Image Steganography for Data Embedding & Extraction using LSB Technique

Preeti Kumari
Department of Computer Science and Engineering
DAV University
Jalandhar, India(Punjab)

Ridhi Kapoor
Department of Computer Science and Engineering
DAV University
Jalandhar, India(Punjab)

ABSTRACT

Security is the main concern in today's world due to the rapid growth of information technology. In this research work, the steganographic is the method or process in which the useful information or data, concealing into another form such as image, text, audio and video. The main concern in this work is to provide the confidentiality, availability, integrity and authenticity of information. In a steganographic technique that embeds concealment of information with unremarkable cover media so the third party and hackers do not provoke it. For digital image steganographic many applications of decryption, compression, encryption and embedding methods are used. Noise and quality of the images are reduced or change due to compression. The LSB (Least Significant Bit) insertion technique is used to sustain noise in the images. The parameters which are evaluated such as PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) of the proposed embedding system with respect to tradition technique and robustness is discussed and also providing security to secrete messages.

Keywords

Steganography;LSB;Embedding;Extraction:Information hiding.

1. INTRODUCTION

With advancement in the digital communication technology and the growth of computer power and storage, the problems with ensuring individuals' privacy become important challenging. Due to the development of the internet the most significant issues in networking are the security of data or information [3]. Steganography, coming from the Latin word *Steganos* that means roof or covered and *graphic* means writing. Steganography is defined as the process of embedding the secret messages into another file such that no one else than receiver knows the present of secret messages. In cryptography technique which is also used for information hiding. Cryptography is defined as transferring the text or data onto transparent to non-transparent format for providing the security from third party access. It applies the encryption method to encrypt or convert the message for non readable format, but it doesn't hide the contents of messages.

Huge or large amount of data is easy to copy and destroy by the hackers through the internet. The purpose of steganography is that to detect the presence of covert data onto harmless looking media called to cover media that is text, audio, video or digital images. The secret writing is the technique in which information is transferred or exchanged over the non-secured communication channel. The main terminologies are used in steganography system are: cover image, secret image, embedding algorithm and secret key. The cover image is that the carrier of information in the form of video, audio, image, text and other digital media. The secret image is that the careers of secret information in the format of digital media from unauthorized person or hackers. The secret key is that key used to convert the plain text to cipher text or from cipher text to plain text. The secret key is that key which is used for embedding the extract the information that is only depending upon the steganography LSB technique.

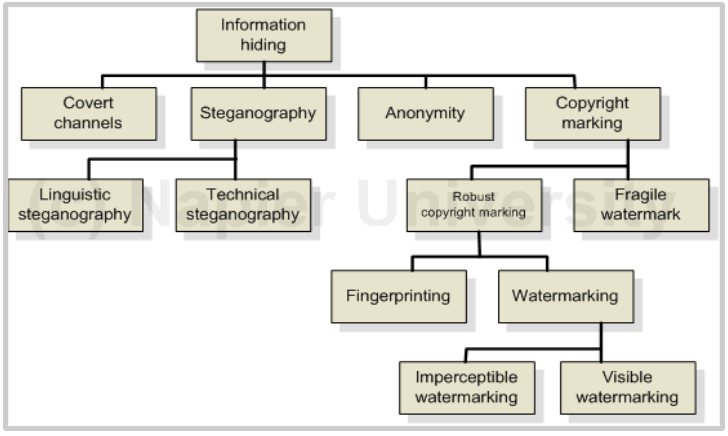


Fig 1: Classification of data hiding methods

The substitution algorithm is those who are used to insert the hidden information about the cover image. In embedding algorithm the one file is a club or adds into another file. The extracting algorithm is that which subtracts the secret message from cover message. In the steganography system initially sender may choose the specific cover image and also select the secret image or password which is hidden inside it. The coding technique is that which converts the secret image of a highly secured form that obtains the storage file. Then sender can send the stage file by email, chatting or any other digital media. The Steganos file which contains the carrier message as well as the secret information. When the receiver receives the message, to decode the message by applying the extracting algorithm and same key or password is used by the sender. By applying the extracting algorithm the stage file providing the cover image and secret message. Images are an effective way for the data hiding. Steganographic technique is divided into two categories such as: Spatial domain technique and Frequency domain technique [1]. The spatial domain algorithm is that which adjust the least bit of the pixel level of the cover image. In Frequency domain technique is that in which frequency coefficients are modified by the cover image that are discrete cosine transform (DCT), discrete wavelet transform (DWT), discrete Fourier transform (DFT).

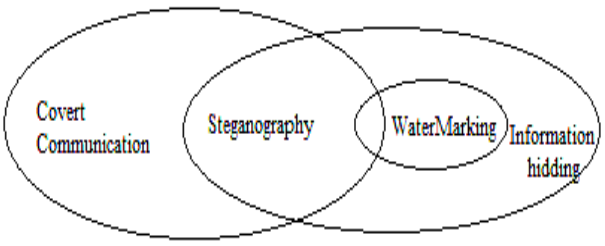


Fig 2: Classification of data hiding methods

The Figure 2 shows the relationship between stenography and other fields. This shows that the steganography is correlated with cryptography and watermarking and the information hiding methods that are also used for secret communication.

2. LITERATURE REVIEW

In Literature review, this shows the communication between sender and receiver secretly. In which steganography uses the technique that is the Least Significant Bit (LSB). In which the various techniques are explained that are explained as:

It [2] focused on quickly developing of steganography and steganalysis. In information security the comparison between steganalysis and steganography becomes the most important issue. For hiding the information the digital images are mostly used as a cover image. The performance is calculated due to spatial domain embedding and transfer domain embedding techniques.

At [5] discussed that the goal of combining both steganography and cryptography is that which provide higher security. They provide the integrity, non-repudiation, authenticity and confidentiality to users. In which firstly secret message is encrypted with the use of encryption algorithm for secure communication and also use the secret key. In which LSB substitution technique is used for embedding and extraction methods that provide the much security for covert communication also.

It [7] observed that spatial domain technique that applies the LSB insertion to embed data into the cover image. It processed parallel or serially by use of guide to fast the data hiding process. The stage image that provides efficient imperceptibility but less security for secret messages.

In [6] proposed that on various images the data encryption standard is applied on it due to steganography technique. Encryption executes with the help of s-boxes and using two Labs insertion information is embedded in the last stage.

As proposed the steganography method that provides very secure protection for private data in the medical system. This method mapped firstly cover image into a 1D pixel sequence by Hilbert filling curve after that portioning into non-overlapping embedding units with three consecutive pixels [9]. This method also uses adaptive pixel pair matches to embed digits into pixel value between the three pixels. To resolve the optimization problem, minimal distortion of the pixel turneries affected by data embedding can be produced.

A novel steganography technique that holds patient information inside a medial image using a key that is generated by 3 coloring problems. This technique is based on the reversibility as the original medical image is reconstructed after extracting from a stage image that contains the embedded data. Due to embedding of patient information in medical image the capacity and visual quality remains retained [10].

It presented the reversible data hiding technique in which after extracting the hidden data he can extract the cover image from the stage image without any disturbance. In [12] this paper a semi-reversible data hiding method is proposed to employ the interpolation and least significant substitution techniques. Before hiding the secret data for better quality and capacity the interpolation technique is used to measure the rising and falling cover image. To embed the secret data LSB substitution is used.

In [13] observed a joint application of encryption, embedding and compression techniques digital image steganography. Due to compression technique the noise is produced in an image.

3. BACKGROUND AND PRELIMINARIES

In order to sustain noise at lower levels in an image she uses the LSB insertion technique that embeds the data or bits and inserted in last 2 LSB's of an image. In this paper firstly compressed the secret data after that encrypt the resulting bits. Those encoded bits are transferred into an image. In this section the main goal of providing the different aspects of authentic steganography technique. These aspects are robustness, capacity and imperceptibility. To provide the robustness, the steganography technique uses the encryption algorithm. The capacity can be increased or decreased according to the compression (loss and lossless) technique and the imperceptibility can be preserved due to the changes in embedding method at minimum amount [2].

JPEG-LS is used for JPEG images and it is a lossless compression technique. This technique provides the low complexity lossless compression. It is efficient and very simple techniques that are used for preserving the quality of the images and also compare the efficiency. For the encrypted images im2double that is the image transformation function is used. The image transformation function that is im2double is needed to change and modify the image intensity values and other parameters to resize the data or information.

Encrypt Image = K - im2doubleS (original Image)

Where K is the value of intensity which is subtracted from original image. The K key is generated using random numbers (key generated). A random number is generated as ruined by MATLAB. LSB Substitution is the method used for hiding information. Due to LSB Substitution method secret bits are replaced with the least bit of the pixels with a cover image that is undetectable to human eyes. The LSB Substitution technique uses embedding and extraction processes. In the LSB Embedding process the large amount of data or information is embedded into the cover image the data may be audio, video, text and images [5]. In encryption, due to the substitution cipher the bits of pain-text may be replaced with the bits of cipher-text and the bits are in the form of letters, characters and others.

The Least Significant Bit Technique is most widely used technique and known as LSB technique. It is divided into two parts such as LSB replacement and LSB matching. In LSB replacement method the LSB bits of cover image are replaced with the secret message of bits. In LSB matching method the pixel values are incremented and decremented according to the secret bits.

The LSB Insertion technique is common and popular embedded technique in which information is stored in the cover image. According to the size of an image that the quality of data or information is transferred into the cover image and bits of secret image due to the LSB insertion. It simply works by rearranging cover image of a pixel having least significant bit with the secret image that are to be hidden. For example the letter S (01010011) can be hidden with the use of LSB insertion [4].

Pixel values before LSB insertion:

11000001 01001110 11110011
00110010 10101011 01100101
10000110 11111100 11001011

Pixel values after LSB insertion of 'S' will be:

11000000 01001111 11110010
00110011 10101010 01100100
10000111 11111101 11001011

With the LSB insertion to imperceptible for human eyes, altering the least significant bits of the stage image that will slightly change the color from the cover image that is the original image. The reason by imperceptibility is that minor changes in the color pixels between cover image and stage image by unit1.changes in the color pixels between cover image and stage image by unit1.

4. MOTIVATION

Reversible data hiding is the process in which after extracting the embedding messages, then the original image can be redestroyed back through lossless compression. This technique is very useful for medical images, military and covert communication where hackers don't modify or steal the secret information except the sender and receiver. As per the literature surveyed so far a steganographic system should be capable of providing security, imperceptibility, robustness and capacity [8]. The main purpose of this technique is to high security in the form of encrypted images. For encryption and decryption purpose LSB technique is used. The LSB substitution technique is used to find out the objectives of the proposed work is to formulate a steganographic system that will satisfy the following parameters:

- To provide the highest security for secret messages.
- Comparison of traditional technique with proposed technique.

5. PROPOSED METHOD

In this paper the Least Significant Bit Substitution algorithm is the process in which embedding and extracting methods are used. This algorithm is used for information hiding. The architecture of the proposed system is shown below:

The purpose of the proposed system is to provide a strong steganographic technique that accomplishes embedding capacity and high security while preserve imperceptibility and quality of the image [6].

5.1. Data Embedding Algorithm

5.2 Data Extracting Algorithm

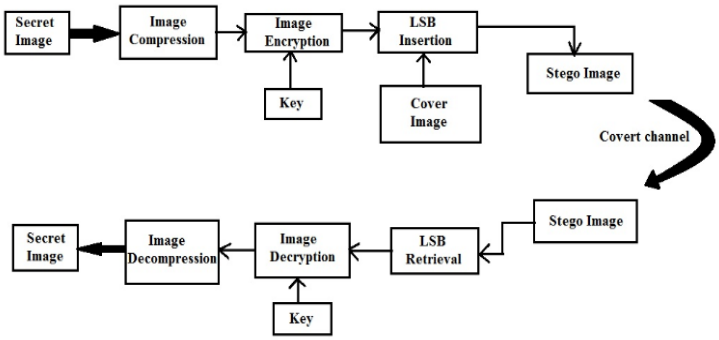


Fig 3: The architecture of the Proposed Steganographic System

The working of the proposed methodology is represented in Fig.4.In which for providing high capacity and robustness the images are firstly compressed. These are compressed by two methods such as: lossless compression technique and lossy compression technique [9].

5.1 Data Embedding Algorithm

In the proposed technique the data or information embedding technique is that in which large amount of data can be embedded into the original image. It allows the user to choose the appropriate the image which is best suited for cover image and less susceptible to the steganalysis attacks. The database is produced from which the best cover images are extracted. For embedding procedure initially select the appropriate image from the database is known as a cover image.

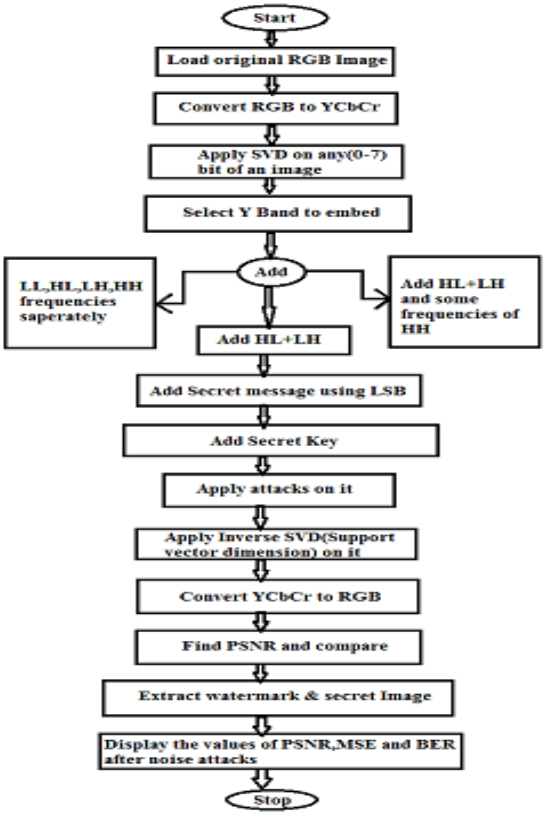


Fig 4: The Proposed Approach

First of all load the original color image (RGB) and convert the RGB image to YCbCr [7]. Then applying Support Vector Dimension (SVD) on any bit of an original image. The Y band is chosen to embed the watermark on an image and applied separately lower to lower, lower to higher, higher to lower, higher to higher to the watermarked images. Compressed the watermarked image by applying the lossless compression technique. The compressed image is produced then the substitution encryption algorithm is applying for that for encryption purpose. Store the original image which is affected by watermark that is staged or watermarked image. Add the secret image with the help of an LSB substitution technique. For encryption a key is used which is created by random generator. The image so produced is the watermarked image. The watermarked image and the key send to the receiver through the internet. The receiver receives the secret key very securely through covert path. The embedding and extracting algorithm is explained as below:

Algorithm for Embedding Process:

Input: Original Image P, Key K, Secret Image S

Output: Watermark Image P'

Step 1: Select the appropriate original image P of size MxN from the database.

Step 2: Load the original color image (RGB).

Step 3: Convert RGB to YCbCr.

Step 4: Apply SVD on any (0-7) bit of an original image.

Step 5: Select Y band to embed the watermark:-

5.1: Add to LL, HL, LH and HH separately

5.2: Add to (HL+LH) together

5.3: Add to (HL+LH) and some frequencies of HH

Step 6: Store the position of original image affected by watermark.

Step 7: Add secret image using LSB technique.

Step 8: Add secret key.

Step 9: End.

5.2 Data Extraction Algorithm

The data extraction process is that which convert the cipher text into the plain text by using a secret key. Mapping the pixels into an image is known as extraction method. The requirements for data extraction are watermarked image and the secret key [10]. For extraction process applies the inverse support vector dimension on watermarked image. With the use of a secret key the decryption is done only. Then it transfers the YCbCr to RGB image, form and calculate the PSNR values of the original image and watermarked image. Extract the original and the watermark image. The quality of the image doesn't degrade while decompression. The human eyes can't detect easily. It provides the high security to the secret image that cannot alter by hackers or intruder easily.

Algorithm for Extracting Process:

Input: Watermark Image P', Key K

Output: Secret Image S, original Image P

Step 1: Extract the Stego image and choose any no of bit of LSBs of Watermark image.

Step 2: Apply Inverse SVD on the Watermark image.

Step 3: Convert YCbCr to RGB.

Step 4: Find the PSNR fidelity measure between original image and watermarked images.

Step 5: Extract secret and Watermark images.

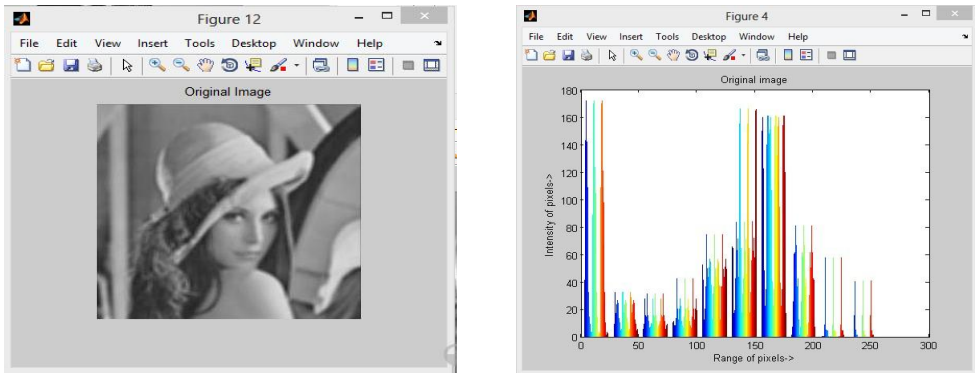
Step 6: Display the values of parameters PSNR and MSE between cover image and watermark image and also represent the graphs of PSNR and MSE after noise attack.

Step 7: End.

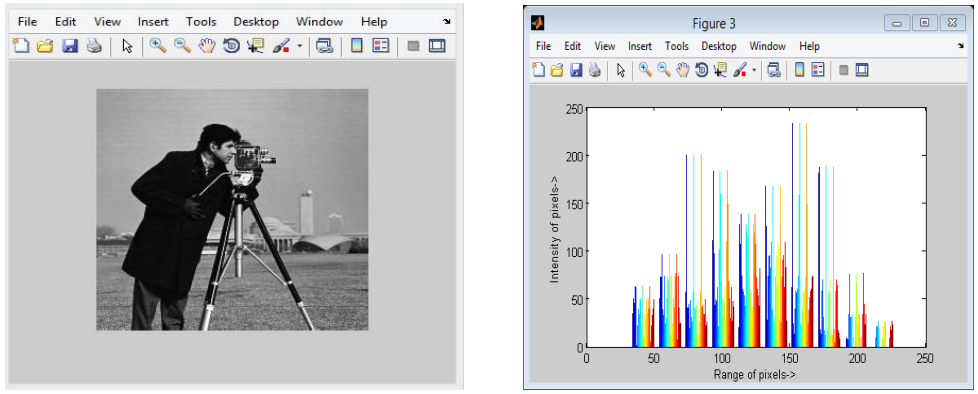
6. EXPERIMENTAL RESULTS

In this section represent the results of using proposed method cover image, hold the secret information inside it. Firstly, we choose the original image which is selected from the database. The original image and secret images are shown in the Figure 5 with their histograms. Naturally the stage that means Stego is looking similar as the original image, but with the use of histogram and visually looks like small changes due to the changes in the least pixel value of the image [13]. Steganography change the pixel value during embedding process and after extraction process also. A minor difference between original and watermark images that why we use the steganographic, cryptography and watermarking techniques that combined to provide much security for secret communication.

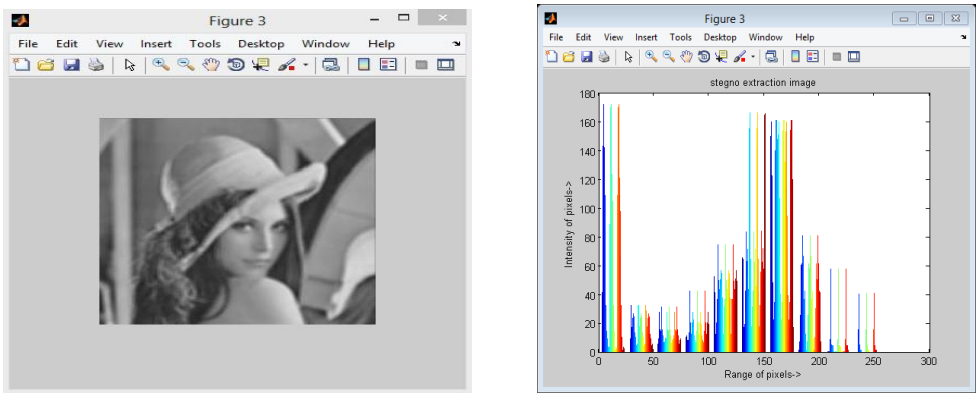
In which the watermark image that means stego image which is produced after the encryption process. The different attacks are applied to it for analyzing the capacity of an image. The sharpened attack, contrast attack and salt & pepper attacks are applied to the watermark image.



(a)



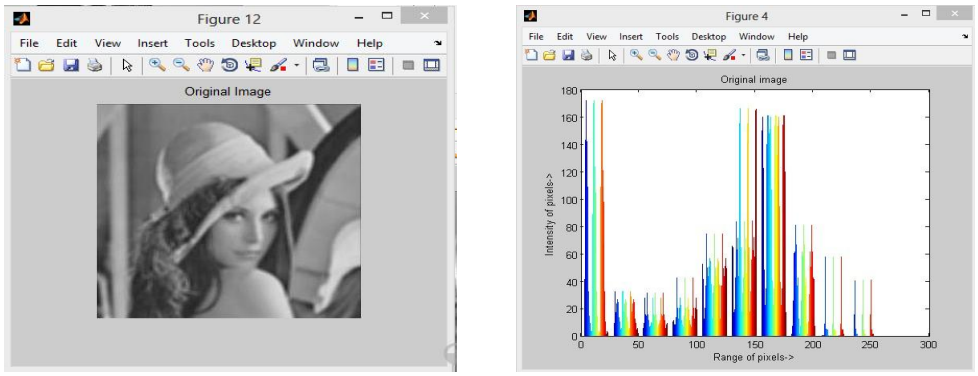
(b)



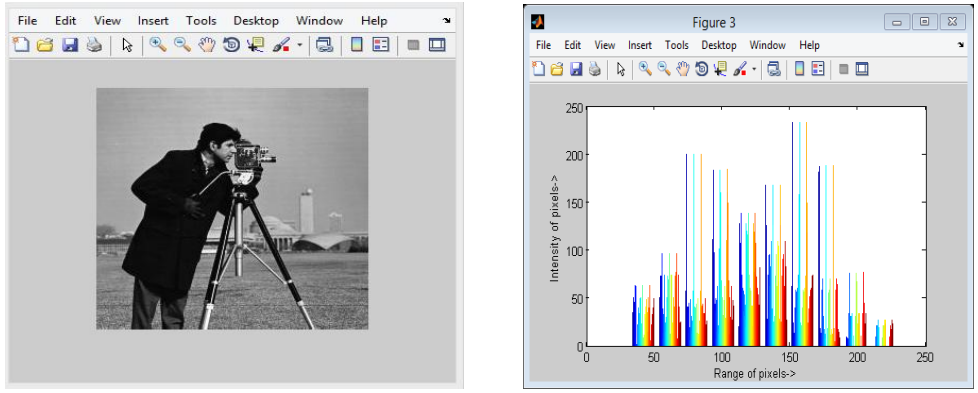
(c)

Fig 5. Original Image (a), Secret image(b) and Watermark image(c) with their histogram

Due to encryption process and decryption process the quality of an image should be degraded to preserve the quality of the image we are applying the attacks on the stage image and find the parameters such as PSNR and MSE. Due to increases the PSNR values and lesser the MSE values the image should be looking similar at the size and quality.



(a)



(b)

Figure 6. After Extraction the Original image (d) and Secret image (e) with their histogram

The steganography has very important factor which is Peak Signal to Noise Ratio (PSNR). The PSNR value shows the quality of an image that means if the image has higher PSNR values, that means the image has very good quality and similar as the watermark image and if the values of PSNR are low then the quality should be degraded and looks very identical to the watermark image.

$$PSNR = 10 * \log(255^2 / MSE)$$

Table 1. Parameter values of Proposed Method

Features	Proposed
Security	High
MSE	Low
PSNR	High
Robustness	High
Imperceptibly	High

Payload Capacity	Medium

$$MSE = 1/mn \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [f(x,y) - g(x,y)]^2$$

To evaluate the Peak Signal to Noise ratio then firstly we find the Mean Square Root Error (MSE) values. We find the muse, value of the reconstructed image and if the image having a low MSE value that means there are lesser error ratios between original and watermark image. And if the image having a high error ratio between original and watermark image [11]. The various attacks which are applied in the watermark image shows the bar graphs in the Figure 7 & Figure 8.

The proposed technique is evaluated the various parameters such as high security and high robustness and high imperceptibility and lower MSE and High PSNR values. The parameters are used for providing much security and unnoticeable the difference between original and watermarked image [12]. This is the best technique for covert communication for applying least bit significant technique (LSB) on the images.

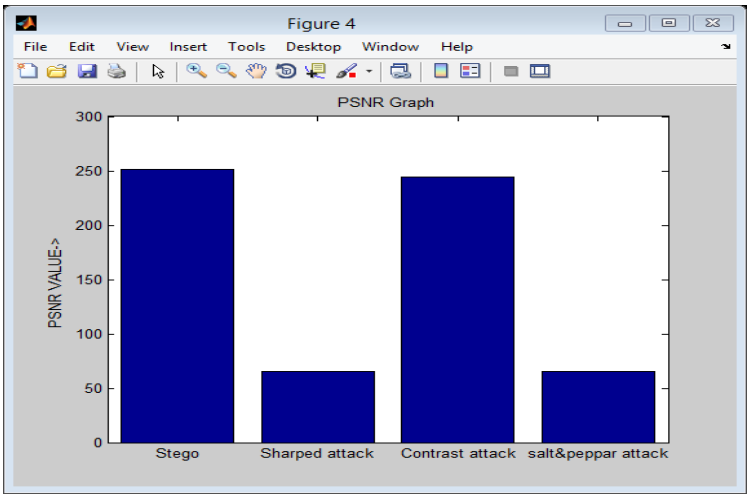


Fig 7. PSNR Results

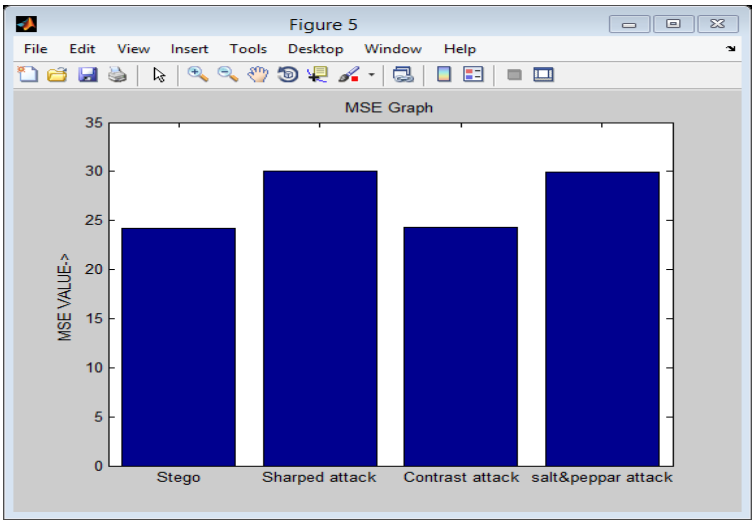


Fig 8. MSE Results

7. CONCLUSION

This paper explained the terms cryptography steganographic and watermarking that are used for data hiding. In this paper, it successfully embeds the data into 8-bit image. These are combined and become a powerful tool to which provide much security for secret communication. In this paper we compute a technique that covert the RGB image to YCbCr and apply support vector dimension at least bit of the image on encryption side. On the decryption side apply inverse support vector dimension at least bit of the image. Apply some attacks on the watermarked image that simply alter the bits of secret image directly into the LSB plane of the original image that is the reason which is not easily noticeable by publicly. In this paper the parameters which are evaluated such as PSNR and MSE that provide better results than the related work. For future work apply the new techniques for secret communication that provides much security.

8. ACKNOWLEDGMENTS

I would like to thank all the individuals whose support and encouragement have made the completion of this work possible. The paper has been written with the kind assistance, guidance and active support of my department who have helped me in this work.

9. REFERENCES

[1] Amirtharajan, R., R. Akila, and P. Deepikachowdavarapu. "A comparative analysis of image steganography." International journal of computer applications, Vol. 2, No.3, 2010, pp: 41-47.

[2] Huayong, Ge, Huang Mingsheng, and Wang Qian. "Steganography and Steganalysis based on the digital image." Image and Signal Processing (CISP), 2011 4th International Conference on. Vol. 1. IEEE, 2011.

[3] Nagaraj, V., Dr V. Vijayalakshmi, and Dr G. Zayaraz. "Modulo based Image Steganography Technique against Statistical and Histogram Analysis." IJCA Special Issue on "Network Security and Cryptography" NSC,2011.

[4] Jagwinder Kaur and Sanjeev Kumar, "Study and Analysis of Various Image Steganography Techniques", IJCSIT, Vol. 2,No. 3, 2011.

[5] J.J.Garcia-Hernandez, "Exploring reversible digital watermarking in audio signals using additive interpolation error expansions,"in The Eighth International Conference On Intelligent Information Hiding and Multimedia Signal Processing,I.C.Society,Ed.Vol. 8,2012.

[6] Ramaiya, Manoj Kumar, Naveen Hemrajani, and Anil Kishore Saxena. "Improvisation of Security aspect in Steganography applies DES."*Communication Systems and Network Technologies (CSNT), 2013 International Conference on*. IEEE, 2013.

[7] Dagadita, Monica Adriana, Emil-Ioan Slusanschi, and Razvan Dobre. "Data Hiding Using Steganography." *Parallel and Distributed Computing (ISPDC), 2013 IEEE 12th International Symposium on*. IEEE, 2013.

[8] Huang, Fangjun, et al. "Distortion function designing for JPEG steganography with uncompressed side-image." *Proceedings of the first ACM workshop on Information hiding and multimedia security*. ACM, 2013.

[9] Jing Liu, Guangming Tang, Yifeng Sun., A secure steganography for privacy protection in healthcare system. Springer, New York, 2013.

[10] P. Thiyagarajan, G. Aghila."Reversible dynamic, secure steganography for medical image using graph coloring,"Health Policy and Technology, Vol.2, No.3, 2013, pp. 151-161.

[11] Mansi S. Subhedar, Vijay H. Mankar."Current status and key issues in image Steganography." A survey of computer science review, Vol. 13-14, 2014, pp. 95-113.

[12] Jung, Ki-Hyun, and Kee-Young Yoo. "Steganographic method based on interpolation and LSB substitution of digital images," Multimedia Tools and Application, 2014.

[13] Mahajan, Palak, and Ajay Koul. "CEET: A Compressed Encrypted & Embedded Technique for Digital Image Steganography,"IOSR Journal of Computer Engineering, VOL. 16, NO. 2, 2014, pp. 44-52.