I. J. Mathematical Sciences and Computing, **2020, 4, 42-69**
Published Online August 2020 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmsc.2020.04.05

Comparative Analysis of Steganography Technique for Information Security

Pooja Yadav
J.C. Bose University of Science and Technology, YMCA Faridabad
E-mail: poojayadav137@gmail.com

***Sangeeta Dhall**
J.C. Bose University of Science and Technology, YMCA Faridabad
E-mail: sangeeta_dhall@yahoo.co.in

Received: 03 May 2019; Accepted: 13 May 2020; Published: 08 August 2020

Abstract: Organisations need information security to reduce the risk of unauthorized information disclosure, use, modification and destruction. To avoid this risk and ensure security diverse solutions are available such as Cryptography, Steganography and Watermarking. Encryption changes the form of information but latter two hide records or watermark in some medium. This paper is an effort to explore one of the solutions i.e. Steganography. It is a mechanism of hiding secret information in text, image, audio or video carriers. Broadly, these are classified in various categories such as Spatial domain, Transform domain and Distortion Technique. This work intends to give an overview of above mentioned techniques in detail by comparing algorithms based on performance metrics such as Bhattacharyya Coefficient, Correlation Coefficient, Intersection Coefficient, Jaccard Index, MAE, MSE, PSNR and UIQI. After analysing the MATLAB simulation and comparison based on different performance metrics, LSB Substitution and Pseudorandom technique are best suited for generating highly matched stego image with respect to their cover image.

Keywords: Information Security, MATLAB, Performance Metrics, Steganography Mechanism.

1. INTRODUCTION

Now-a-days data is the most precious aspect of today's business, so it needs security to minimize the risk to a level that is acceptable to the organisations. Top industries spend billions of dollars to secure their networks and keep the business-related data safe and secure. All businesses in this world are dependent on computers for controlling the large money transfers between banks, insurance, markets, medical field and satellites [7, 8]. In military application also information security plays a vital role because of the transfer confidential data from one place to another place securely. So information security is the need of today's lives for transferring data from sender end to receiver end without any disturbance and loss. Also in medical field there is a growing requirement to secure patient's medical information since we see an upward trend in number of related data breaches from 2009-2018 as shown below in Fig.1.

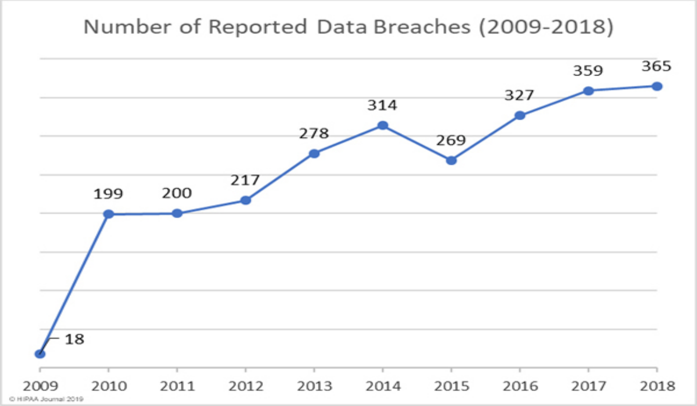

Fig.1. U.S. Department of Health and Human Services Office for Civil Rights statistics [8]

Information Security is the practice of preventing unauthorised access, disclosure, disruption, use, modification, inspection, recording and destruction of information. That information may be physical or electronic one. Information can be anything like data in mobile phone, profile on social media, biometric and any confidential information regarding any field [1, 6]. Cryptography, Watermarking, Mobile Computing and Cyber Forensics etc. are the available solution for data hiding to protect confidential data from deceivers, hackers and spies. There are three main concerns of Information Security system, commonly known as CIA.

- Confidentiality
- Integrity
- Availability

a) Confidentiality: Confidentiality means information is not disclosed to any unauthorized Individuals and entities.
b) Integrity: Integrity means maintaining the completeness and accuracy of the data which is been processed to transfer from sender end to receiver end. This means data cannot be edited and modified by any unauthorised way.
c) Availability: Availability means information or data must be available when needed. It clearly means data must be available when needed.

To address above mentioned concerns, Steganography plays a vital role since it reduces the risk of unauthorized access and enables movement of information from sender end to receiver end without any loss. Some of the desirable features of good steganography schemes are enlisted below:

- ➢ Imperceptibility: It evaluates the quality of the stego-image with respect to the original or cover image after the embedding secret information. Visual inspection of snapshots of images prior to and following embedding is the gauge of this property.
- ➢ Robustness: It is a significant parameter to access a steganography technique, and it can be computed by measuring the Peak Signal to Noise Ratio (PSNR), Mean Absolute Error (MAE) and Mean Square Error (MSE).
- ➢ Security: The security analysis of a method is done by evaluating the pixel values, possibility allotment and histograms between the cover and stego image. Diverse parameters used to assess the security are Jaccard index, UIQI, Bhattacharya coefficient, etc.
- ➢ Information Retrieval: It checks the correspondence between the retrieved and actual secret information.

For a system to be secured these factors should have optimum values. This paper surveys various steganography schemes available in literature and does an thorough

Investigation by the factors mentioned above.

The whole paper is organized as follows: Section II provides literature survey; Section III gives the description of basic steganography technique along with its classifications. Section IV describes basic terminology along with classification based on domain, considered for implementation. Section V describe algorithm and block diagram of each implemented mechanism. Section VI shows simulation set up parameters and performance metrics, Section VII gives Snapshots and results of analysis and Section VIII depicts the conclusion which is followed by references.

2. LITERATURE SURVEY

Table 1 provides list of relevant review papers already implemented by researchers. This table provides detail regarding techniques implemented and comparison criterion taken along with key features.

Table 1. Literature Survey

S.No.	Research Name	Author/ Year	Domain	Techniques Surveyed	Comparison Criterion	Features
1	A review on Steganography Techniques	Jasleen Kour and Deepankar Verma(2014)	Spatial/ Transform	LSB Substitution, DCT	1)Robustness - PSNR, MSE, SNR 2) Payload Capacity 3)Imperceptibility	This paper emphasize on 1) Hiding the existence of data so that no one can detect its presence. 2) Secrecy is achieved by embedding data into cover image and generating a stego-image.
2	Review Paper on different methodology of steganography based data hiding	S. Uma Maheswari and D.Jude Hemanth (2015)	Spatial/ Frequency	LSB Substitution, DCT and DWT	1)Imperceptibility 2) Embedding capacity 3) Computational complexity	This paper emphasize on some of the key issues of the Image Steganography such as Imperceptibility, Embedding capacity, Robutness and Computational complexity. 1) Saptial domain techniques having low computational complexity and robustness with high embedding capacity and medium imperceptibility. 2) Frequency domain techniques having low computational complexity and embedding capacity with high robustness and imperceptibility.
3	Review Paper on Image Steganography Techniques	Mohammed A. Saleh (2018)	Spatial	LSB Substitution	Robustness - PSNR	This paper emphasize on improving security of LSB Substitution technique in which 1) Messages are encrypted using Advanced Encryption Standard (AES), thus making it harder for unauthorized people to extract the original message. 2) But it is restricted merely to BMP and PNG image formats, and it uses a sharable text key. 3) It does not provide an encryption for neither for a secret data, nor for a shareable key. 4) In DWT method, which has a negative impact on performance
4	Comparative study of Image Steganography Techniques	Himanshu Arora and Cheshta Bansal (2018)	Spatial/ Transform	LSB Substitution, DCT and DWT	1) Robustness-PSNR, MSE 2) Perceptual Transparency 3)Temper Resistance 4) Computational Complexity	This paper emphasize on the integrity of hidden image is of 1) High capacity 2) High PSNR ratio 3) Integrity of stego image inside the cover image. Drawbacks – 1) In Spatial domain, High extra bit of signature with hidden message. 2) In Transform domain, Noticable artifact of hidden data and low computational complexity in transform domain.

5	A literature Review on Various Recent Steganography Techniques	Anupriya Arya and Sarita Soni (2018)	Spatial/ Transform	LSB Substitution, DCT, DWT and Distortion Technique	1)Computational Complexity 2) Payload 3) Embedding Capacity	This paper focus on hiding the secret or confidential message in an original file so that it is Unintelligible to an interceptor. 2) And addressed the concept of embedding the secret message into an image using LSB technique and then applied AES algorithm to provide better security.
6	A Review on Steganography Techniques	Wafaa Mustafa Abdullaha and Abdul Monem S. Rahmab (2016)	Transform	DCT, DWT and SVD	1)Imperceptibility 2) Robustness	This paper presents numerous steganographic techniques that have been recently proposed for hiding the secret data within the cover-images efficiently and obtained efficient results in terms of image quality but the capacity was limited. Drawbacks – 1) Spatial domain techniques have low level of security. 2) Transform domain schemes restricted with low embedding capacity. 3) The quality of the stego-image is an essential aspect which is constrained with the embedding capacity.
7	A Survey Paper on Stegnaograhy Techniques	Dr. Rajkumar L Biradar and Ambika Umashetty	Spatial/ Transform	LSB DCT, DWT AND DFT or FFT	1) Robustness 2)Perceptual Transparency 3) Temper Resistance 4) Computational Complexity	This paper emphasize on different proposed techniques which show that 1) visual quality of the image is degraded when hidden data increased up to certain limit using LSB based methods. 2) Many of the embedding techniques can be broken or shows indication of alteration of image by careful analysis of the statistical properties of noise or perceptually analysis.

As observed from Table 1, existing papers in literature have given limited details of steganography techniques. Thus, this work aims for the following offerings.

- An attempt is made to wrap up most of the mechanisms classify on the basis of domain. i.e., spatial and frequency to surge security of data.
- Several performance metrics are used for different types of analysis to get the best Technique. Robustness analysis (MSE, MAE, PSNR), Security analysis (Jaccard Index, Correlation coefficient, Intersection Coefficient, Bhattacharya coefficient, UIQI) and Imperceptibility analysis.
- After analyzing all consideration superlative technique is identified for different types of parameters, to facilitate researchers to select the mechanism as per strengths, in given applications.

3. Steganography

Steganography is the technique of hiding the secret data by embedding it into an audio, video, image or text file used as a carrier object. It is not only the art of hiding data but also hiding the fact of transmission of message [6]. Steganography hides the secret data in other file in such a way that only the recipient knows the existence of the secret message. The word steganography combines the Greek words **stegano** meaning “concealed” and **graphe** meaning “writing”. To transmit steganography secret messages many different carrier formats such as text, image, audio or video can be utilized. Digital images are most popular form of carriers because of huge scope for hiding information in digital images since images can be of megabytes or more and a similar amount of information can be embedded into it.

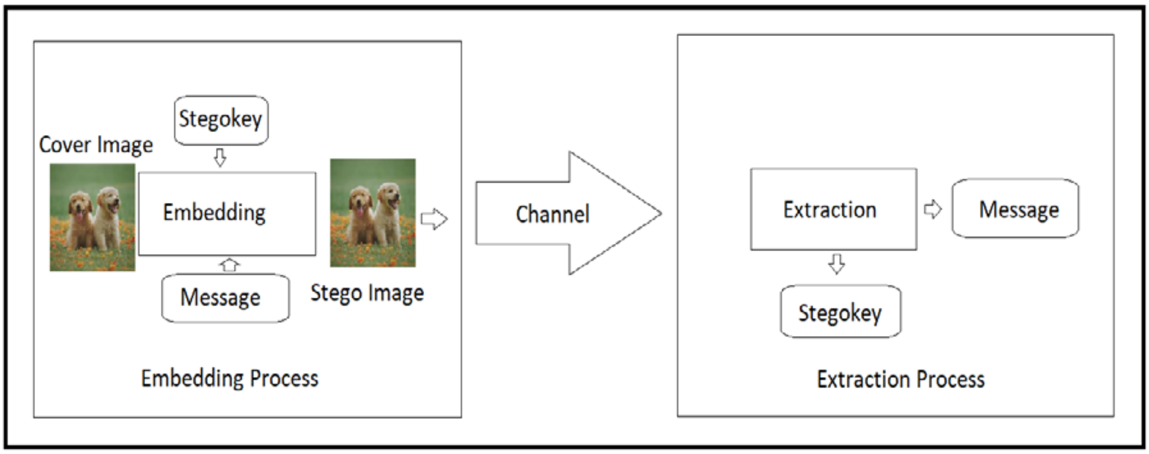

Fig.2. Process of Image Steganography

The process of image steganography includes two parts i.e. embedding process and retrieval process [9]. The embedding and the retrieval process are connecting with a transmission channel to transfer the secret data from sender end to receiver end as shown above in Fig.2.

Embedding process can be defined as the process in which large amount of data is embedded into the original image using embedding algorithm and stego key to produce a stego image which is the combination of cover image and the secret message and retrieval process can be defined as the process in which the secret message is extracted from the stego image using retrieval algorithm and stego key as shown below in Fig.3.

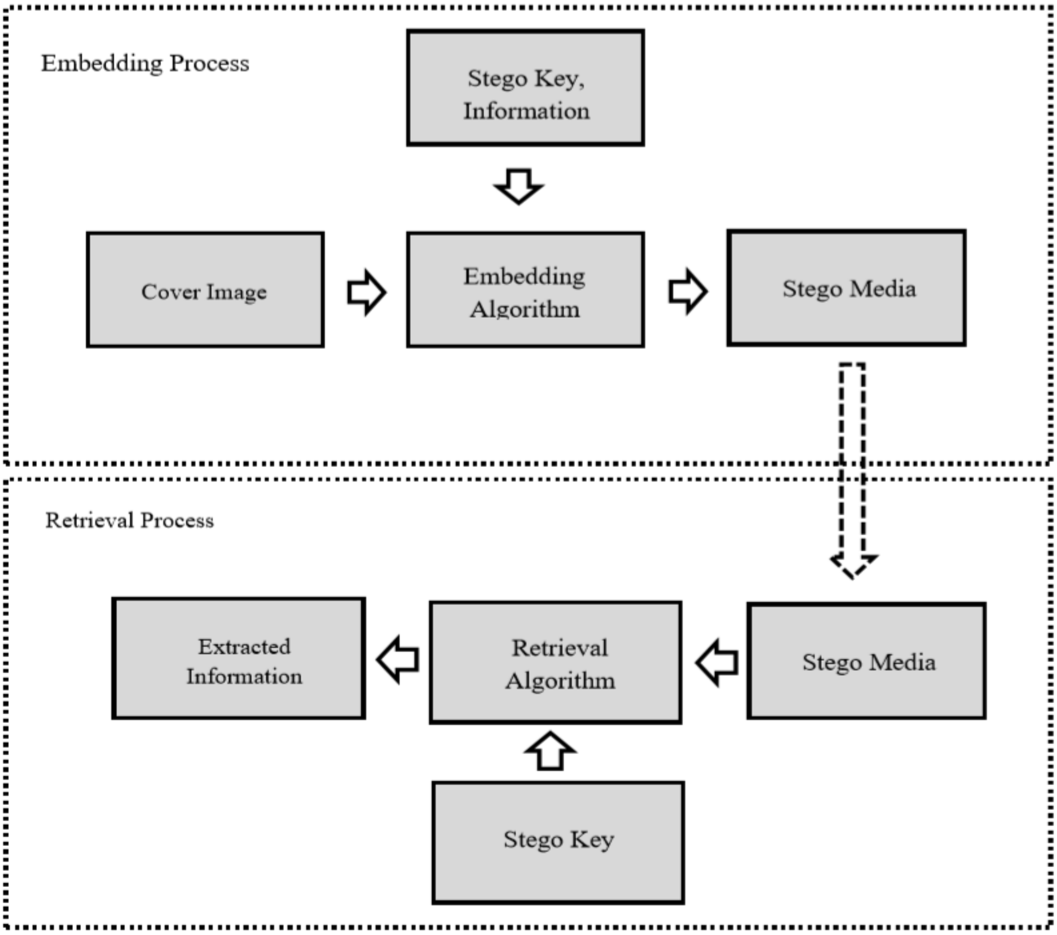

Fig.3. Steganography Process

3.1 Classification of Steganography on the Basis of Cover Media

On the basis of cover media, steganography in divided into five categories such as image steganography, audio steganography, video steganography, text steganography and network steganography as shown in Fig.4.

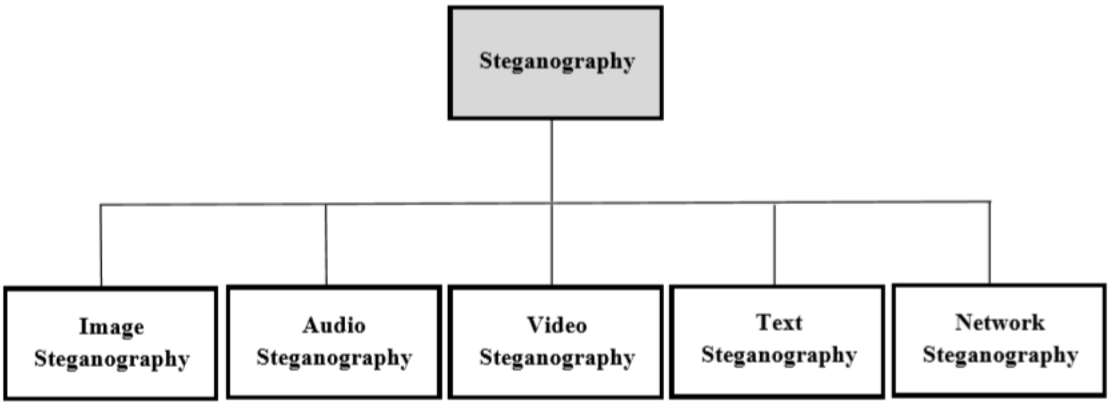

Fig.4. Types of Steganography on the basis of cover media

- **Image Steganography:**

Image Steganography is the technique of hiding the secret data by taking the cover object as image. In this process, the cover image pixel intensities are used to hide the secret data [6,12]. Images are widely as cover image because there are number of bits present in digital representation of an image.

- **Audio Steganography:**

Audio Steganography is the process of hiding the secret data in audio files. This method of Steganography hides the data in WAV, AU and MP3 sound files. There are three different methods of audio steganography [6,7]. These methods are:

a) Low Bit Encoding
b) Phase Coding
c) Spread Spectrum

- **Video Steganography:**

Video Steganography is the technique of hiding any type of data or file into digital video format. In this process, video file is used as carrier for hiding the secret data or information [7,12]. Normally, DCT (discrete cosine transforms) change the values which are used to hide the data in each of the images in the video which is unnoticeable by the human eye. Different formats used by video steganography are H.264, AVI, MPEG and Mp4.

- **Text Steganography:**

Text Steganography is the method of hiding the confidential data or information inside the text files. Using this method, the confidential data or information is hidden behind every nth letter of every words of the text message [6,12]. There are three different methods are used in text steganography. These methods are:

a) Format Based Method
b) Random and Statistical Method
c) Linguistics Method

- **Network Steganography:**

Network Steganography is also called Protocol Steganography. This technique involves hiding the secret data or information by taking the network protocol such as TCP, ICMP, IP and UDP etc., as a cover carrier [7, 12]. Steganography can be used in the OSI layered model because of the existing covert channels is present in it.

4. Image Steganography terminologies

There are four different terminologies used in image processing [10]. These are:

a) **Cover Image**: The original image which is used as a carrier for hiding the secret information.
b) **Message:** The actual message or confidential information which is used to hide into the cover image.
c) **Stego Image**: Embedding the secret message into cover image. The combination of secret message and cover image is called Stego Image.
d) **Stego Key:** A key is used for embedding or extracting the message from the cover image and stego image.

4.1 Different Techniques for Embedding Information

Image Steganography is classified mainly into two different categories such as:

a) Spatial Domain Technique
b) Transform Domain Technique

These two categories are further divided into different sub categories as shown below in Fig.5.

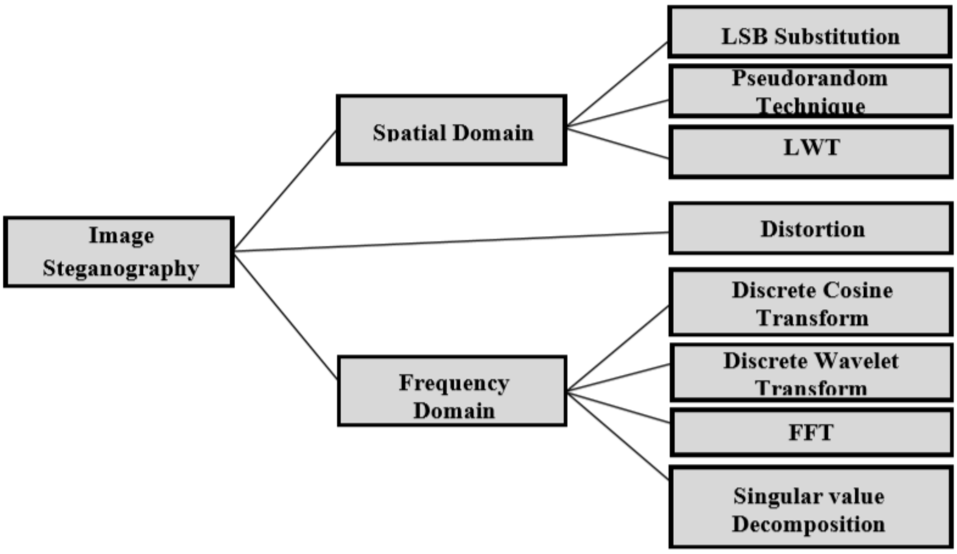

Fig.5. Classification of Image Stenography Technique

4.1.1 Spatial Domain Method

In this domain method of steganography technique, the secret data is directly embedded in the intensity of the pixels [10,17]. It means some of the pixel values of the cover carrier is changed directly during the hiding of the secret data. Spatial domain Technique is classified into following categories:

a) LSB Substitution
b) Pseudorandom Technique
c) Distortion Technique
d) Singular value Decomposition

4.1.2 Transform Domain Technique

In this technique, the secret message is embedded in the frequency domain of the cover image [10,17]. This way of hiding message in a cover image is more complex than others. This technique is broadly classified as:

a) Discrete Fourier Transformation Technique(DFT)
b) Discrete Cosine Transformation Technique(DCT)
c) Discrete Wavelet Transformation Technique(DWT)

5.Algorithms for Implementation of Different Image Steganography Techniques

5.1 Spatial Domain Methods

5.1.1 Least Significant Bit (LSB) Technique

In this technique of steganography, the LSBs of the pixel values of the cover image are modified according to message bits. By modifying the first most right bit of an image we can insert our secret message and it also makes the image unnoticeable, but if our message is too large it will start modifying the second right most bit and so on and an attacker can easily notice the changes in the cover image [1,11,13]. The process is described in Fig.6.

Embedding Algorithm:

1) Read the cover image and the text message which is to be hidden in cover image.
2) Convert the text message to the binary bits.
3) Calculate the LSB of each pixels of the cover image.
4) Replace the LSB of the cover image with each bit of the secret message one by one.
5) Write the stego image.

Retrieving Algorithm：

1) Read the stego image in matrix of pixels values.
2) Access the LSB of pixels of stego image containing the secret message. These bits are combined to form bytes and bytes are combined to form the complete the message bits.
3) In next step each pixel value of stego image is converted into binary.
4) Access the LSB of the image in which secret bits are present.
5) Retrieve the message bits and convert these set of 8-bits into character i.e. text message.
6) Finally, we get the required secret information.

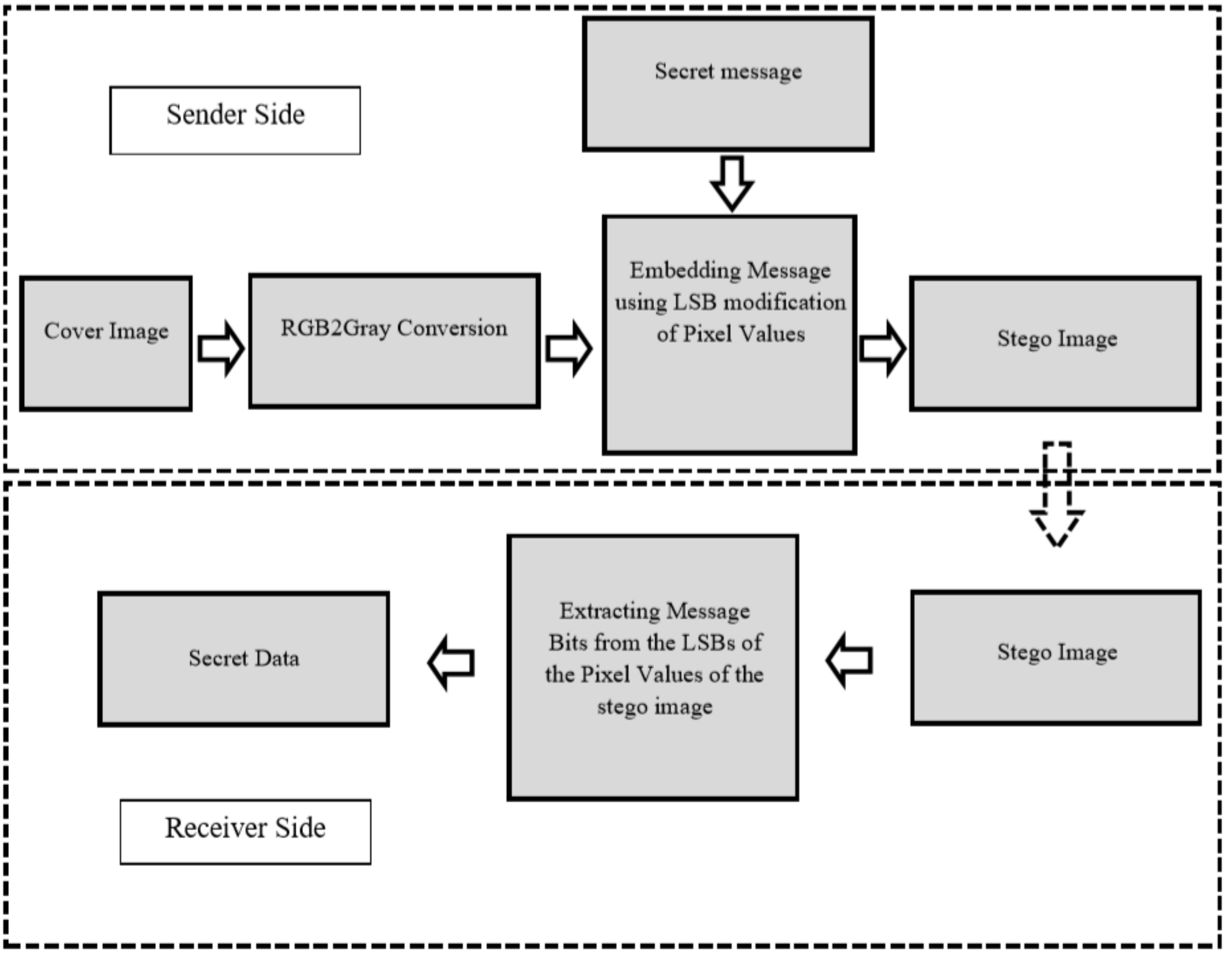
Sender Side
Secret message
Cover Image
RGB2Gray Conversion
Embedding Message using LSB modification of Pixel Values
Stego Image
Stego Image
Extracting Message Bits from the LSBs of the Pixel Values of the stego image
Secret Data
Receiver Side

Fig.6. Flow Diagram for LSB Substitution

5.1.2 Pseudorandom Technique

In this technique of steganography, a pseudorandom number generator is used to embed the secret message over the cover pixels in a random manner. Both the sender end and the receiver end share the stego key as a random number generator. In this process a random sequence is created in which the interval between two embedded bits is determined randomly [1,7,14]. The secret message bits are stored according to the interval between two embedded bits. Complete process is described in Fig.7.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Extract the red plane or any of the planes from the cover image in which message bits.
3) Convert the secret message into the binary bits before embedding into the cover image.
4) Initialize the random key and randomly identify the pixels of the cover image. The initialised random key is basically a seed which is used to generate same set of random values every time that random number generator command is used.
5) Now LSB of the randomly selected pixels will be modified as per the bits of the secret message. So the message bits are stored into the LSB of the cover image.
6) In next step the modified pixel value is fed back to its respective place. According to the size of the message bits the LSBs of the pixels of the cover image are modified.
7) Write the stego image.

Retrieval Algorithm:

1) Read the stego image.
2) Again, initialize the random key as initialized in embedding process and randomly identify the pixels of the cover image. The randomly generated key is basically a seed which is used to generate the same set of random values every time that random number generator command is used.
3) This random key is same at both ends.

4) Read the LSB of each identified pixel of the stego image.
5) Now these bits are combined to form the complete secret message.
6) Convert each 8 bits into character i.e. text message.
7) Finally, we get the require text message

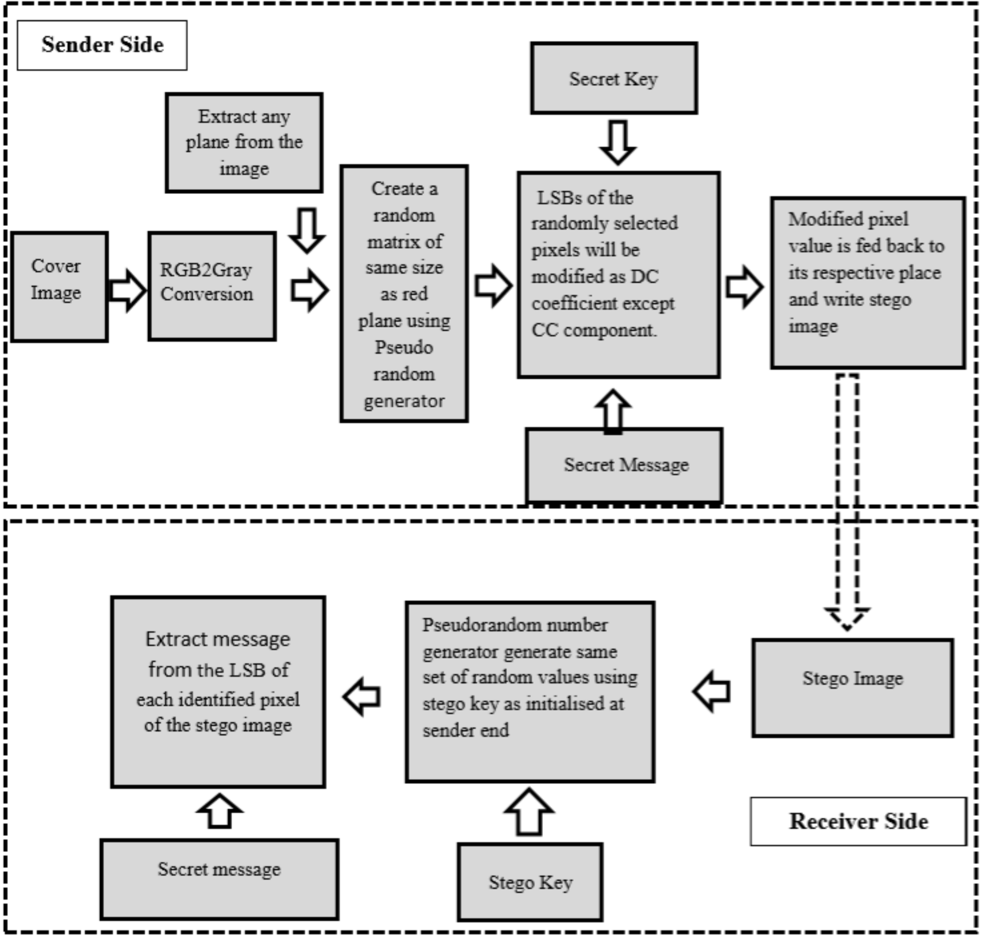
Sender Side
Extract any plane from the image
Secret Key
Cover Image
RGB2Gray Conversion
Create a random matrix of same size as red plane using Pseudo random generator
LSBs of the randomly selected pixels will be modified as DC coefficient except CC component.
Modified pixel value is fed back to its respective place and write stego image
Secret Message
Extract message from the LSB of each identified pixel of the stego image
Pseudorandom number generator generate same set of random values using stego key as initialised at sender end
Stego Image
Receiver Side
Secret message
Stego Key

Fig.7. Flow Diagram for Pseudorandom Technique

5.1.3 Distortion Technique

The distortion method is used to store the secret data by distorting the signal. In this technique modification in LSB of the pixel value is performed if the value of the secret bit is 1 else pixel value will remain unchanged. This technique choose the same approach as pseudorandom technique in which different cover pixels are used for hiding the secret message [1,7]. An encoder applies a sequence of modification to the cover image and the decoder phase decodes the encrypted data to the original data with the secret bits using some secret key. Complete process is described in Fig.8.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Convert the secret message into the binary bits before embedding into the cover image.
3) Initialize the random key and randomly identify the pixels of the cover image. The initialised random key is basically a seed which is used to generate same set of random values every time that random number generator command is used.
4) Each message bit is checked sequentially.
5) LSB of the randomly selected pixel will be modified as per given conditions:
    a) If secret bit=1 then;
    b) Pixel value is checked, if pixel value< 128;
    c) Increase pixel value by x where x= 1.
    d) If pixel value >=128, decrease pixel value by x.

6) Insert the message bits in the LSB of the any of the plane's pixel. This modified pixel value is fed back to its respective position.
7) As per the size of the message data LSB of image pixels are modified.

8) Write the stego image.

Retrieve Algorithm:

1) Read the stego image.
2) Again initialize the random key as initialized in embedding process and randomly identify the pixels of the cover image. The randomly generated key is basically a seed which is used to generate the same set of random values every time that random number generator command is used.
3) This random key is same at both ends.
4) Calculate the difference of pixel value of each identified pixel of stego image and cover image,
5) The secret message bit is retrieved as per given conditions:
    a) If difference is equal to zero then secret bit =0;
    b) Otherwise if difference =1, then secret bit= 1.
6) Extract the message bit from the LSBs of the pixels of the given plane.
7) Combine the bits to form a complete message.
8) Convert each 8 bits into character i.e. text message.
9) Finally, we get the require text message.

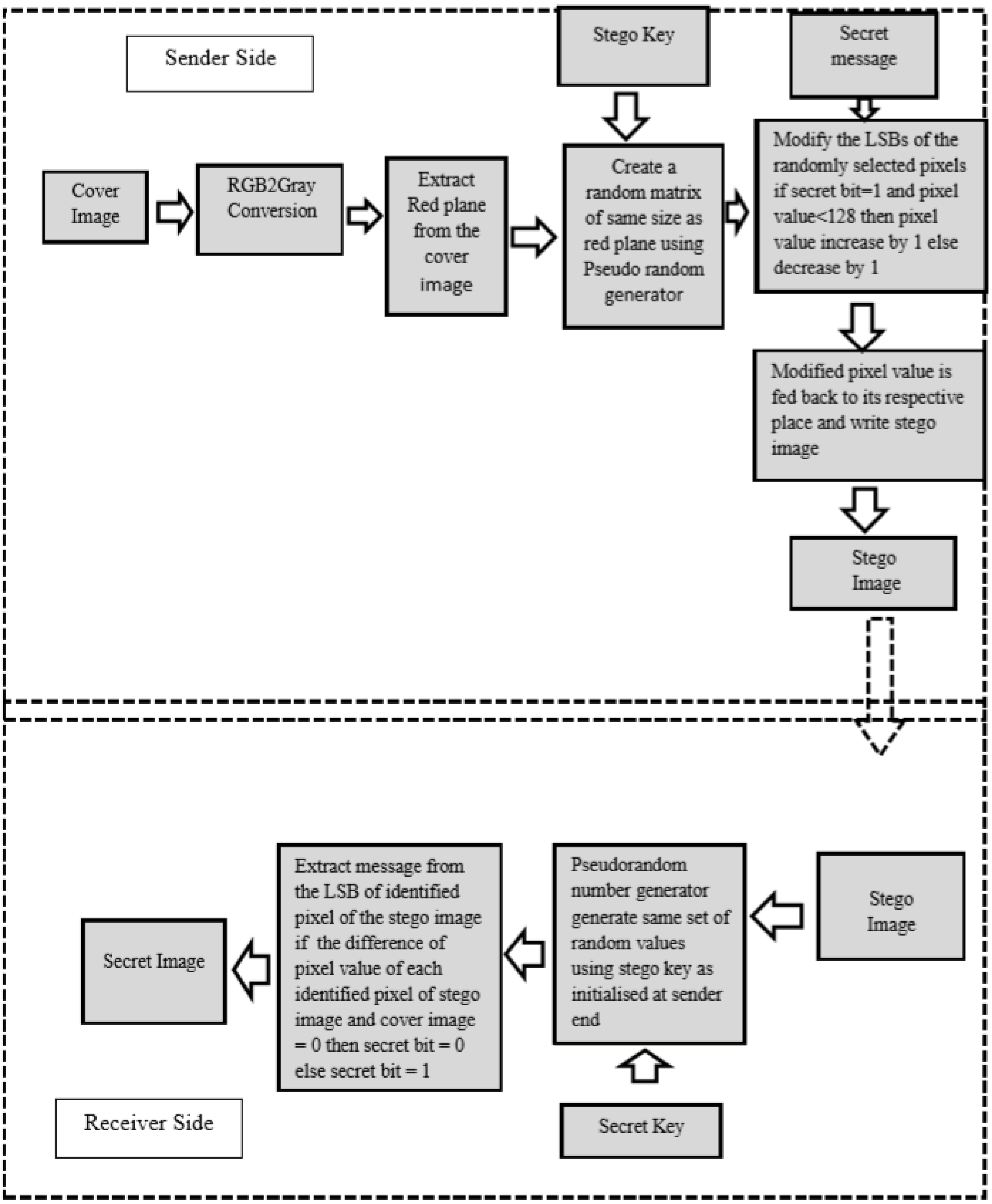
Sender Side
Stego Key
Secret message
Cover Image
RGB2Gray Conversion
Extract Red plane from the cover image
Create a random matrix of same size as red plane using Pseudo random generator
Modify the LSBs of the randomly selected pixels if secret bit=1 and pixel value<128 then pixel value increase by 1 else decrease by 1
Modified pixel value is fed back to its respective place and write stego image
Stego Image
Extract message from the LSB of identified pixel of the stego image if the difference of pixel value of each identified pixel of stego image and cover image = 0 then secret bit = 0 else secret bit = 1
Pseudorandom number generator generate same set of random values using stego key as initialised at sender end
Stego Image
Secret Image
Receiver Side
Secret Key

Fig.8. Flow Diagram for Distortion Techniques

5.1.4 LWT Technique (Lifting Wavelet Transform Technique)

In LWT Technique, the main feature of lifting wavelet scheme is that all constructions are derived in the spatial domain. It doesn’t require complex mathematical calculations that are required in traditional methods [4]. Lifting scheme is simplest and efficient algorithm to calculate wavelet transform. It doesn’t depend on Fourier transforms. Lifting scheme is used to generate second-generation wavelets, which are not necessarily dilation and translation of a particular function. One of the most popular advantages of this wavelet transform is that it allows a faster number of computations as compared to discrete wavelet transform which is very attractive for real time low power applications. Complete process is described in Fig.9.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Convert the secret message into the binary bits before embedding into the cover image.
3) Apply LWT on the cover image and divide the image into four different band i.e. CA,CH, CV and CD.
4) The message bits are embedded into LSBs of the pixel values using typecast function into CH band because typecast function converts the data type without changing the underlying data.
5) Apply inverse LWT on the modified LSBs of the pixel values of the CH band and the other bands of the image together and reconstruct the image.
6) Read the stego image.

Retrieving Algorithm:

1) Read the Stego image.
2) Extract the message bit from the LSBs of the pixel values of the image using typecast function.
3) Combine the bits to form a complete message.
4) Convert each 8 bits into character i.e. text message.
5) Finally, we get the require text message.

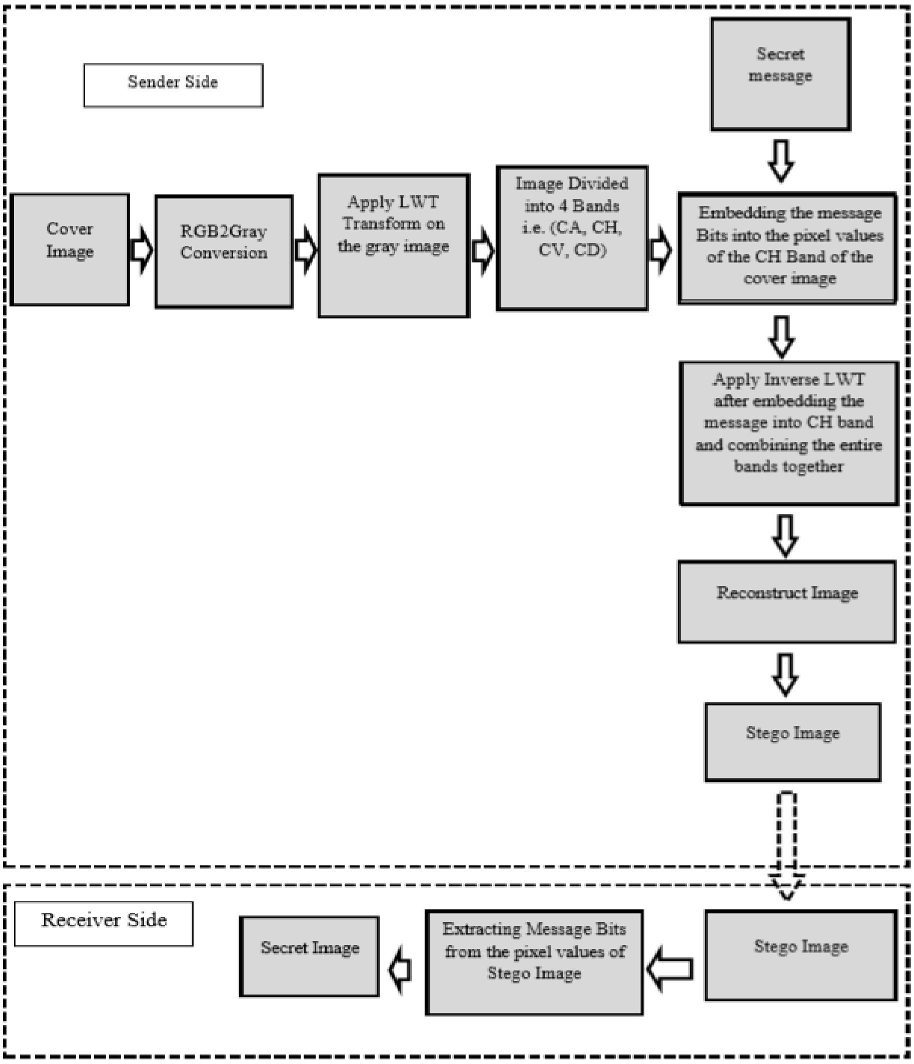
Sender Side
Secret message
Cover Image
RGB2Gray Conversion
Apply LWT Transform on the gray image
Image Divided into 4 Bands i.e. (CA, CH, CV, CD)
Embedding the message Bits into the pixel values of the CH Band of the cover image
Apply Inverse LWT after embedding the message into CH band and combining the entire bands together
Reconstruct Image
Stego Image
Receiver Side
Secret Image
Extracting Message Bits from the pixel values of Stego Image
Stego Image

Fig.9. Flow Diagram for LWT Technique

5.2 Frequency Domain Techniques

5.2.1 DCT Technique (Discrete Cosine Transform Technique)

In Discrete cosine transform technique of steganography, the cover image is converted into Frequency domain. It organised the image content into components of different importance with respect to the image visual quality [1,13]. This is the most common algorithm utilized in image steganography as a standard for JPEG image format with image quantization and compression. In image processing, the cover image is quantized after applying DCT to improve compression rate. Complete process is described in Fig.10.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Convert the secret message into the binary bits before embedding into the cover image.
3) The cover image is converted into blocks of size 8×8pixels.
4) Take blocks of cover image in which we want to embed our message bit and converted these blocks into frequency domain using DCT Technique. Round off the values of the blocks of the cover image after applying the DCT transformation. The top left value in the block is the DC value which is average of the entire block. It is the lowest frequency cosine coefficient.
5) Embed the message bits in the LSBs of the blocks of pixel values using "typecast function". Typecast function is used to modifying or changing the data type without changing the underlying data.
6) Calculate the inverse DCT of the modified blocks and reconstruct the image.
7) Read the Stego Image.

Retrieval Algorithm:

1) Read the stego image.
2) Stego image is broken into blocks of size 8×8pixels.
3) All the blocks of the stego image is converted into frequency domain using DCT transformation. Round off the values of the pixels of the stego image after applying DCT transformation.
4) The top left value in the block is the DC value which is average of the entire block. It is the lowest frequency cosine coefficient.
5) Again use the function typecast to change the data type without changing the underlying data.
6) Read the LSB of each DC coefficient.
7) Combine the bits to form a complete message.
8) Convert each 8 bits into character i.e. text message.
9) Finally, we get the require text message.

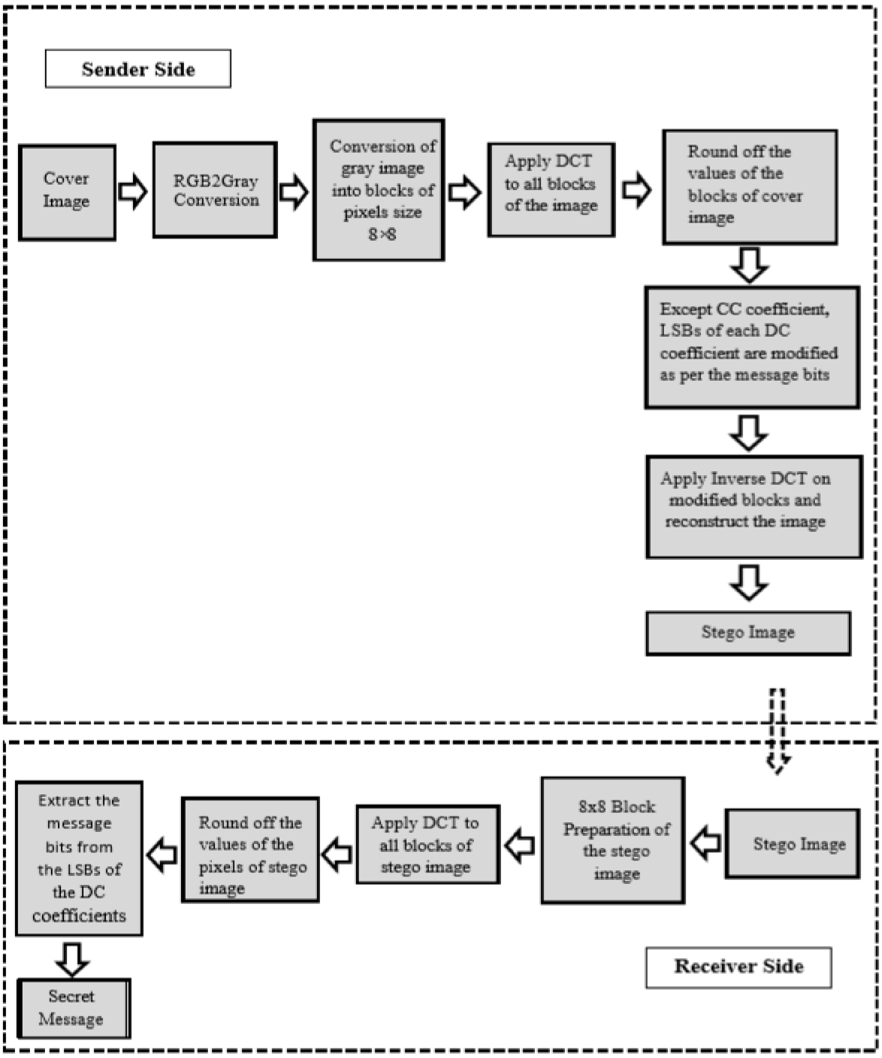
Sender Side
Cover Image
RGB2Gray Conversion
Conversion of gray image into blocks of pixels size 8×8
Apply DCT to all blocks of the image
Round off the values of the blocks of cover image
Except CC coefficient, LSBs of each DC coefficient are modified as per the message bits
Apply Inverse DCT on modified blocks and reconstruct the image
Stego Image
Stego Image
8x8 Block Preparation of the stego image
Apply DCT to all blocks of stego image
Round off the values of the pixels of stego image
Extract the message bits from the LSBs of the DC coefficients
Secret Message
Receiver Side

Fig.10. Flow Diagram for DCT Technique

5.2.2 DWT Technique (Discrete Wavelet Transform Technique)

DWT is another technique of frequency domain transformation proposed by Haar transformation. This technique is divided into two operations i.e. Horizontal operation and vertical operation. In this process of steganography DWT identifies the high and low frequency information of each pixel of the image. It is the mathematical code for decomposing the image hierarchically [5,1,15]. It is mainly used for processing of non-stationary signal. The wavelet transform based on small wave called wavelets of different frequency and limited duration. DWT perform in one dimension and in the two-dimensional plane. Complete process is described in Fig.11.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Convert the secret message into the binary bits before embedding into the cover image.
3) Convert the coloured image into gray scale image.
4) Apply DWT on cover image to divide it into four bands i.e., LL, LH, HL and HH.
5) The message bits are embedded into LSBs of the pixel value of any band except LL band.
6) Apply inverse DWT on the modified band and reconstruct the image.
7) Read the stego image.

Retrieve Algorithm:

1) Read the stego image.
2) Extract the message bit from the LSBs of the pixel values of the modified band.
3) Combine the bits to form a complete message.
4) Convert each 8 bits into character i.e. text message.
5) Finally, we get the require text message.

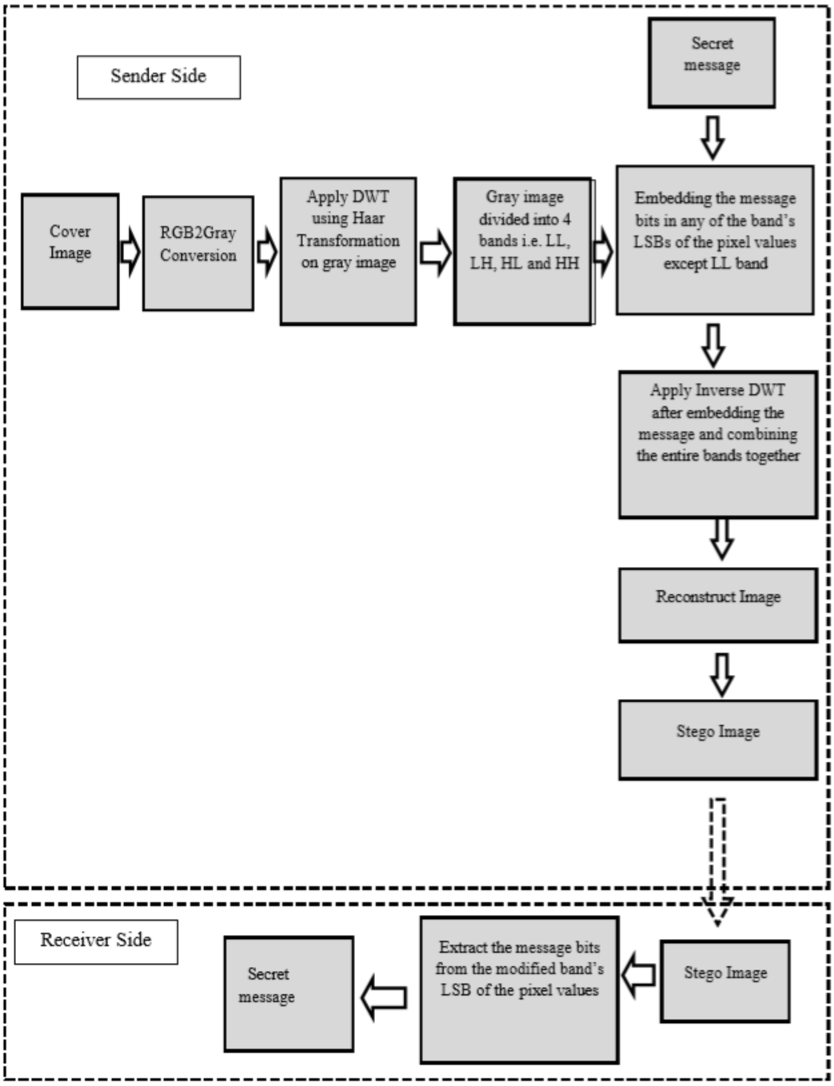
Sender Side
Secret message
Cover Image
RGB2Gray Conversion
Apply DWT using Haar Transformation on gray image
Gray image divided into 4 bands i.e. LL, LH, HL and HH
Embedding the message bits in any of the band's LSBs of the pixel values except LL band
Apply Inverse DWT after embedding the message and combining the entire bands together
Reconstruct Image
Stego Image
Receiver Side
Secret message
Extract the message bits from the modified band's LSB of the pixel values
Stego Image

Fig.11. Flow Diagram for DWT Technique

5.2.3 FFT Technique (Fast Fourier Transform Technique)

This algorithm is used for calculating the Discrete Fourier Transform (DFT) of sequence and its inverse. It converts a signal from its original domain to frequency domain and frequency domain to its original domain [3]. Secret data can be hidden in image in the Fourier or frequency domain which can be defined as the inverse of pixels or special units and as inverse of time unit. In this method first of all Discrete Fourier Transform using Fast Fourier Transform (FFT) has been applied to the cover image which is used during open channel communication. This gives two component –real and imaginary component or the magnitude and phase component visualized as images. While communicating through an open channel an imperceptible vision is provided without distortion in the quality of the stego image. The embedding of the secret message bits into the carrier image- magnitude and the phase component is performed by this steganography technique. Complete process is described in Fig.12.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Convert the secret message into the binary bits before embedding into the cover image.
3) Apply FFT on the cover image.
4) The message bits are embedded into LSBs of the pixel values using typecast function because typecast function converts the data type without changing the underlying data.
5) Apply inverse FFT on the modified LSBs of the pixel values of the cover image and reconstruct the image.
6) Read the stego image.

Retrieve Algorithm:

1) Read the Stego image.
2) Apply FFT on stego image.

3) Extract the message bit from the LSBs of the pixel values of the image using typecast function.
4) Combine the bits to form a complete message.
5) Convert each 8 bits into character i.e. text message.
6) Finally, we get the require text message.

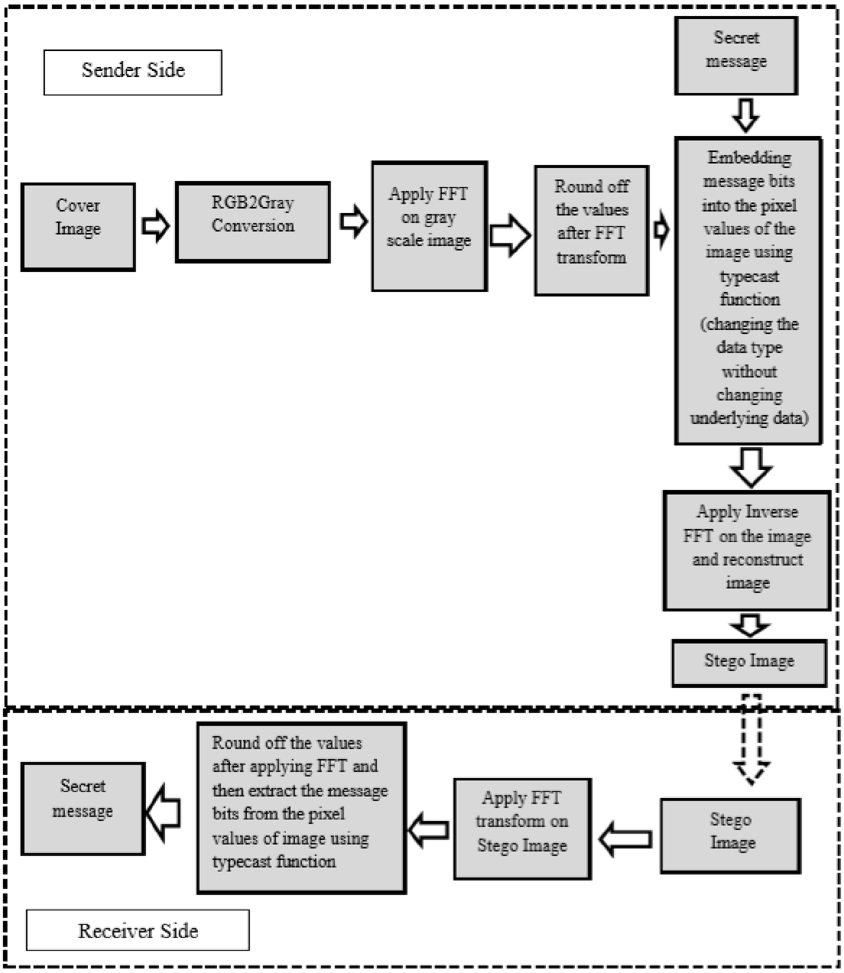
Sender Side
Secret message
Cover Image
RGB2Gray Conversion
Apply FFT on gray scale image
Round off the values after FFT transform
Embedding message bits into the pixel values of the image using typecast function (changing the data type without changing underlying data)
Apply Inverse FFT on the image and reconstruct image
Stego Image
Stego Image
Apply FFT transform on Stego Image
Round off the values after applying FFT and then extract the message bits from the pixel values of image using typecast function
Secret message
Receiver Side

Fig.12. Implementation for FFT Technique

5.2.4 Singular Value Decomposition Technique (SVD)

SVD is a matrix factorization technique commonly used for producing low-rank approximations. Given an m × n matrix A with rank r, the singular value decomposition SVD (A) is given by

$$SVD (A) = U \times S \times V$$

Where U, S and V are of dimensions m × m, m × n and n × n respectively. U and V are two orthogonal matrices known as the left and the right singular vectors respectively and S is the diagonal matrix called the singular matrix. The unique property of singular values in SVD is that, they are non- negative [5,16]. It provides the best low-rank linear approximation of the original matrix A. Its property makes it particularly interesting for our application. Complete process is described in Fig.13.

Embedding Algorithm:

1) Read the cover image and the secret message.
2) Convert the secret message into the binary bits before embedding into the cover image.
3) Apply SVD on the cover image after converting the gray image into double. The image is converted into three planes i.e. (u v s).
4) The message bits are embedded into LSBs of the pixels of any band except v band.
5) Apply inverse SVD on the modified band and reconstruct the image.
6) Read the stego image.

Retrieve Process:

1) Read the stego image.
2) Apply SVD on the stego image.
3) Extract the message bit from the LSBs of the pixels of the band.
4) Combine the bits to form a complete message.
5) Convert each 8 bits into character i.e. text message.
6) Finally, we get the require text message.

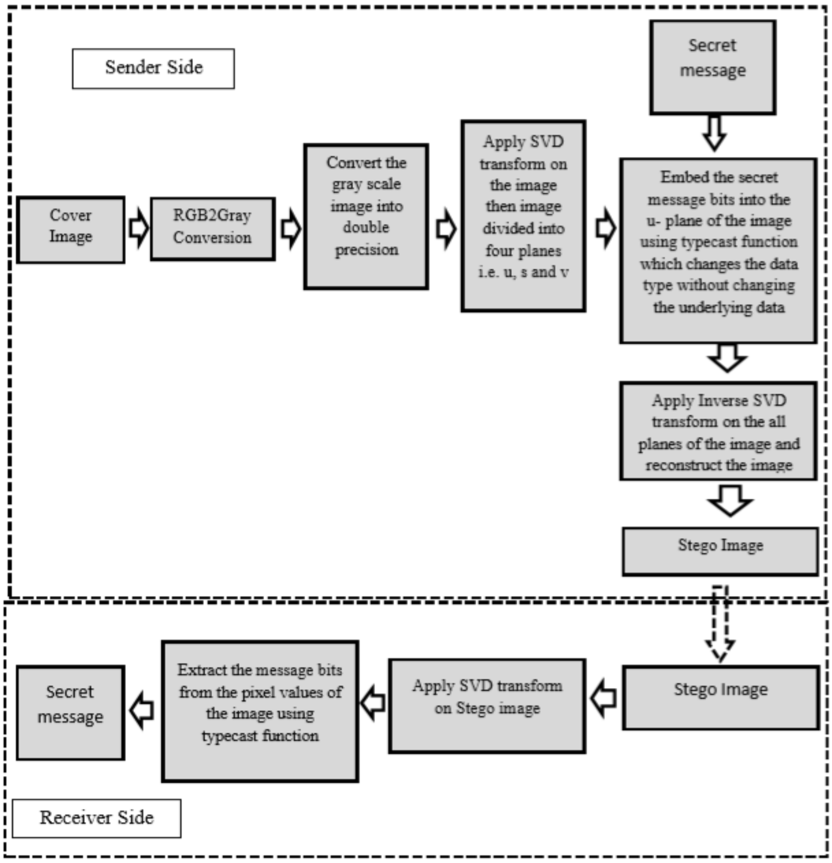
Sender Side
Secret message
Cover Image
RGB2Gray Conversion
Convert the gray scale image into double precision
Apply SVD transform on the image then image divided into four planes i.e. u, s and v
Embed the secret message bits into the u- plane of the image using typecast function which changes the data type without changing the underlying data
Apply Inverse SVD transform on the all planes of the image and reconstruct the image
Stego Image
Stego Image
Apply SVD transform on Stego image
Extract the message bits from the pixel values of the image using typecast function
Secret message
Receiver Side

Fig.13. Flow Diagram for SVD Technique

6. Simulation Set up parameters

6.1. Setup Parameter

The set up parameters used for simulation are given in table 2. The values given in table mention specification of the images, processor, memory size of available machine and version of the MATLAB programming tool, which are actually used during the experimental analysis of different steganography mechanisms.

Table 2. Setup Parameters for Simulation

Parameter	**Values**
Data Size	53×8 bits
Image Size	256 × 256 128 × 128 64 × 64
Image Category	Grey Image(.jpg format)
Programming Language Tool	MATLAB R2014a
Simulation Implemented	64 Bit MATLAB
Processor	1.6GHz dual core Intel i5
Memory Size	8GB/1TB 5400rpm DDR4 RAM

6.2 Performance Matrices

6.2.1 Bhattacharyya Coefficient

This coefficient measures the similarity between the cover image and the stego image by using probability distribution method [2].
Formula for Bhattacharyya coefficient is given by:

$$BC(X,Y) = \sum_{i=1}^{N} \sqrt{X(i)Y(i)} \quad (1)$$

Where, T1 is the cover image and T2 is the stego image.
BC (X, Y) is the Bhattacharyya coefficient between image matrices T1 and T2.
X and Y are the probability distributions of image T1 and T2.
If value of Bhattacharyya coefficient is 1 it signifies perfect match and if coefficient is equal to 0 then it signifies total mismatch.

6.2.2 Intersection Coefficient

Histograms of the intersection count the common number of the pixels of same value between the histograms of cover image and stego image [2].
The intersection coefficient is given by:

$$I(X,Y) = \sum_{i=1}^{N} \min\,(X(i), Y(i)) \quad (2)$$

Where, T1 is the cover image and T2 is the stego image.
I (X, Y) is the intersection coefficient between image matrices X and Y.
X and Y are the probability distributions of the images T1 and T2.
If value of intersection coefficient is equal to 1 it signifies perfect match and if coefficient is equal to 0 then it signifies total mismatch.

6.2.3 Correlation Coefficient

It is a measure of the linear correlation between images i.e. covers image and stego image, giving a value +1 and -1 where 1 it signifies perfect match and -1 signifies total mismatch.
The correlation coefficient is given by:

$$\rho(X,Y) = \frac{cov(X,Y)}{\sigma X \sigma Y} \quad (3)$$

Where, T1 is the cover image and T2 is the stego image.
ρ(X, Y) is the correlation coefficient between image matrices X and Y.
$(X,)$ is the covariance between matrices X and Y.
σX is the standard deviation of X.
σY is the standard deviation of Y.

6.2.4 Jaccard Index

This index is also known as Jaccard Similarity Coefficient which is used for comparing similarity between the cover image and the stego image.
The jaccard coefficient is given by:

$$J(X,Y) = \frac{X \cap Y}{X \cup Y} \quad (4)$$

Where, T1 is the cover image and T2 is the stego image.
J(X, Y) is the correlation coefficient between image matrices X and Y.
X ∩ Y is the intersection of matrices X and Y.
X U Y is the union of matrices X and Y.
The value of jaccard index lies between 0 and 1. 1 signifies perfect match and 0 signifies total mismatch.

6.2.5 Universal Image Quality Index (UIQI)

This index is used to measure the changes in stego image with respect to the cover image [2]. In this method the comparison of the image is broken down into three parts:

i. Luminance comparison (LC)
ii. Contrast comparison (CC)
iii. Structural comparison (SC)

The UIQI is given by:

$$L(X,Y) = \frac{2\mu X\mu Y}{\mu X2 + \mu Y2} \tag{5}$$

$$C(X,Y) = \frac{2\sigma X\sigma Y}{\sigma X2+\sigma Y2} \tag{6}$$

$$S(X,Y) = \frac{2\sigma XY}{\sigma X+\sigma Y} \tag{7}$$

$$UIQI(X,Y) = L(X,Y) * C(X,Y) * S(X,Y) \tag{8}$$

Where, X is the cover image and Y is the stego image.
µX is the mean of matrix X.
µY is the mean of matrix Y.
$\boldsymbol{\sigma}$X is the standard deviation of matrix X.
$\boldsymbol{\sigma}$Y is the standard deviation of matrix Y.
$\boldsymbol{\sigma}$XY is the covariance between matrices X and Y.

6.2.6 Mean Square Error (MSE)

This method is a quantitative representation of the error that occurs in the stego image with respect to the cover image [2, 17].
MSE is given by:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \tag{9}$$

Where, m × n is the size of the image.
For coloured image, image size will be m×n×3.

6.2.7 Mean Absolute Error (MAE)

Mean absolute error is the average of absolute error between the cover image and the stego image.
MAE for colour image is given by:

$$MAE = \frac{1}{mn}\sum_{i=1}^{n}\sum_{j=1}^{m}|f(i,j) - y(i,j)| \tag{10}$$

Where, m × n is the size of the image.
For coloured image, image size will be m×n×3.

6.2.8 Peak Signal to Noise Ratio (PSNR)

This is most commonly used parameter to measure the quality of the cover image after embedding the secret message bits into it [2,17]. Higher the PSNR value shows maximum robustness of the stego image.
The PSNR is given by:

$$PSNR = 10\log_{10}(\frac{MAX^2}{MSE}) \tag{11}$$

Where, MAX is the maximum value of pixel in the image.

7. Results

7.1 Security Analysis

Security is the ability of the mechanism to hide the secret message in such a way that before and after embedding Image pixel values should not alter much. [10, 13, 16]. The security analysis of a method is done by evaluating the pixel values, possibility allotment and histograms between the cover and stego image. Security of the Steganography technique can be measured by calculating the Bhattacharyya Coefficient (BC), Intersection Coefficient (IC), Correlation Coefficient (CC), Jaccard Index (JI), and Universal Image Quality Index (UIQI), of the stego image with respect to the cover image.

7.1.1 Bhattacharyya Coefficient (BC)

Table 3. BC v/s Image Size

BC			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	1	1	1
Pseudorandom	0.9999	1	1
DCT	0.957	0.9711	0.9787
DWT	0.9849	0.998	0.9996
FFT	0.6305	0.8409	0.9213
SVD	0.9999	1	1
Distortion	0.8827	0.8839	0.8838
LWT	0.9868	0.9968	0.9995

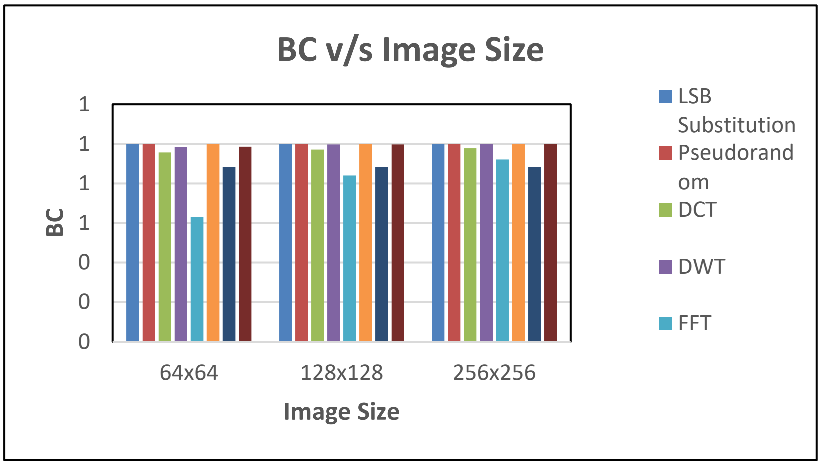

Fig.14. BC v/s Image Size

- As per results highest value shows perfect matching which is 1. The value of different techniques conveys that in LSB, Pseudorandom, LWT, SVD, the cover image and stego image are very similar.
- FFT has highest mismatching between two images.
- For LSB, SVD and Pseudorandom techniques, higher value of BC represents desirable outcomes and helps in generating highly matched stego image with respect to their cover image.

7.1.2 Intersection Coefficient (IC)

Table 3. IC v/s Image Size

IC			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	1.00	1.00	1.00
Pseudorandom	0.99	1.00	1.00
DCT	0.80	0.83	0.86
DWT	1.00	0.96	1.00
FFT	0.42	0.66	0.79
SVD	0.99	1.00	1.00
Distortion	0.66	0.63	0.62
LWT	0.88	0.95	0.98

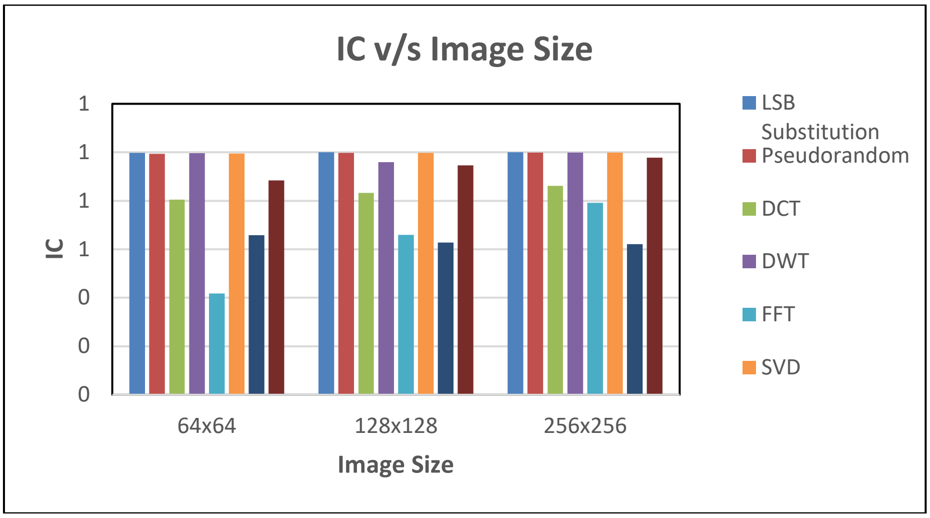

Fig.15. IC v/s Image Size

- As per the result LSB, Pseudorandom, DWT and SVD techniques have highest number of common pixels in both images.
- Distortion, DCT and FFT gives lowest count for the number of pixels in both images.
- Higher value of Intersection Coefficient is needed for getting better results. In case of LSB, SVD & Pseudorandom techniques, the value of IC is higher as compared to other techniques.

7.1.3 Correlation Coefficient (CC)

Table 4. CC v/s Image Size

CC			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	0.9999	0.9999	0.9999
Pseudorandom	1	1	1
DCT	0.9313	0.9047	0.9033
DWT	0.9884	0.9965	0.999
FFT	0.9092	0.7905	0.9303
SVD	1	1	1
Distortion	0.9345	0.9285	0.9259
LWT	0.9939	0.995	0.9987

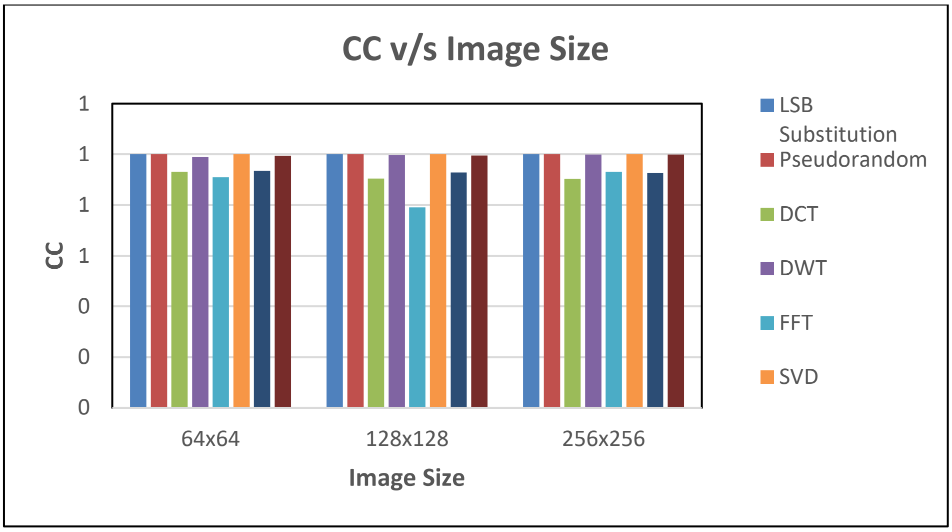

Fig.16. CC v/s Image Size

- As per results highest value shows perfect matching which is 1. The value of different techniques convey that in LSB, Pseudorandom, LWT, SVD, the cover image and stego image are very similar as shown in Fig.16.
- FFT, DCT and distortion have highest mismatching between two images.
- Requirement of higher Correlation Coefficient is suitable for getting desirable results. As depicted in above figure, for LSB, Pseudorandom and SVD techniques CC shows highest value.

7.1.4 Jaccard Index (JI)

Table 5. JI v/s Image Size

JI			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	1	1	1
Pseudorandom	1	1	1
DCT	0.9749	0.9751	0.9743
DWT	0.9961	0.9979	0.9993
FFT	0.4632	0.7184	0.8532
SVD	1	1	1
Distortion	0.9387	0.9571	0.9708
LWT	1	0.9999	1

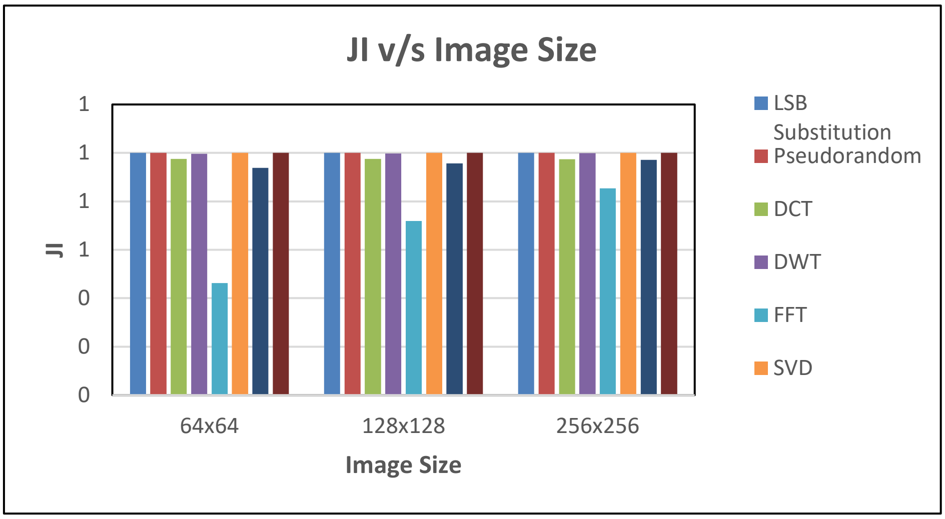

Fig.17. JC v/s Image Size

- As per the results the jaccard index is highest for LSB, Pseudorandom and DWT techniques and lowest for FFT technique as shown in Fig.17.
- Techniques having higher Jaccard Index help in securing the message more efficiently by generating highly matched stego image with respect to cover image.

7.1.5 Universal Image Quality Index (UIQI)

Table 6. UIQI v/s Image Size

UIQI			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	1	1	1
Pseudorandom	1	1	1
DCT	0.9545	0.9399	0.9437
DWT	0.9941	0.9982	0.9995
FFT	0.4556	0.7741	0.9443
SVD	1	1	1
Distortion	0.9044	0.8877	0.8834
LWT	0.9969	0.9975	0.9994

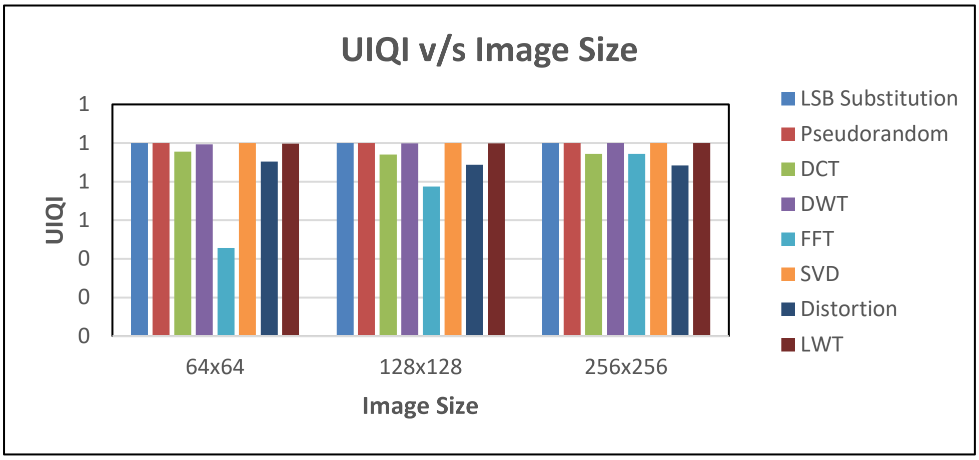

Fig.18. UIQI v/s Image Size

- As a results image quality index of spatial domain is highest as shown in Fig.18.
- Image quality index of transform technique FFT and distortion shows lowest values.
- UIQI parameter assist in getting a better correlation between stego image and cover image which means higher the value of JI , better will be the output.

7.2 Robustness Analysis

Robustness ensures capability of algorithm to save the secret information into cover Image. It is a significant parameter to access a steganography technique, and it can be computed by measuring the Peak Signal to Noise Ratio (PSNR), Mean Absolute Error (MAE) and Mean Square Error (MSE).

7.2.1 Mean Absolute Error (MAE)

Table 7. MAE v/s Image Size

MAE			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	7.3E-04	8.1E-05	3.1E-05
Pseudorandom	3.2E-03	1.1E-03	2.3E-04
DCT	5.1E+00	5.7E+00	5.5E+00
DWT	1.1E+00	5.8E-01	2.6E-01
FFT	1.5E+01	8.3E+00	3.6E+00
SVD	3.1E-03	7.1E-03	2.5E-03
Distortion	7.5E+00	8.1E+00	8.2E+00
LWT	3.2E-01	2.4E-01	1.0E-01

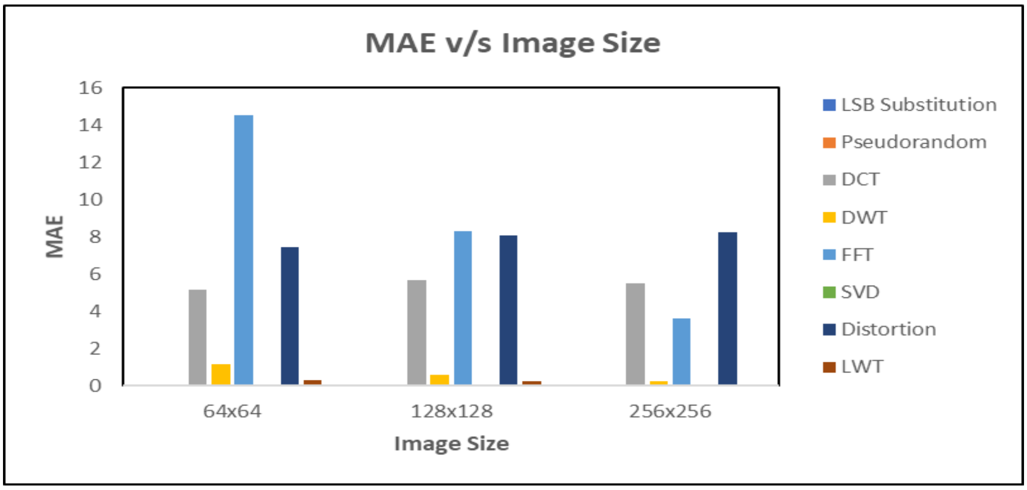

Fig.19. MAE v/s Image Size

- As a results MAE is highest for FFT technique. In comparison to this technique MAE for other techniques is too small or negligible as shown in Fig.19.
- As much as the value of MAE is lower leads towards the desirable results in maintaining the similarity between the stego image and the cover image which helps in making the system more secure and integrated.

7.2.2 Mean Square Error (MSE)

Table 8. MSE v/s Image Size

MSE			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	6.1E-05	6.1E-05	4.6E-05
Pseudorandom	9.5E-03	3.3E-03	6.9E-04
DCT	8.0E+01	7.8E+01	7.8E+01
DWT	1.4E+01	6.0E+00	2.0E+00
FFT	2.3E+02	1.2E+02	6.2E+01
SVD	5.1E-03	4.2E-03	1.3E-02
Distortion	5.3E+01	5.1E+01	5.0E+01
LWT	3.9E+00	2.7E+00	8.8E-01

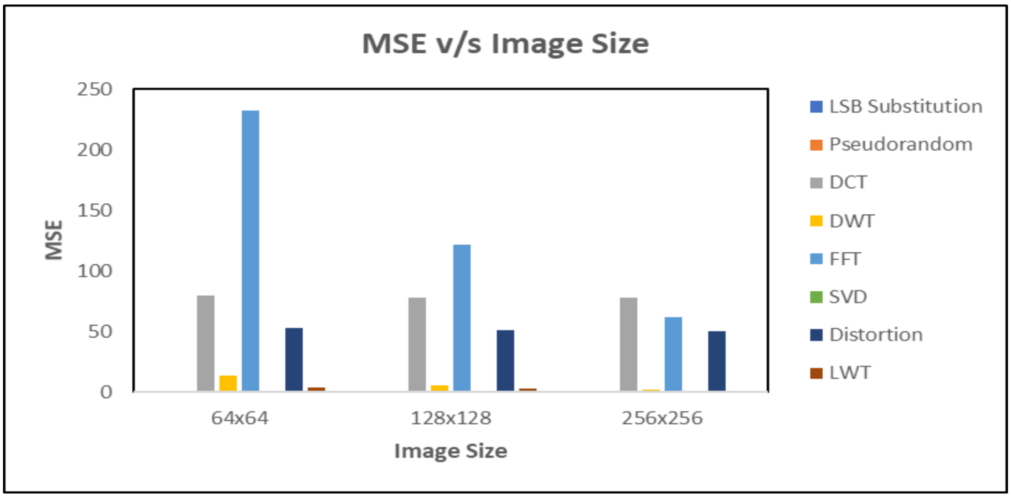

Fig.20. MSE v/s Image Size

- As per the result the MSE is highest for FFT and DCT technique.

- In comparison to these two techniques MSE for other technique is too small or negligible except distortion as shown in Fig.20.
- There is always been a need of the low value of MSE for getting a desirable result or for finding the better correlation between both of the images. As shown in above figure, MSE is lower for these techniques such as LSB, pseudorandom and SVD which means these techniques are more suitable as compared to other techniques.

7.2.3 Peak Signal to Noise Ratio (PSNR)

Table 9. PSNR v/s Image Size

PSNR			
Techniques	**64x64**	**128x128**	**256x256**
LSB Substitution	79.48	90.28	91.52
Pseudorandom	38.34	72.95	79.76
DCT	22.69	21.53	21.54
DWT	36.70	40.35	45.18
FFT	24.47	27.27	30.19
SVD	71.03	71.95	66.86
Distortion	30.87	31.07	31.14
LWT	42.30	43.75	48.69

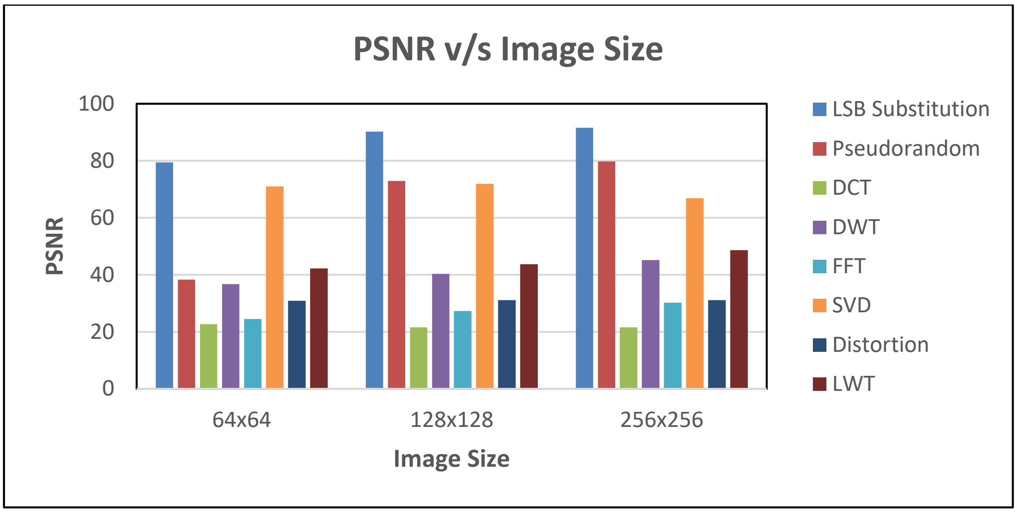

Fig.21. PSNR v/s Image Size

- As per the result PSNR is highest for LSB technique and minimum for DCT technique as shown in Fig.21.
- Spatial domain techniques have high signal to noise ratio in comparison to frequency domain.
- There is an inverse relationship between PSNR and MSE. So a higher value of PSNR indicates the low value of error rate and gives better quality of stego image with respect to cover image.
- For getting a desirable result, higher value of PSNR is always needed. As shown in above figure, LSB and Pseudorandom techniques having the highest value of PSNR which are suitable for achieving integration of the secret message because of the better quality of stego image with respect to cover the image.

7.3 Imperceptibility Analysis

7.3.1 Snapshots

Figure 10 shows original and stego images of different sizes after undergoing different mechanism. Visual inspection or qualitative analysis of these snapshots is the measure of Imperceptibility of steganography technique. High Imperceptibility is desirable, as it ensures that no unauthorized person can get information regarding availability of data in Image. As observed from the figure spatial domain mechanisms have high imperceptibility in comparison to frequency domain.

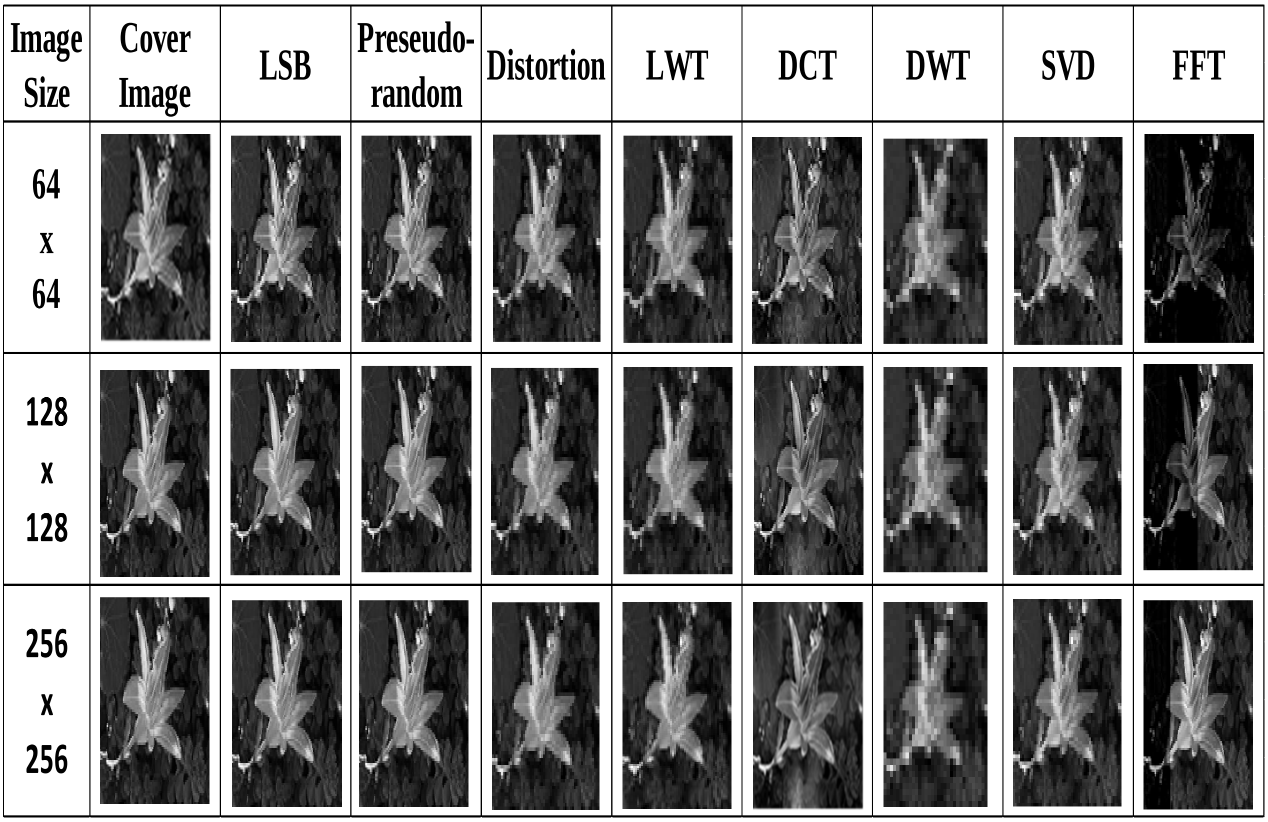

Fig.22. Snapshots for different sizes and techniques of Cover Images and Stego Images

8. Conclusion

After implementation of different steganography mechanisms and evaluate on the basis of different performance matrices final conclusion table is described as under (Table 10).

Table 10. Comparison table on the basis of performance metrics

	Techniques							
	High			Medium		Low		
Parameters	LSB	Pseudorandom	SVD	LWT	DWT	Distortion	FFT	DCT
BC	1	1	1	0.9968	0.998	0.8839	0.8409	0.9711
CC	0.9999	1	1	0.9975	0.9965	0.9285	0.7905	0.9047
JI	1	1	1	0.9999	0.9979	0.9571	0.7184	0.9751
IC	1	1	1	0.95	0.96	0.63	0.66	0.83
MAE	8.10E-05	1.10E-03	7.10E-03	2.40E-01	5.80E-01	8.10E+00	8.30E+00	5.70E+00
MSE	6.10E-05	3.30E-03	4.20E-03	2.70E+00	6.00E+00	5.10E+01	1.20E+02	7.80E+01
PSNR	90.28	72.95	71.95	43.75	40.35	31.07	27.27	21.53
UIQI	1	1	1	0.9975	0.9982	0.8877	0.7741	0.9399

- Amongst all the techniques LSB, Pseudorandom and SVD techniques have highest PSNR and lowest MAE, MSE which results into getting similarity between both stego image and cover image.
- As per the resultant graphs DCT technique has highest MSE and lowest PSNR value. Frequency domain techniques provide low robustness with low PSNR value and low perceptual quality.
- Spatial domain mechanisms showing better correlation between both stego image and cover image which helps in maintaining the confidentiality and integrity of the secret message.

- As per the results shown for different parameters, it is clearly concluded that Spatial Techniques have highly possible matched stego image with respect to cover image.
- For LSB and Pseudorandom Techniques, defined parameter such as BC, CC, IC, UIQI and PSNR have the highest value and lowest MSE along with MAE, which allows secret data to be hidden without degrading the perceptual quality of an image.
- Most of the existing research papers focus on evaluating techniques only on four to five performance metrics whereas this research paper considers evaluating techniques on at least 8 parameters. It will help researches to have a broader picture about results as compared to the pre-existing ones.
- Future work can be extended by taking attacks and noises into consideration because the channel through which stego-image will communicate is prone to large number of susceptibilities.

References

[1] Sangeeta Dhall, Bharat Bhushan and Shailender Gupta, “An In-depth Analysis of Various Steganography Techniques” in International Journal of Computer Networks and Applications Volume 2, Issue 1 (2015)

[2] Karthikeyan B, Asha S, and Poojasree B, “Gray Code Based Data Hiding in an Image using LSB Embedding Technique” in International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1, May 2019

[3] Afsha Shaukat Mahesh Chaurasia and Prof. Goutam Sanyal,”A Novel Image Steganography Technique using Fast Fourier Transform” in Fifth International Conference On Recent Trends In Information Technology 2016.

[4] N Sathisha1, K Suresh Babu2, K B Raja2, and K R Venugopal ,“Image Steganography Based on Mantissa Replacement using LWT” in International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015.

[5] Priyanka Chouksey, and Dr. Prabhat Patel, “Secret Key Steganography technique based on three-layered DWT and SVD algorithm” in International Journal of Engineering Trends and Technology (IJETT) – Volume 35 Number 9 - May 2016

[6] Er. Babita Sant, “A Review: Network Security Based On Cryptography & Steganography Techniques” in International Journal of Advanced Research in Computer Science Volume 8, No. 4, May 2017.

[7] Sangeeta Dhall, Bhuvnesh Kumar and Rashmi Chawla, ”A Comprehensive Analysis of Various Steganography Techniques Under Different Attacks” in IEEE Conference ID: 40353 2017 4th International Conference.

[8] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[9] Preeti Kumari and Ridhi Kapoor, “Image Steganography for Data Embedding & Extraction using LSB Technique” in International journal of Computer Applications & Information Technology- Volume 9 Issue 2, July 2016.

[10] Divya.A1 and S.Thenmozhi, “Steganography: Various Techniques In Spatial and Transform Domain” in International Journal of Advanced Scientific Research and Management, Vol. 1 Issue 3, March 2016.

[11] K.Thangadurai and G.Sudha Devi, “An analysis of LSB Based Image Steganography Techniques” in International Conference on Computer Communication and Informatics , Jan. 2014, Coimbatore, INDIA.

[12] Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain and K. Raja Sekhar, “Performance Evaluation Parameters of Image Steganography Techniques” in International Conference on Research Advances in Integrated Navigation System, April, 2016.

[13] Ali Sheidaee and Leili Farzinvash, “A Novel Image Steganography Method Based on DCT and LSB” in 9th International Conference on Information and Knowledge Technology, October, 2017.

[14] Rupali Bhardwaj and Vaishali Sharmab,“Image Steganography Based on Complemented Message and Inverted bit LSB Substitution” in 6th International Conference On Advances In Computing & Communications,September, 2016.

[15] Vijay Kumar and Dinesh Kumar, “Performance Evaluation of DWT Based Image Steganography” in IEEE 2nd International Advance Computing Conference, 2010.

[16] Hanaa A. Abdallah, Mohiy M. hadhoud and Abdalhameed A. Shaalan , “An Efficient SVD Image Steganographic Approach”in IEEE, 2009.

[17] Rejani. R, Dr. D. Murugan and Deepu.V.Krishnan, “Comparative Study of Spatial Domain Image Steganography Techniques” in Int. J. Advanced Networking and Applications Volume: 07, 2015.

Authors’ Profiles

Ms. Pooja Yadav is B.Tech (Electronics and Communication Engineering) and M.Tech (Electronics and Communication Engineering). Her academic interests include network security.

Ms. Sangeeta Dhall is B.Tech (Instrumentation and Control Engineering), M.Tech (Electronics and Instrumentation) and pursuing her Ph. D in the area of network security. Her academic interests include network security, embedded systems and digital system design. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

How to cite this paper: Pooja Yadav, Sangeeta Dhall. " Comparative Analysis of Steganography Technique for Information Security ", International Journal of Mathematical Sciences and Computing (IJMSC), Vol.6, No.4, pp.42-69, 2020. DOI: 10.5815/ijMSC.2020.04.05