coefficient. Then velocity of the swarm and particles is updated. After updating velocity, positions of particles are also updated. The above procedure is repeated for no. of iterations (n) defined. After n iterations, a set of (n+1) best positions is obtained. From these (n+1) positions, the position with the best fitness value is chosen as the best position. The entire procedure is repeated further to generate new sets of positions to produce the gbest.

Out of these n no. of gbests, the position with the highest fitness value where highest fitness is PSNR+100*correlation, is chosen as the best position and the corresponding values of the embedding factors are stored as the optimized embedding factor used for embedding

watermark. The PSNR value obtained after convergence is quiet satisfactory(25.7253), which claims the robustness and the efficacy of the proposed method.

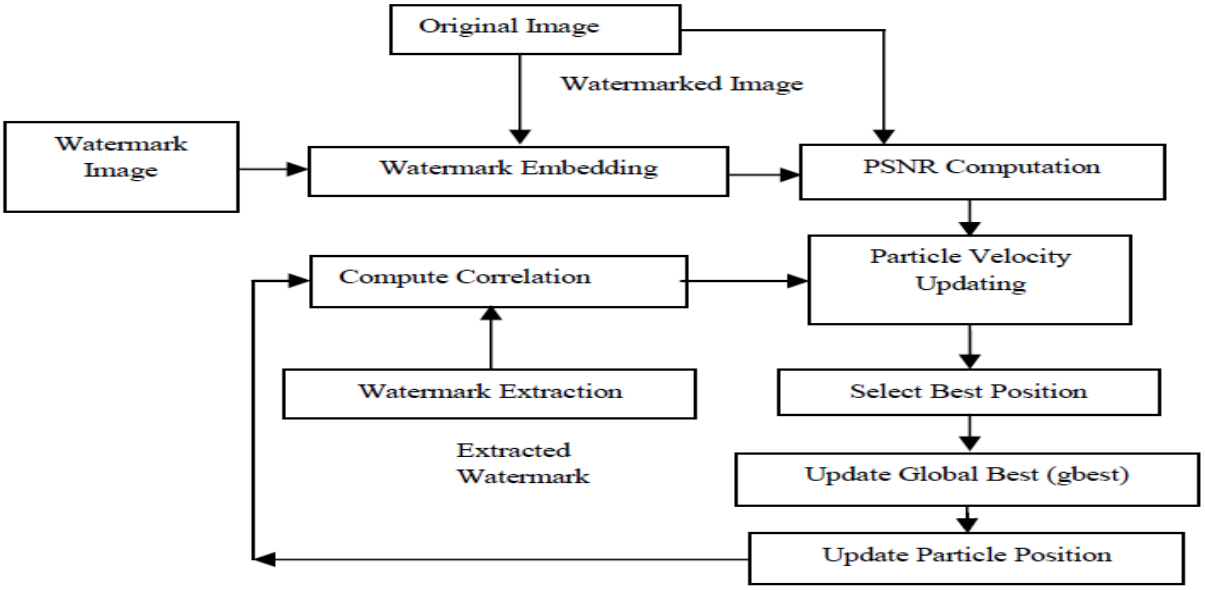


Fig 2.1 Data Embedding & Extraction Procedure of Chaudhuri et al method

Advantages

(i) This proposed method is robust enough against various common attacks on biomedical images

10)Punam Bedi, Roli Bansal, Priti Sehgal, "Using PSO in a spatial domain based image hiding scheme with distortion tolerance" The Journal of Computers and Electrical Engineering 39 (2013) 640–654

This paper presents an efficient spatial domain based image hiding scheme, using Particle Swarm Optimization (PSO). Here, PSO is used to find the best pixel locations in a gray scale cover image where the secret gray scale image pixel data can be embedded. The objective function for PSO is defined in such a way that both quality and robustness of the stego image are acceptable. This results in a stego image which is not only good in quality but is also able to sustain certain noise and compression attacks during transmission. The results when compared with some recent data hiding techniques in the spatial domain show better stego image quality along with distortion tolerance.

Particle Swarm Optimization (PSO) is a population based stochastic optimization technique, inspired by social behavior of bird flocking or fish schooling. Each particle or individual in the population represents a potential solution. The particles are flown through a multidimensional search space, where the position of each particle is adjusted according to its own experience and that of its neighbors. All the particles have fitness values which are calculated by the objective function to be optimized by the PSO algorithm and have velocities which direct the movement of the particles. The PSO process is iterative. After generating an initial swarm the value of the fitness function is evaluated in every iteration and the velocity and position of each particle is updated accordingly. The algorithm is terminated when one of the following occurs:

(i) Maximum number of iterations has been reached

(ii) An acceptable solution has been found

(iii) No improvement is observed over a number of iterations

Advantages

(i) Good in quality

(ii) Robust to certain image processing attacks

Disadvantage

(i) Embedding capacity is low

CHAPTER 3

PROPOSED METHODOLOGY

3.1 FRACTIONAL FOURIER TRANSFORM (FRFT)

The FRFT belongs to the class of time – frequency representations that have been extensively used by the signal processing community. In all the time – frequency representations, one normally uses a plane with two orthogonal axes corresponding to time and frequency. The fractional Fourier transform (FRFT) is a family of linear transformations generalizing the Fourier transform. It can be thought of as the Fourier transform to the n-th power, where n need not be an integer thus, it can transform a function to any intermediate domain between time and frequency. The Classical Fourier transform (FT) is one of special case, which the fractional Fourier Transform (FRFT). The FRFT relies on a parameter α and can be interpreted as a rotation by an angle α in the time-frequency plane. One of special case in FRFT with $\alpha = \pi / 2$ corresponds to the FT, and an FRFT with $\alpha = 0$ corresponds to the identity operator. When α is not equal to a multiple of 0.5π, the FRFT is equivalent to do $\alpha / (0.5\pi)$ times of FT.

The FRFT is defined by means of the transformation kernel as

$$K_\alpha(t,u) = \begin{cases} \sqrt{(1 - j\cot\alpha)/2\pi}\; e^{j(t^2+u^2/2)\cot\alpha - jut\csc\alpha} & \text{, if } \alpha \text{ isn't a multiple of } \pi \\ \delta(t-u) & \text{, if } \alpha \text{ is a multiple of } 2\pi \\ \delta(t+u) & \text{, if } \alpha+\pi \text{ is a multiple of } 2\pi \end{cases} \quad (3.1)$$

The fractional Fourier transform of a function x, with an angle α, is defined as the function $R^\alpha = X_\alpha$

$$X_\alpha(u) = \int_{-\infty}^{\infty} x(t) K\alpha(t,u)\, dt \quad (3.2)$$

$$K_\alpha(t,u) = \begin{cases} \sqrt{(1 - j\cot\alpha)/2\pi}\; e^{j(u^2/2)\cot\alpha \int x(t) e^{j(t^2/2)\cot\alpha - jut\csc\alpha}} & \text{, if } \alpha \text{ isn't a multiple of} \\ \delta(t-u) & \text{, if } \alpha \text{ is a multiple of } 2\pi \\ \delta(t+u) & \text{, if } \alpha+\pi \text{ is a multiple of } 2\pi \end{cases} \quad (3.3)$$

3.1.1 Computation of the fractional Fourier transform

The FRFT of a signal x(t) as given by Eq. (3.8) can be computed by the following steps:

1. Product by a chirp—chirps are functions whose frequency is linearly increasing with time

2. A Fourier transform with its argument scaled by cosec(function)

3. Another product by a chirp

4. A product by a complex constant

R_{α} represents the signal to correspond to the original coordinates (t,w) counterclockwise rotates to the original coordinates (u,v) with angle $\boldsymbol{\alpha}$ in time-frequency plane, as Fig. 3.1.

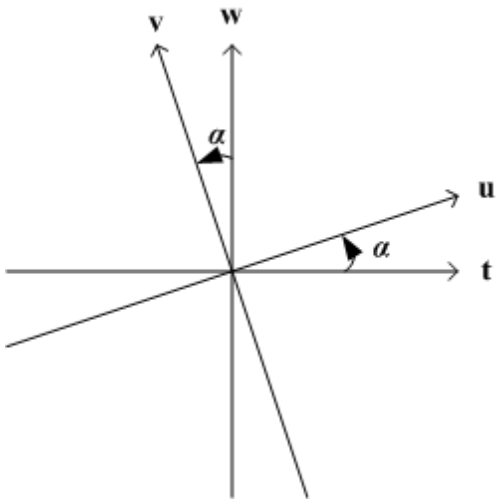


Fig 3.1 The original coordinates (t,w) rotates to the original coordinates (u,v) with angle α in time-frequency plane.

3.1.2 Properties of the fractional Fourier transform

Let F_{α} denote the operator corresponding to the FRFT of angle α. Under this notation, some of the important properties of the FRFT operator are listed below:

1. Identity operator

F_0 is the identity operator. The FRFT of order $\alpha = 0$ is the input signal itself. The FRFT of order $\alpha = 2\pi$ corresponds to the successive application of the ordinary Fourier transform 4 times and therefore also acts as the identity operator, i.e. $F_0 = F_{\pi/2} = I$.

2. Fourier transform operator

$F_{\pi/2}$ is the Fourier transform operator. The FRFT of order $\alpha = \pi/2$ gives the Fourier transform of the input signal.

3. Successive applications of FRFT

Successive applications of FRFT are equivalent to a single transform whose order is equal to the sum of the individual orders.

$$F_{\alpha}(F_{\beta}) = F_{\alpha+\beta} \tag{3.4}$$

4. Inverse

The FRFT of order $-\alpha$ is the inverse of the FRFT of order a since

$$F_{-\alpha}(F\alpha) = F\alpha - \alpha = I \tag{3.5}$$

3.2 APPLICATIONS OF FRFT

Fractional Fourier Transform finds applications in many fields.

1. Filter Design
2. Optics Analysis & Optical Implementation
3. Space-Variant Pattern Recognition
4. Sampling & Modulation
5. Encryption & Phase Retrieval
6. Signal Synthesis
7. Multiplexing

3.3 FIREFLY ALGORITHM

The flashing light of fireflies is an amazing sight in the summer sky in the tropical and temperate regions. There are about two thousand firefly species, and most fireflies produce short and rhythmic flashes. The pattern of flashes is often unique for a particular species. The flashing light is produced by a process of bioluminescence, and the true functions of such signaling systems are still debating. However, two fundamental functions of such flashes are to attract mating partners (communication), and to attract potential prey. In addition, flashing may also serve as a protective warning mechanism. The rhythmic flash, the rate of flashing and the amount of time form part of the signal system that brings both sexes together. Females respond to a male's unique pattern of flashing in the same species, while in some species such as photuris, female fireflies can mimic the mating flashing pattern of other species so as to lure and eat the male fireflies who may mistake the flashes as a potential suitable mate.

It is known that the light intensity at a particular distance r from the light source obeys the inverse square law. i.e., the light intensity I decreases as the distance r increases in terms of

$I=1/ r^2$. Furthermore, the air absorbs light which becomes weaker and weaker as the distance increases. These two combined factors make most fireflies visible only to a limited distance, usually several hundred meters at night, which is usually good enough for fireflies to communicate. The flashing light can be formulated in such a way that it is associated with the objective function to be optimized, which makes it possible to formulate new optimization algorithms.

The firefly algorithm (FA) is a metaheuristic algorithm, inspired by the flashing behavior of fireflies. The primary purpose for a firefly's flash is to act as a signal system to attract other fireflies. Xin-She Yang formulated this firefly algorithm by assuming:

(i) All fireflies are unisexual, so that one firefly will be attracted to all other fireflies;

(ii) Attractiveness is proportional to their brightness, and for any two fireflies, the less bright one will be attracted by (and thus move to) the brighter one; however, the brightness can decrease as their distance increases;

(iii)If there are no fireflies brighter than a given firefly, it will move randomly.

The brightness should be associated with the objective function. Firefly algorithm is a nature-inspired metaheuristic optimization algorithm. Based on these three rules, the basic steps of the firefly algorithm (FA) can be summarized as the pseudo code.

3.3.1 Pseudo code of the firefly algorithm (FA)

Begin;

Initialize algorithm parameters:

MaxGen: the maximal number of generations

γ: the light absorption coefficient

r: the particular distance from the light source

d: the domain space

Objective function $f(x)$, $x = (x1, ..., xd)^T$

Generate initial population of fireflies xi (i = 1, 2, ..., n)

Light intensity Ii at xi is determined by $f(x_i)$

Define light absorption coefficient γ

while (t <MaxGeneration)

for i = 1 : n all n fireflies

for j = 1 : i all n fireflies

if (Ij > Ii), Move firefly i towards j in d-dimension; end if

Attractiveness varies with distance r via exp[−γr]

Evaluate new solutions and update light intensity

end for j

end for i

Rank the fireflies and find the current best

end while

Post process results and visualization

3.3.2 Attractiveness

In the firefly algorithm, there are two important issues: the variation of light intensity and formulation of the attractiveness. For simplicity, we can always assume that the attractiveness of a firefly is determined by its brightness which in turn is associated with the encoded objective function. In the simplest case for maximum optimization problems, the brightness I of a firefly at a particular location x can be chosen as $I(x) \alpha f(x)$. However, the attractiveness β is relative, it should be seen in the eyes of the beholder or judged by the other fireflies. Thus, it will vary with the distance r_{ij} between firefly i and firefly j. In addition, light intensity decreases with the distance from its source, and light is also absorbed in the media, so we should allow the attractiveness to vary with the degree of absorption.

In the simplest form, the light intensity I(r) varies according to the inverse square law

$$I(r) = I_s/r^2 \tag{3.6}$$

where I_s is the intensity at the source.

For a given medium with a fixed light absorption coefficient , the light intensity I varies with the distance r. That is

$$I = I_0 e^{-\gamma r} \tag{3.7}$$

where I_0 is the original light intensity.

Since a firefly's attractiveness is proportional to the light intensity seen by adjacent fireflies, we can now define the attractiveness β of a firefly as

$$\beta = \beta_0 \, e^{-\gamma r\hat{}2} \tag{3.8}$$

Where β0 is the attractiveness at r = 0. Since it is often faster to calculate1/(1 + r2) than an exponential function, the above function, if necessary, can be approximated as

$$\beta = \beta o / (1+\gamma r\hat{}2) \quad (3.9)$$

3.3.3 Distance and Movement

The distance between any two fireflies i and j at position x_i and x_j is

$$r_{ij} = \|x_i - x_j\| = \sqrt{\sum_{k=1}^{d} (x_{i,k}-x_{j,k})^2} \quad (3.10)$$

where $x_{i,k}$ is the i^{th} firefly's k^{th} component of the spatial coordinate x_i.

The firefly i's movement towards another brighter firefly j is found by

$$xi = xi + \beta_0 e^{-\gamma r\hat{}2}(x_j-x_i) + \alpha (rand - 1/2) \quad (3.11)$$

where the randomization parameter α € [0, 1] and rand is the random number.

3.4 PROPOSED DATA HIDING SCHEME

The proposed image hiding scheme aims at searching optimum locations adaptively in the cover image in frequency domain to hide a secret data so that the stego image thus produced is good in quality. The proposed work uses Fractional Fourier Transform to convert the cover image into frequency domain and Firefly Algorithm (FA) to find optimal location in cover that image. The following subsections discuss the objective function to be used by Firefly Algorithm and the algorithms for secret data hiding and extraction.

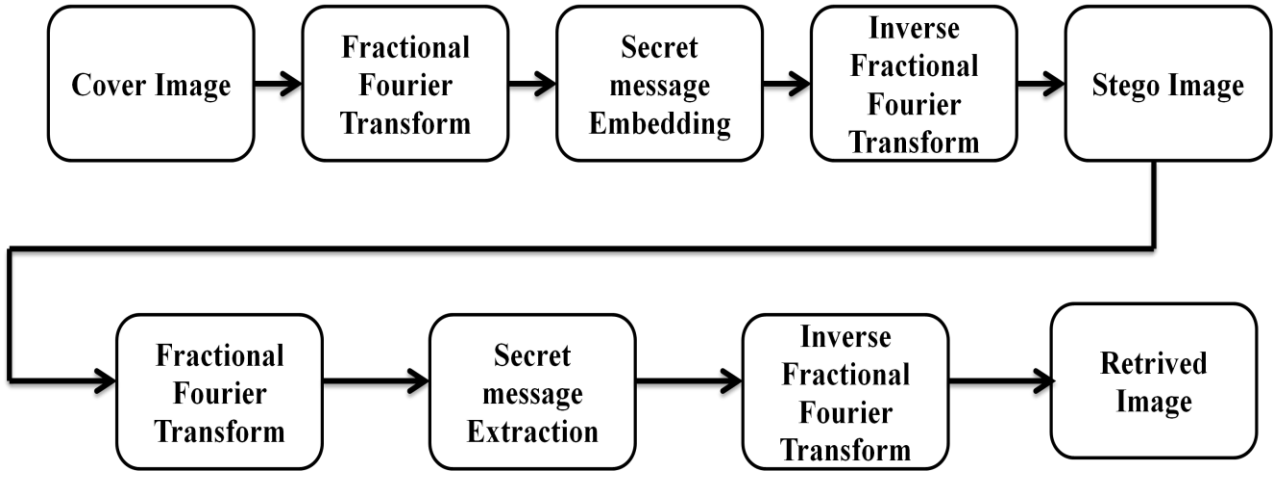


Fig 3.2 Block diagram of proposed method

3.4.1 Objective function

The objective function to be used by the FA module is set in such a way that both quality and robustness of the stego image are acceptable. The quality of the stego image is calculated using Structural Similarity Index (SSIM) which is defined as follows:

$$SSIM\ (x,y) = (2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2) / (\mu^2_x+\mu^2_y+c_1)(\sigma^2_x+\sigma^2_y+c_2) \quad (3.12)$$

Where x and y are same size window of the cover and stego image and μ_x and μ_y are corresponding x and y averages. σ^2_x and σ^2_y are the variances of x and y and σ_{xy} is the covariance of x and y. c_1 and c_2 are constants.

The Bit Error Rate (BER) represents the robustness of the stego image is defined as:

$$BER = \sum_{k=0}^{n} b \oplus b' / N \quad (3.13)$$

Where b and b' are embedded and extracted bits respectively, N is the total number of secret bits embedded and $\oplus$ represents the XOR operation. The value of BER will be anywhere between 0 and 1. If BER value closer to 1 then the error value of extracted data is higher. The value of BER is calculated after retrieving the secret data from the stego block. The aim of the proposed technique is to minimize BER of the embedded and the extracted secret data and to maximize the SSIM index between the cover and the stego images.

In order to cater to the two objectives in the objective function, the proposed technique uses a linear blending aggregate approach to multi objective optimization. Hence the objective function F minimized by FA is defined as:

$$F = \gamma\ (1- SSIM(B,B')) + (1- \gamma)\ BER \quad (3.14)$$

Where γ is the experimentally calculated weighting constant and B and B' are corresponding cover image and stego image block.

3.4.2 Embedding the secret data

The proposed framework for embedding a secret data in a cover image in the transform domain is shown in Fig.3.4. The embedding technique finds optimum locations of pixels in the host image in transform domain, using FA. The fitness function to be used by the FA module is based on the quality and distortion tolerance of the stego image as discussed in the previous subsection. These output locations of the FA module are then used to embed the secret data.

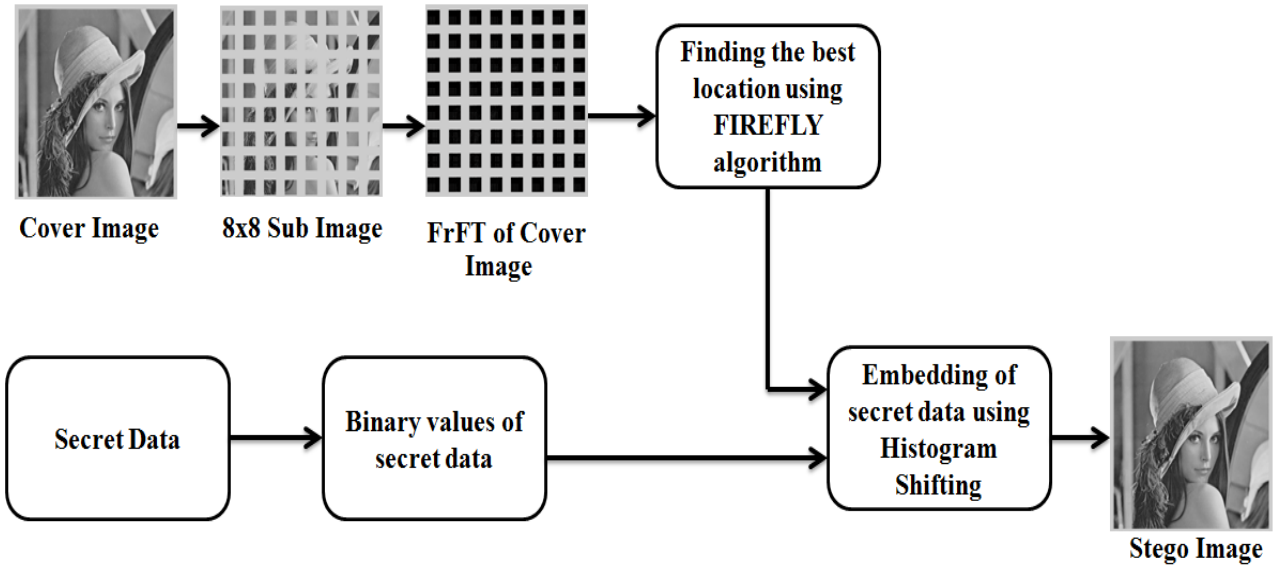


Fig 3.3 Proposed framework for embedding a secret image in a cover image.

The steps to embed the secret data into cover image are presented below

Step 1: Get cover image and secret data: Read the cover image I (MxN) and the secret data to be hidden.

Step 2: The secret data is converted into binary and then secret word W is formed by concatenating the binary bits. The length of W be len.

Step 3: Dividing cover image into number of blocks of size 8x8 as B_i, i = 1…. t. Thus, the number of secret data bits to be hidden in each block is calculated as r = len/t.

Step 4: Each block is converted into transform domain using Fractional Fourier Transform with the angle of rotation α ranges from 0 to 360 degree.

Step 5: To find the best location in each block using firefly algorithm, we need to perform the following:

- set the initial parameters:

  nf (Number of fireflies),

  its (Maximum number of iterations)

  γ (weighting constant)

  α (randomization parameter between 0 & 1)

c1 and c2 (constants)

rand (random number)

- Each firefly has the size of number bits to be hidden in each block r. If r is 5 then each firefly represents the group of 5 bits which is chosen from 64 pixel block.

- Next, the objective function to be used by the FA module is set as discussed in the previous subsection. Although the SSIM has a relatively simple mathematical definition, experiments show that it outperforms the PSNR under different types of image distortion. The objective function minimized by FA is given by Eq. (3.14) in Section 3.4.1.

- In every iteration, for each firefly, the r bits secret data are embedded in the firefly pixels and the stego image block is computed. Once the stego block is computed, the secret bits are extracted and SSIM of the original and stego block are computed and BER between embedded bits b and extracted bits b' is computed. These two values are used to calculate the fitness of the firefly with respect to the objective function (Eq. (3.14)). The maximum value of the objective function is stored as great value. Then the fireflies will choose random location and this process is repeated until the following conditions occur:

    - Number of iteration exceeds maximum number of iterations
    - No improvement is obtained in the successive iterations
    - An acceptable result has been found

  Once the terminating condition occurs then the corresponding location of the firefly of the great value has been chosen as final location. The resulting location represents the optimum solution which when used for embedding, will result in better image quality.

Step 6: Embedding Process: The r bits from secret word W is embedded in the final location of each block. For this purpose the histogram shifting method is used. First the entire pixel value of final location is decremented by 1. Then the maximum value will be found among the final location. Now we embed the secret data in the place of the maximum value. If the secret data is 1 then the maximum value will be increased by1. If the secret data is 0 then the maximum value will be left unchanged. Similarly all the secret data will be embedded in the corresponding block.

Step 7: To ensure the reversibility of embedding, location map is used. The index of the final location and its maximum value have been stored in the location map.

Step 8: After embedding all sub blocks are subjected to inverse fractional fourier transform to create the stego image.

3.4.3 Extracting the secret data

Step 1: Divide the stego image into a number of blocks of size M x N.

Step 2: Fractional Fourier transform with 120 degree of rotation is applied to each block to convert the stego image into transform domain.

Step 3: The maximum value of each stego image block is compared with the maximum value of the corresponding final location in the location map. If the stego image block maximum value is greater than the final location maximum value then bit 1 is extracted and if stego image block maximum value is equal to the final location maximum value then bit 0 is extracted.

Step 4: The value of the stego image block maximum is decremented by 1 whenever the secret bit 1 is extracted.

Step 5: Similarly all the secret data will be extracted from the corresponding block.

Step 6: To reproduce the cover image, inverse fractional fourier transform is applied to all the blocks.

3.5 DIFFERENT ATTACKS AFFECTING THE IMAGE

There are number of attacks affecting the image quality. They are Salt and pepper noise, Gaussian noise, Poisson noise, Speckle noise, Resizing and Blurring, Image Sharpening and Scaling, Image Rotation and Flipping, Image patching, Stair case artifacts and stir mark attacks.. etc. They may destroy the image and the data embedded and also affect PSNR, SSIM, etc.

3.5.1 GAUSSIAN NOISE

Gaussian noise represents statistical noise having probability density function (PDF) equal to that of the normal distribution, which is also known as the Gaussian distribution. In other words, the values that the noise can take on are Gaussian-distributed. A special case is white Gaussian noise, in which the values at any pair of times are identically distributed and statistically independent (and hence uncorrelated). In communication channel testing and modeling, Gaussian noise is used as additive white noise to generate additive white Gaussian noise. In telecommunications and computer networking, communication channels can be affected by wideband Gaussian noise coming from many natural sources, such as the thermal vibrations of atoms in conductors (referred to as thermal noise or Johnson-Nyquist noise), shot

noise, black body radiation from the earth and other warm objects, and from celestial sources such as the Sun.

Principal sources of Gaussian noise in digital images arise during acquisition eg. Sensor noise caused by poor illumination and/or high temperature, and/or transmission eg. Electronic circuit noise. In digital image processing Gaussian noise can be reduced using a spatial filter, though when smoothing an image, an undesirable outcome may result in the blurring of fine-scaled image edges and details because they also correspond to blocked high frequencies. Conventional spatial filtering techniques for noise removal include: mean (convolution) filtering, median filtering and Gaussian smoothing.

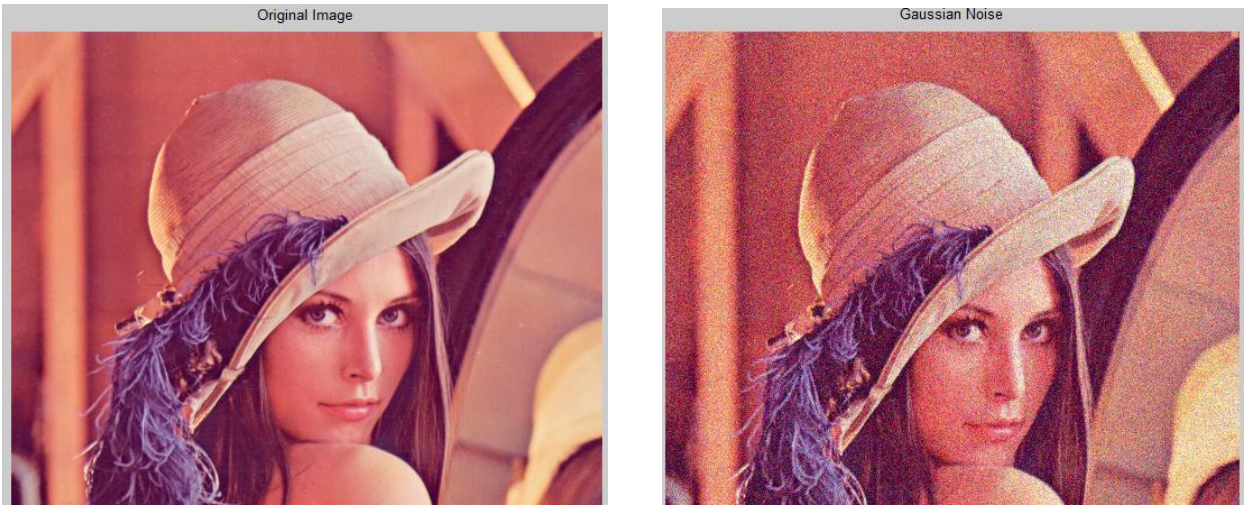


Fig 3.4 Lena image and its Gaussian affected version

3.5.2 POISSON NOISE

Shot noise or Poisson noise is a type of electronic noise which can be modeled by a Poisson process. In electronics shot noise originates from the discrete nature of electric charge. Shot noise also occurs in photon counting in optical devices, where shot noise is associated with the particle nature of light. Shot noise may be dominant when the finite number of particles that carry energy (such as electrons in an electronic circuit or photons in an optical device) is sufficiently small so that uncertainties due to the Poisson distribution, which describes the occurrence of independent random events, are of significance. It is important in electronics, telecommunications, optical detection, and fundamental physics.

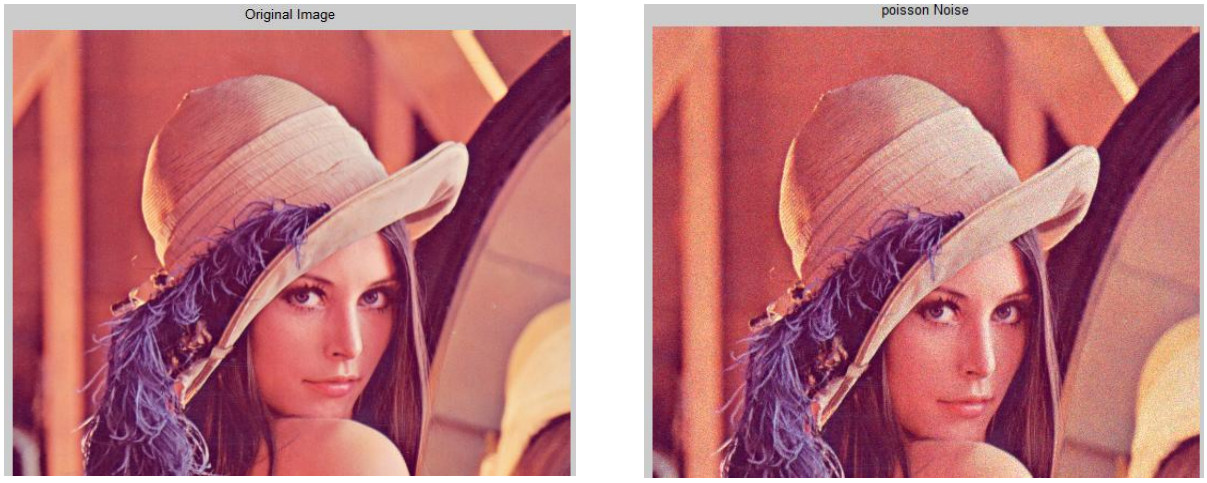


Fig 3.5 Lena image and its Poisson affected version

3.7.3 IMPULSE NOISE

Impulse noise is caused by malfunctioning pixels in camera sensors, faulty memory locations in hardware, or transmission in a noisy channel. Two common types of impulse noise are the salt-and-pepper noise and the random-valued noise. For images corrupted by salt-and-pepper noise (respectively, random-valued noise), the noisy pixels can take only the maximum and the minimum values (respectively, any random value) in the dynamic range. There are many works on the restoration of images corrupted by impulse noise for instance, the nonlinear digital filters. The median filter was once the most popular nonlinear filter for removing impulse noise because of its good denoising power and computational efficiency. However, when the noise level is over 50%, some details and edges of the original image are smeared by the filter. The other names of salt and pepper noise are fat-tail distributed noise, spike noise. An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions. This type of noise can be caused by analog-to-digital converter errors, bit errors in transmission, etc. It can be mostly eliminated by using dark frame subtraction and interpolating around dark/bright pixels.

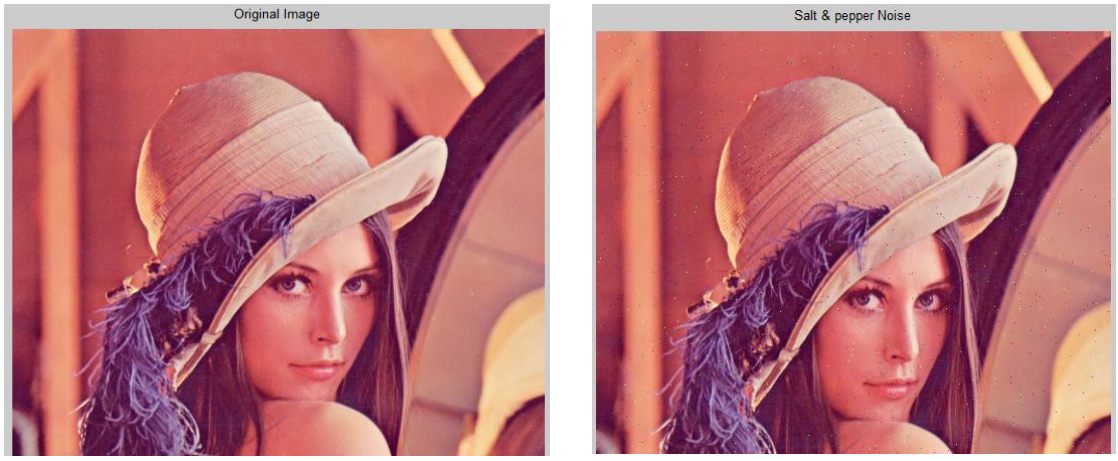


Fig 3.6 Lena image and its Salt & Pepper affected version

3.7.4 IMAGE ROTATION

Image rotation is performed by computing the inverse transformation for every destination pixel. Output pixels are computed using bilinear interpolation. RGB images are computed by evaluating one color plane at a time. There are no gamma corrections so purists might want to correct for image gamma before and after rotation.

The rotation operator performs a geometric transform which maps the position (x_1,y_1) of a picture element in an input image onto a position (x_2,y_2) in an output image by rotating it through a user-specified angle θ about an origin O. In most implementations, output locations which are outside the boundary of the image are ignored. Rotation is a special case of affine transformation. The rotation operator performs a transformation of the

$$x_2 = \cos(\theta) *(x_1-x_0)-\sin(\theta)*(y_1-y_0)+x_0 \quad (3.15)$$

$$y_2 = \sin(\theta)*(x_1-x_0)+\cos(\theta)*(y_1-y_0)+y_0 \quad (3.16)$$

Where (x_0,y_0) are the coordinates of the center of rotation (in the input image) and θ is the angle of rotation with clockwise rotations having positive angles.

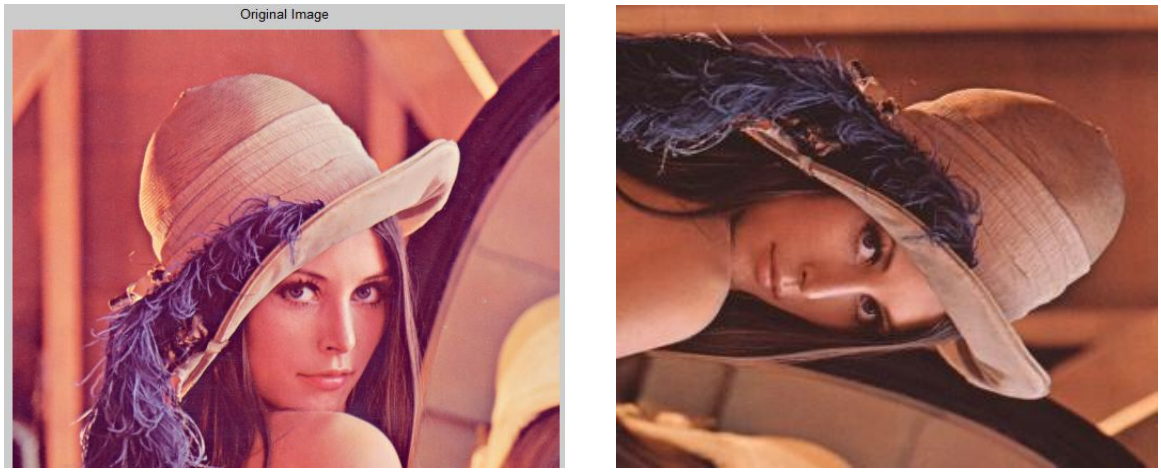


Fig 3.7 Lena image and its Clock wise rotated version

3.7.5 IMAGE SCALING

Image scaling is the process of resizing a digital image. Scaling is a non-trivial process that involves a trade-off between efficiency, smoothness and sharpness. With bitmap graphics, as the size of an image is reduced or enlarged, the pixels that form the image become increasingly visible, making the image appear "soft" if pixels are averaged, or jagged if not. With vector graphics the trade-off may be in processing power for re-rendering the image, which may be noticeable as slow re-rendering with still graphics, or slower frame rate and frame skipping in computer animation.

3.7.6 IMAGE CROPPING

Cropping refers to the removal of the outer parts of an image to improve framing, accentuate subject matter or change aspect ratio. Depending on the application, this may be performed on a physical photograph, artwork or film footage, or achieved digitally using image

editing software. The term is common to the film, broadcasting, photographic, graphic design and printing industries. It is not possible to "un crop" a cropped image unless the original still exists or undo information exists: if an image is cropped and saved (without undo information), it cannot be recovered without the original.

Fig 3.8 Lena image and its Cropped version

CHAPTER 4

RESULTS AND DISCUSSIONS

The various performance metrics of the proposed method has been evaluated and compared the results with other techniques such as LSB substitution, genetic algorithm and other existing techniques. Matlab 7 has been used for the implementation of our technique. In the implementation, five standard gray scale images of size 512x512 have been used to hide secret data of 96 KB using this method. The input cover image is divided into 8x8 sized blocks and Firefly Algorithm is applied block wise to obtain best pixel locations in each block. Each block of a cover image is used to hide 24 bits of the input secret data. The value of weighting constant used in firefly algorithm is chosen experimentally to be 0.5.

The various performance metrics are

(i) Peak Signal to Noise Ratio (PSNR)
(ii) Mean Structural Similarity Index (MSSIM)
(iii) Average difference
(iv) Structural Content (SC)
(v) Image Fidelity
(vi) Correlation Coefficient

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

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

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

Mean Structural Similarity Index (MSSIM) is defined as:

$$MSSIM = 1/M \{ \sum_{j=1}^{M} SSIM(Xj, Yj) \} \quad (4.2)$$

Where M is the number of blocks in the image and $SSIM(X_j, Y_j)$ is calculated using eq 3.12.

Average Difference (AD) is defined as:

$$\sum_{j=1}^{M} \sum_{K=1}^{N} \left[X(j,k) - \hat{X}(j,k) \right] \Big/ MN \quad (4.3)$$

Where X(j,k) and X^(j,k) are the cover image and reconstructed image blocks.

Structural Content (SC) is defined as:

$$SC = \sum_{j=1}^{M} \sum_{k=1}^{N} X(j,k)^2 \Big/ \sum_{j=1}^{M} \sum_{k=1}^{N} \hat{X}(j,k)^2 \quad (4.4)$$

Where X(j,k) and X^(j,k) are the cover image and reconstructed image blocks.

Image Fidelity (IF) is defined as:

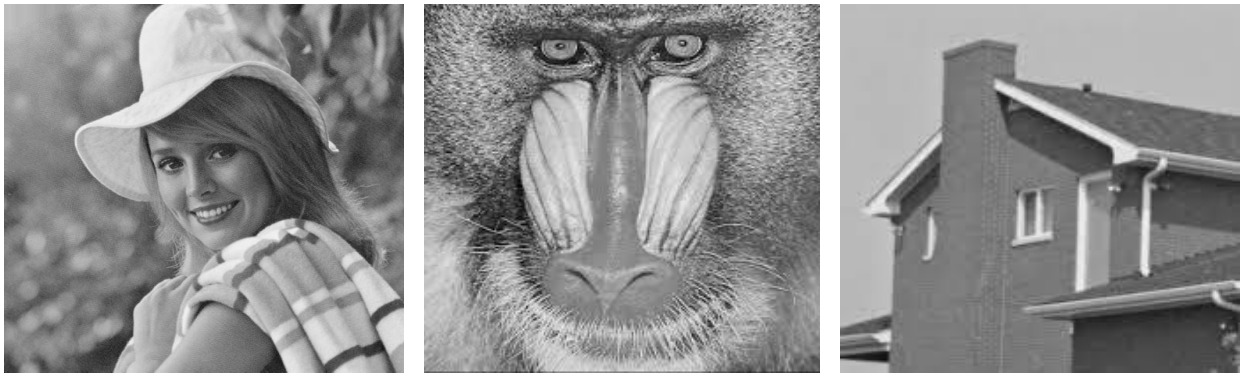
$$IF = 1 - \sum_{j=1}^{M}\sum_{K=1}^{N}\left[X(j,k) - \hat{X}(j,k)^2 \right] \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N}\left[X(j,k)^2 \right] \quad (4.5)$$

Where X(j,k) and X^(j,k) are the cover image and reconstructed image blocks.

Normalized Correlation Coefficient (NK) is defined as:

$$NK = \sum_{j=1}^{M}\sum_{K=1}^{N}\left[X(j,k)\,\hat{X}(j,k) \right] \Big/ \sum_{j=1}^{M}\sum_{k=1}^{N}\left[X(j,k)^2 \right] \quad (4.6)$$

Where X(j,k) and X^(j,k) are the cover image and reconstructed image blocks.
Normally AD, SC, IF and NK are in the range of 0 to1. SC, IF and NK very near to or one is the best and AD should be zero.



(a) (b) (c)

(d) (e)

Fig 4.1 Cover Image (a) Elaine, (b) Baboon, (c) House, (d) Lake, and (e) Lena.

Tables 4.1 and 4.2 list the comparative PSNR and MSSIM values respectively between cover and stego images for all the techniques. These results are further illustrated by graphs in Fig. 4.2. It can be clearly seen that the proposed technique outperforms the other techniques because embedding the secret data in FA generated locations results in minimum distortion of

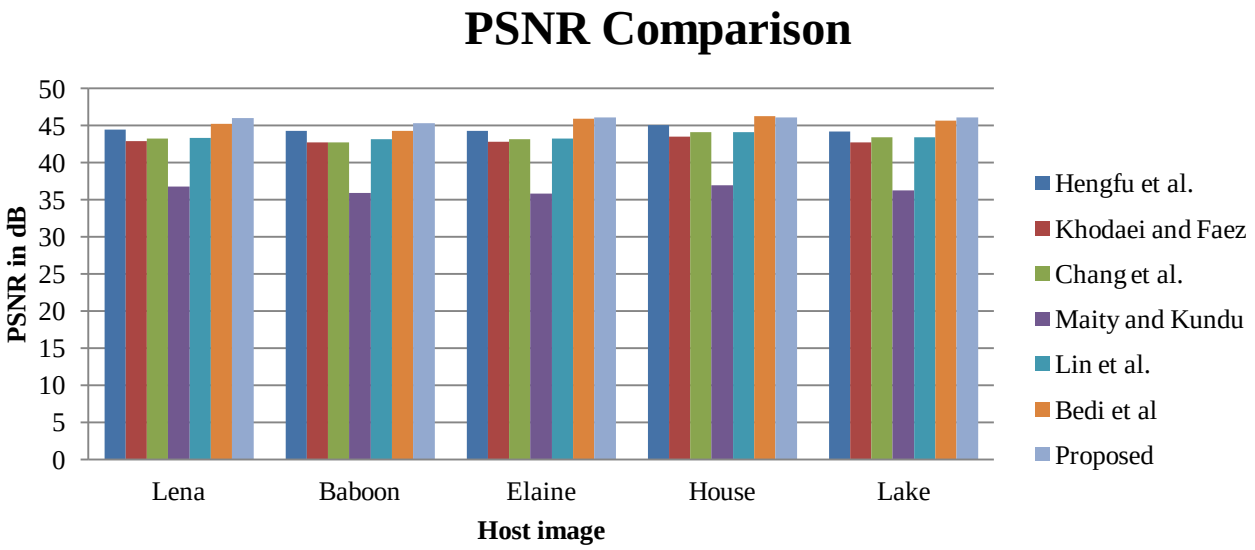
the cover image and thus produces a good quality stego image. Although, the histogram based embedding method results in a stego image which is good in quality. The techniques proposed by Khodaei and Faez and Chang et al. have good data embedding capacity, but lack robustness. The technique proposed by Maity and Kundu results in a stego image of lower quality as it works better when the amount secret embedded data is low in which case it exhibits good tolerance to distortions in the stego image.

S. No	Host image	Hengfu et al. method	Khodaei and Faez method	Chang et al. method	Maity and Kundu method	Lin et al. method	Bedi et al method	Proposed method
1	Lena.png	44.43	42.87	43.24	36.75	43.31	45.19	45.9708
2	Baboon.jpg	44.31	42.71	42.75	35.89	43.18	44.31	45.2927
3	Elaine.png	44.24	42.79	43.19	35.81	43.22	45.93	46.0392
4	House.jpg	45.04	43.46	44.08	36.92	44.11	46.28	46.0410
5	Lake.jpg	44.17	42.76	43.39	36.22	43.42	45.67	46.0469

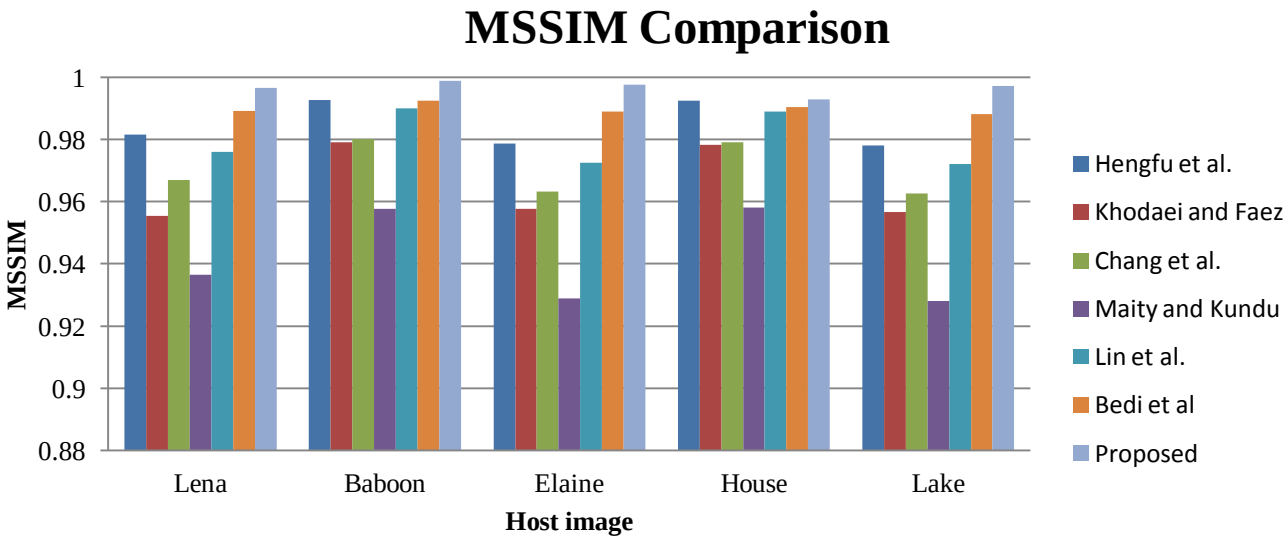
Table 4.1 PSNR in dB obtained after embedding the secret data of 96 KB in different cover images at an angle of rotation α=120.

S. No	Host image	Hengfu et al. method	Khodaei and Faez method	Chang et al. method	Maity and Kundu method	Lin et al. method	Bedi et al method	Proposed method
1	Lena.png	0.9815	0.9554	0.9669	0.9365	0.9760	0.9892	0.9966
2	Baboon.jpg	0.9928	0.9792	0.9802	0.9578	0.9901	0.9926	0.9989
3	Elaine.png	0.9787	0.9576	0.9633	0.9289	0.9725	0.9890	0.9977
4	House.jpg	0.9925	0.9782	0.9792	0.9581	0.9891	0.9905	0.9929
5	Lake.jpg	0.9781	0.9566	0.9626	0.9281	0.9721	0.9882	0.9973

Table 4.2 MSSIM obtained after embedding the secret data of 96 KB in the different cover images at an angle of rotation α=120.



(a)



(b)

Fig 4.2 Comparison of (a) PSNR and (b) MSSIM values obtained from various techniques when secret data is embedded in host images Lena, Baboon, Elaine, House and Lake.

Fig 4.3 shows the performance evaluation of this algorithm by comparing it with five recent algorithms of Hu et al., Luo et al., Li et al., Hong and Zeng et al. for standard 512 × 512 sized gray-scale images: Lena, Baboon. According to the figure, it is clear that the proposed algorithm achieves a better performance compared with other state-of-the-art works. It provides a larger PSNR whatever the test image or embedding rate is.

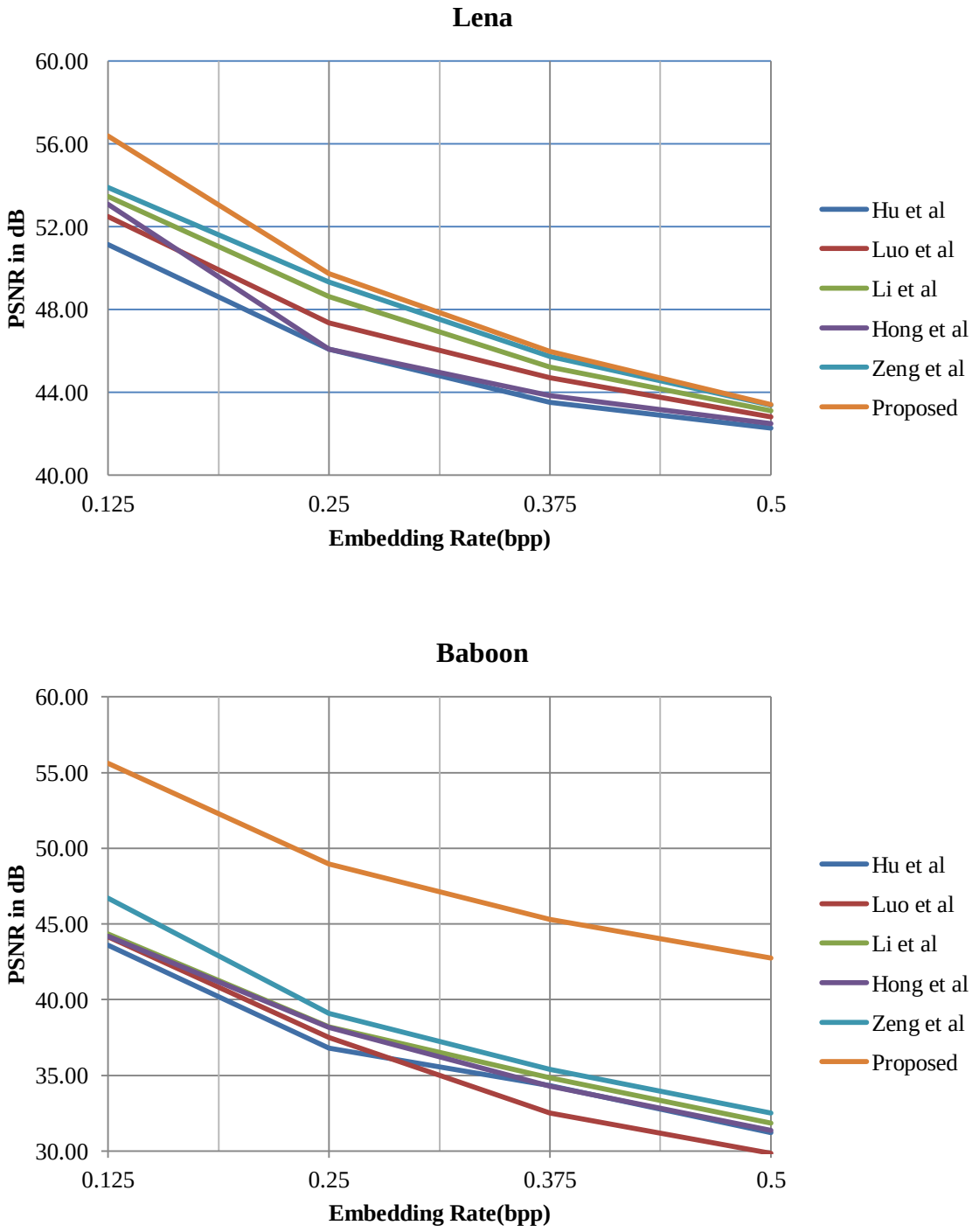


Fig 4.3 Performance comparison between the Proposed, Hu et al., Luo et al., Li et al., Hong and Zeng et al.

Table 3 lists the PSNR and MSSIM values of Lena image for different angle of rotation. From the Table 3 the angle of rotation 315 degree provides better result. Table 4 lists the other performance metrics like Average Difference, Structural Content, Image Fidelity, Normalized Correlation coefficient. From the Table 4 it is clear that the proposed method gives better result.

S.No	Angle in degree	PSNR in dB	MSSIM
1	10	45.9360	0.9966
2	25	46.4334	0.9966
3	45	46.4990	0.9956
4	65	46.4494	0.9956
5	85	46.4379	0.9955
6	100	45.9708	0.9960
7	120	45.9708	0.9966
8	135	46.4439	0.9966
9	225	46.4649	0.9955
10	315	46.5200	0.9956

Table 4.3 PSNR and MSSIM values of Lena image for different angle of rotation

Cover Image	Avg Difference	Structural Content	Image Fidelity	Correlation coefficient
Lena.png	0.0000	1.0000	1.0000	1.0000
Baboon.jpg	0.0000	1.0000	1.0000	1.0000
Elaine.png	0.0000	1.0000	1.0000	1.0000
House.jpg	0.0000	1.0000	1.0000	1.0000
Lake.jpg	0.0000	1.0000	1.0000	1.0000

Table 4.4 Performance Metrics

CHAPTER 5

CONCLUSION AND FUTUREWORK

5.1 Conclusion

An efficient reversible data hiding scheme using FRFT and Firefly Algorithm for hiding secret data into cover image has been proposed. This technique can be utilized for hiding a secret data inside an image for covert communication. The cover image has been converted into frequency domain using FRFT and FA was used for finding the best pixel locations in that cover image for hiding the secret data in such a way that the stego image produced was good in quality as well as tolerant to distortions during transmission even at a high embedding rate. The best location has been chosen by objective function which is the combination of Mean Structural Similarity Index (MSSIM) and Bit Error Rate (BER). The pixel locations selected by FA were used to embed secret data via histogram shifting. The gray image used as cover medium can be retrieved with high quality. Peak Signal to Noise Ratio (PSNR), Mean Structural Similarity Index (MSSIM), Average difference, Structural Content (SC), Image Fidelity and Correlation Coefficient has been evaluated and compared with the other reversible data hiding techniques. PSNR, SNR and MSSIM index have been used to measure the stego image quality and BER is used measure the quality of the extracted secret image. The results obtained show the effectiveness of the presented technique in producing better quality stego images and in recovering secret data and cover medium.

5.2 Future work

This project can be extended by using neural networks algorithm to get more accuracy and more information capacity. The image can also be used as the message to be embedded in the carrier image. Parameters like maximum capacity of the message that can be embedded in the image, accuracy can be found using other optimization algorithms and comparison can be done.

REFERENCES

[1] B.Jagadeesh, S.Srinivas Kumar and K.Raja Rajeswari, "Image watermarking scheme using singular value decomposiion, quantization and genetic algorithm", International Conference on Signal Acquisition and Processing, 2010

[2] Che-Wei Lee and Wen-Hsiang Tsai, "A lossless large-volume data hiding method based on histogram shifing using an optimal hierarchical block division scheme", Journal Of Information Science And Engineering XX

[3] Chi-Kwong Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition 37 (2004) 469 – 474

[4] Ching-Sheng Hsu and Shu-Fen Tu, "Finding optimal LSB substitution using ant colony optimization algorithm", Second International Conference on Communication Software and Networks, 2010

[5] Ehsan Vahedi, Caro Lucas , Reza Aghaeizade Zoroofi and Mohsen Shiva, "A new approach for image waermarking by using particle swarm optimization", IEEE International Conference on Signal Processing and Communications (ICSPC 2007), 24-27 November 2007

[6] Guorong Xuan, Yun Q. Shi, Zhicheng Ni, Peiqi Chai , Xia Cui and Xuefeng Tong, "Reversible data hiding for JPEG images based on histogram pairs4th International Conference, ICIAR 2007, Montreal, Canada, August 22-24, 2007. Proceedings, 2007

[7] Hengfu YANG, Xingming SUN and Guang SUN, "A high-capacity image data hiding scheme using adaptive LSB substitution", Radioengineering, vol. 18, no. 4, december 2009

[8] Jun Tian, "Reversible Data Embedding Using a Difference Expansion", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 13, No. 8, August 2003

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

[10] Lingling An, Xinbo Gao, Cheng Deng, and Feng Ji, "Reversible watermarking based on staistical quantity histogram", IEEE Transactions on Image Processing, Vol 21, Mar 2012

[11] M. Fallahpour and M.H. Sedaagi, "High capacity lossless data hiding based on histogram modification", IEICE Elecronics Epress, Vol.4, N0.7, 205-210

[12] 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

[13] 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

[14] 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

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

[16] 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

[17] 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

[18] S. Picek and M. Golub, “On evolutionary computation methods in cryptography,” MIPRO, 2011 Proceedings of the IEEE 34th International Convention, May 2011

[19] Saibal K. Pal, C.S Rai and Amrit Pal Singh, “Comparative sudy of firefly algorithm and particle swarm optimization for noisy non-linear optimization problems”, I.J. Intelligent Systems and Applications, 2012, 10, 50-57, September, 2012

[20] Sayan Chakraborty, Sourav Samanta, Debalina Biswas, Nilanjan Dey, and Sheli Sinha Chaudhuri, “Particle swarm optimization based parameter optimization technique in medicalinformation hiding”, IEEE International Conference on Computational Intelligence and Computing Research, 2013

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

[22] 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

[23] 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

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

[25] 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

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

[27] Zhicheng Ni, Yun Q. Shi, Nirwan Ansari and Wei Su, “Reversible data hiding”, ISCAS '03 IEEE Transactions On Circuits And Systems, Vol. 2, May 2003

LIST OF PUBLICATIONS

- Presented a paper titled "*An Efficient Data Hiding Scheme using Firefly Algorithm in Spatial Domain* " in *IEEE* sponsored 2nd International Conference on Electronics and Communication Systems (ICECS) on 26th and 27th February 2015 held at Karpagam college of engineering, Coimbatore.