A Novel Method for Security of Image Base on Image Steganography Using Hybrid Method

1. Makvana Varsha p 2.Prof.Dr. Kalpesh Wandra

Student, Computer Engineering, C.u.shah collage of engineering & technology, Gujarat,
Dean, Faculty of Tech. & Eng. C.U. Shah University, Gujarat, India

ABSTRACT

Steganography is going to achieve its reputation due to the exponential growth and secret communication of potential computer users over the internet. In this research work, the stenographic is the method or process in which the useful information or data, concealing into another form such as image, text, audio and video. The purpose of it is to carry out secure communication of secret information through internet generally data embedding is achieved in communication, image, text, voice or multimedia content for copyright, military communication, authentication and many other purposes. Breakdown the carrier objects to bring the hidden information it is called steganalysis. LSB replacement is the important and simplest method of image steganography. This paper is used the spatial domain method LSB and the transform domain method DWT.

Keyword: *Steganography*; *LSB*; *cover writing*; Frequency Domain, Spatial domain.

1. Introduction

Since in old day the writing it was necessary to provide medium to secure the confidentiality of written correspondence and to have some means that can detect tempering. There are various methods for information security was introduced from time to time and had undergone Ease of Use [1, 2]. Information security main purpose is Data Confidentiality, Data Integrity, and Authentication. So whatever you send your privet data in communication channel you must take care about of your data. In the computerized world we live so it may possible that unwanted person can gather your data and miss use your data. So high security of the information it is required [1, 2, 3, 10]. Steganography and cryptography is two methods which is used to share the information in protected way.

Steganography is the word is the combination of the two Greek Word which is Steganós, and Graptos. The meaning of steganos is covered or hiding and the meaning of graptos is writing and drawing. So the meaning of the steganography is "covered drawing" or "hiding Writing" [4, 5].Steganography is the art of the undetectable communication. Steganography is one such pro-security mechanism that implanted in way so that the occurrences of secret data are not view (hidden). Steganography systems use multimedia objects like Image, audio, video to hide the secret information. [1, 5].

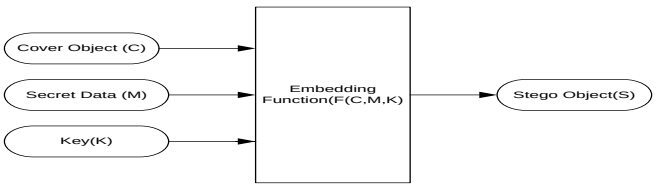


Fig 1: Basic process of steganography

In fig 1 we see the basic model of the steganography. This model is giving the idea about the steganography process. The steganography is containing the four part cover object, secret Data, key and Stego object. Cover object

is known as Carrier objet it is used to put the hidden information on it. The secret data may be any digital media like (text message, image, audio, and video) the communication creator wants to send and secured form unauthorized person. Key is also known as password, it is used to rises the security of steganography process. This decoding key is known only by the receiver so it is able to extract the secret data form object. The output of this process is stego object which is the cover object with the secret message

Cryptography is the art of coding and decoding secret message Cryptography is scrambling the message using the different method so they cannot be understood. Cryptography is change the secret message forms the one from to another from so this is not understood by the unauthorized person [6].

Fig 2: Sample of Cryptography

Steganography and cryptography both are the information security method but not equal to each other [1, 5, 6]. The main differences of that in steganography the secret data is hidden but in cryptography the secret data is shown by the person in non-detected from. [5, 10] .

To rises the level of the safety together the process is used to develop the better protection of secret message. In mixture system first the message is encrypted using the cryptography and then it hides using the steganography. In this case when the steganography is fail due to processes of steganalysis (Break down the carrier object to bring the hidden information) it is still not use because it is encrypted using the cryptography.[5,7]

2. Type of Steganography

Steganography is divided in the different type according to the carrier object is used to hide the secret information. [1, 7, 10].Multimedia is used as the cover object. The cover object is chosen that give the high degree of redundancy [3]. There are four category file format like image, text, audio, video use for information hiding [5, 7, 10].

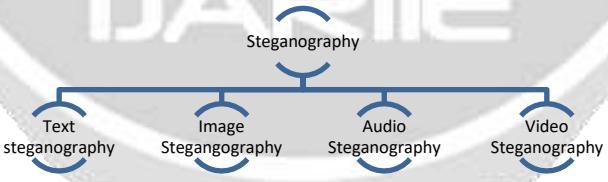


Fig 3: Type of Steganography

Today the large amount of people use image as the data in the internet so image use as carrier object and image is the numerical representation of data so we can say one image is contain the more number of data so it provide the more hiding capacity. It also takes the advantages of the human visualization system.

In image Steganography it is dividing in the two type's spatial Domain steganography and transforms domain steganography [8].

Spatial Domain Method: The spatial domain techniques are manipulating the cover image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. Consequently, the spatial domain techniques are simple and easy to implement [9]. The Least Significant Bit (LSB) is one of the main

techniques in spatial domain image steganography. The simplest and most popular image Steganography method is the LSB Method. . LSB Replacement provides high embedding capacity. In LSB replacement, most significant bits (MSBs) of the secret information are replaced with LSBs of pixels of the cover image. Cover image LSB bit modifying change is not detected by human eye because the amplitude of change is small [1, 2, 3, 4, 5, 6, 8, 9, 10].

Transform domain method: Transform domain also known as frequency domain, such as the Discrete Cosine Transform (DCT) [1, 3, and 9], Discrete Fourier Transform (DFT), or Discrete Wavelet Transform (DWT) [11, 12]. This is a more complex way of hiding information in an image. Various algorithms and transformations are used on the image to hide information in it.it

This paper is present a novel method for image steganography used LSB,DWT and Huffman coding .I use the color image for this . The first image is secret image and second image is cover image. I apply the DWT method on the secret image and then apply the 2D-WWT to each band and compression of each band is done using the Huffman coding and the output image is compressed image. This output image is embedded into cover image using the LSB method.

3. Norm of Steganography

The steganography is the procedure of hiding the data inside the cover object using the steganography principal and the result is the stego- object that is send to the receiver. The receiver is taking out the secreted information from stego object using extract algorithm [7].

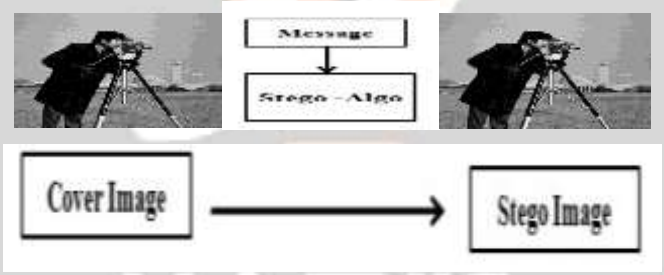


Fig 4: The Norm of Steganography

The norm of steganography method is shown in Fig.4. The principal is saying that the implanting process is done in this way that try to keep the sharp properties of the cover image. The privet information is implanted inside cover image in a way that does not variation properties of cover image in a person's visualization system. The production is new image called stego-image that is looks identical as the cover image.

4. Key Properties of Evaluation method

As we seen in the norm of the steganography it say that the change in the cover image it is done in the way that the cover image and stego image is look similar. The Change in the cover image is not detected by the human eye. The important key properties required in steganography method.

Embedding Capacity: The amount of secret information is can be embedded without humiliation of quality of image. The amount of data that i embedded it lesser as possible because more information more the image has changed. It is easier to Steganalyst to discover the cover image is modified [13].

Imperceptibility: It is also called as invisibility. It is the things in which a person should be unable to differentiate the original and stego object. The stego object that is generated it not be different such that it is visualized by human eye. Always try that the output image (stego-image) is very much similar to cover image [13].

Robustness: It is main aim is that the Steganalyst it have difficulty to determine that the image conations the hidden information or not. To the degree of difficulty required to destroy embedded information without destroying the cover object. A good steganography method is exposed to many attacks that is demonstrates unfounded [13].

Independent of file format: The algorithm it should be intelligent to use different file format for the used as a cover object [10].

5. LITERATURE SURVEY

In 2011 Masoud Nosrati and Ronak karimi, Mhedi Hariri [7] they explains the various type of steganography according the carrier object is selected to hiding secret information. It has provided the base for steganography and help to understand the each method of it.

In 2014 Kanzariya Nitin k [3] The DCT (Discrete Cosine Transform) method used to provide randomness. DCT coefficient method it is used to select the random location of cover objects to hide the secret information.it find the potential location to hide the data using LSB method. Hash function it also used to give the randomness to hide the data [6].

Himanshu Gupta, Dr. Soni changlani [9] it uses LSB method for hiding the data. In LSB On average about half of the bits in the cover image will be modified when embedding the secret image. .However, increasing *n* distorts stego-image. So after this paper study we can say that 2/3 LSB pixel change it is give good stego image.

Ashish Nimavat, Nitin Kanzariya k in 2014 [1] they design hybrid method is the combination of spatial domain LSB method and frequency domain DCT method. The simple LSB method is not secure to provide the randomness this combination is used. Huffman coding is used for lossless secret image compression. Huffman coding it help to increase the PSNR values. The X-box mapping method it used to provide the high embedding capacity [5].

Preeti Kumari and Ridhi Kapoor [14] in 2016 this paper author it used the image compression, encryption and image steganography to provide better image steganography. This method it offers much security and unnoticeable differences between cover image and stego image. This combination it is provide powerful method that provide much security for stealthy communiqué.

In [10] this paper the comparison of the various image steganography techniques is done .This paper author concludes that the agent deicide which steganography method it used then they also has to decide the image file format.

Shrusti Porwal in 2013 [15] paper is giving information the data compression is the two types: lossless and lossy. The Huffman coding and arithmetic coding is used for lossless data compression in this paper the differences of this two compression is given. Huffman coding it has high compression ratio.

In 2012 Nlanjan Dey [12] is used the frequency domain method to hide the multiple secret image. In this first the color image is divide in 3 panel and the apply the DWT method to each panel and DCT method it is apply to HH band of image.it give the high robustness.

Sunil malviya in 2013 it [11] it is design novel method for image compression using the Arithmetic coding method. The 2D-Walsh-Wavelet Transform (WWT) is applied on each 8x8 block of the low frequency sub-band. Firstly dividing each sub-band by a factor and then apply Arithmetic Coding on each sub-band independently. The Walsh Wavelet Transform with arithmetic coding is capable to reduce the redundancy of image.

6. PROPOSED MODEL

The proposed model is work for hiding the secret image in the cover image. In this method I used the embedding algorithm which is hide the secret image into cover image. In this strategy, secret image is compression is done using Huffman coding and DWT method and LSB method to inserted the data to produce the stego image.it provide the stego image more security and good Robustness it provide.

6.1proposed method

Least Significant Bit Replacement: The Least Significant Bit (LSB) is one of the main techniques in spatial domain image steganography. The simplest and most popular image Steganography method is the LSB Method [1, 2, 3]

LSB Replacement provides high embedding capacity. In LSB replacement, most significant bits (MSBs) of the secret information are replaced with LSBs of pixels of the cover image. Cover image LSB bit modifying change is not detected by human eye because the amplitude of change is small [5, 6, 7, 9].

For example a bit pattern for 9 pixels of an 8-bit color image can be as follows: Suppose the first three pixels of the original image have the following values:

[1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 0 1 1 1 0 1 0 0 1]

[1 0 1 0 0 1 1 0 1 1 0 0 0 1 0 0 0 0 0 1 1 0 0]

[1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 1 0 0 0 1 0]

And that of secret image first three pixels is having the following values.

[1 1 1 0 0 1 0 1 1 0 1 1 0 1 1 0 1 1 1 1 0 0 0 1]

The first pixel of secret image is 167 its binary representation 11100101, is embedded into the LSBs of this part of an image, the resulting bit pattern will be as follows:

[1 1 0 0 1 0 0 1 1 1 0 1 1 1 1 1 1 1 1 0 1 0 0 1]

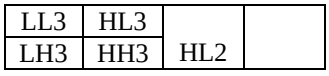
[1 0 1 0 0 1 1 0 1 1 0 0 0 1 0 0 0 0 0 1 1 0 1]

[1 1 0 1 0 0 1 0 1 0 1 0 1 1 0 1 0 1 1 0 0 0 1 0]

Although the 8 bits were inserted in first 8 pixels from trace of an image, only the 2 underlined (highlighted) bits need to be modified. On an average, simply half of the pixel values in an image need to be modified while embedding the secret information. We have 256 possible intensities of 8 bit color image, changing the LSB of a pixel results in small changes in this intensity value. Such modifications cannot be identified by the human eye, thus the secret information is hidden into the carrier successfully.

Discrete Wavelet transformation: This transformation is an extremely necessary way to be used for signal investigation as well as image processing, mainly for multi-resolution demonstration. It may crumble a signal into a number of constituents in frequency domain. 1-D DWT segments a cover image further into two major components known as approximate component and detailed component . A 2-D DWT is used to segment a cover image into mainly four sub components: one approximate component (LL) and the other three include detailed components represented as (LH, HL, HH).

Architecture and algorithms of Discrete Wavelet Transformation for image compression is given below:



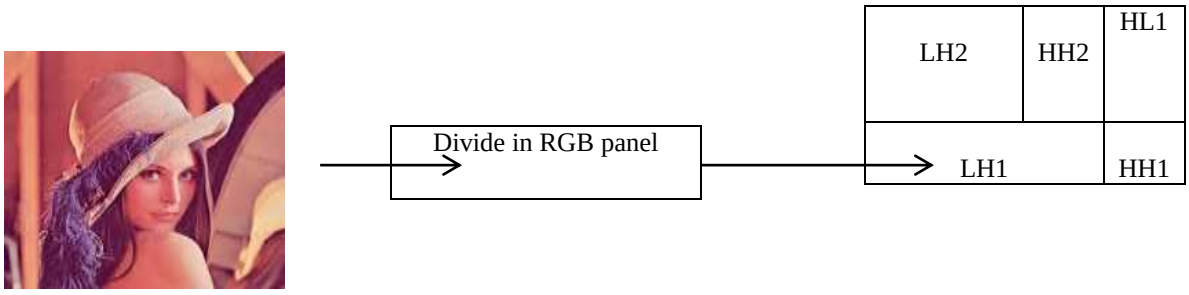


Fig.5: Three phase decomposition using DWT.

Discrete Wavelet Transformation has its individual excellent space frequency localization property. Applying DWT in 2D the input image is divided into 4 non-overlapping multi-resolution sub-bands, namely LL1 (Approximation coefficients), LH1 (vertical details), HL1 (horizontal details) and HH1 (diagonal details). The sub-band (LL1) is processed further to obtain the next coarser scale of wavelet coefficients, until some final scale "N" is reached. When "N" is reached, we'll have 3N+1 sub-bands consisting of the multi-resolution sub-bands (LLN) and (LHX), (HLX) and (HHX) where "X" ranges from 1 until "N" [12].

Huffman Encoding: Huffman encoding is the efficient and lossless data compression method.in Huffman coding the character it is converted into the binary code to compress data. Huffman Encoding reduces the amount of bits for every pixel .it is the popular method to remove the redundancy of data. Huffman codes are optimal codes that guide one symbol of cover image to one code word [5].

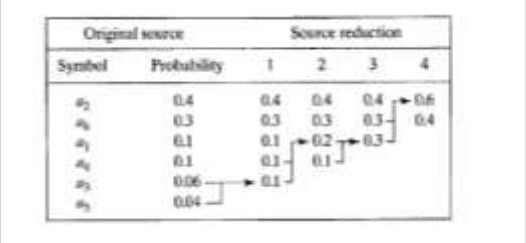


FIG 6: STEP -1 Huffman Encoding

In step-1 create a series of source reductions by ordering the probabilities of the symbol under consideration and combing the lowest probability symbols into single symbol that replaces them in next sources reduction.

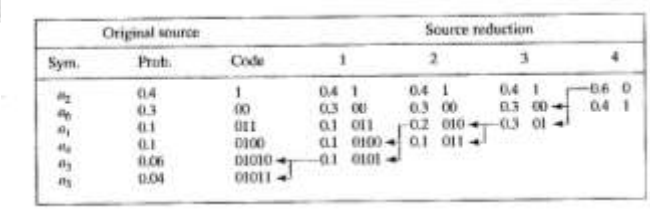


Fig 7: STEP -2 Huffman Encoding

In step-2 Huffman procedure is to code each reduced source starting with source and working back to the original source.

6.2 Proposed algorithm

Embedding Algorithm:
Input: A select the cover image and secret image
Output: Stego image

Step 1: Choose the input image (secret image) from database which you want to compress.
Step 2: Divide selected input image into 8x8 blocks.
Step 3: Apply two levels discrete wavelet transforms.
Step 4: Apply 2D Walsh Wavelet Transform on each 8x8 block of the low-frequency sub-band.

Apply Walsh Wavelet transform and then using Huffman Coding for compress an image.
Step 4 consists of the following:
4.1. Two Levels Discrete Wavelet Transform.
4.2. Apply 2D Walsh-Wavelet Transform on each 8x8 block of the low frequency sub-band.
4.3. Split all values form each transformed block 8x8.
4.4. Compress each sub-band by using Huffman Coding, the first part of Walsh Wavelet compression steps for high frequency, domains, and then second part of Walsh Wavelet compression steps for low frequency.

Step 5: Split all DC values form each transformed block 8x8
Step 6: Apply for compression each sub-band by using Huffman coding.
Step 7: Output image obtained by the compression.
Step 8: Select the Cover image.
Step 9: Hide the output image step 7 using LSB method.
Step 10: Evaluate the stego image.

Recovery Algorithm:
Input: A Stego-image.
Output: Secret image.
Step 1: Identify the potential pixels from the stego image using which is change due to LSB.
Step 2: Retrieve the secret bits from each potential pixel of the stego image.
Step 3: Generate the Secret Image.

At the receiver side, some parameters are required for retrieval of secret image from stego image:
1) Size of Secret Image.
2) Number of bits stored for secret image data.
3) Number of bits replaced in carrier image
4) Key matrix if used for compression.

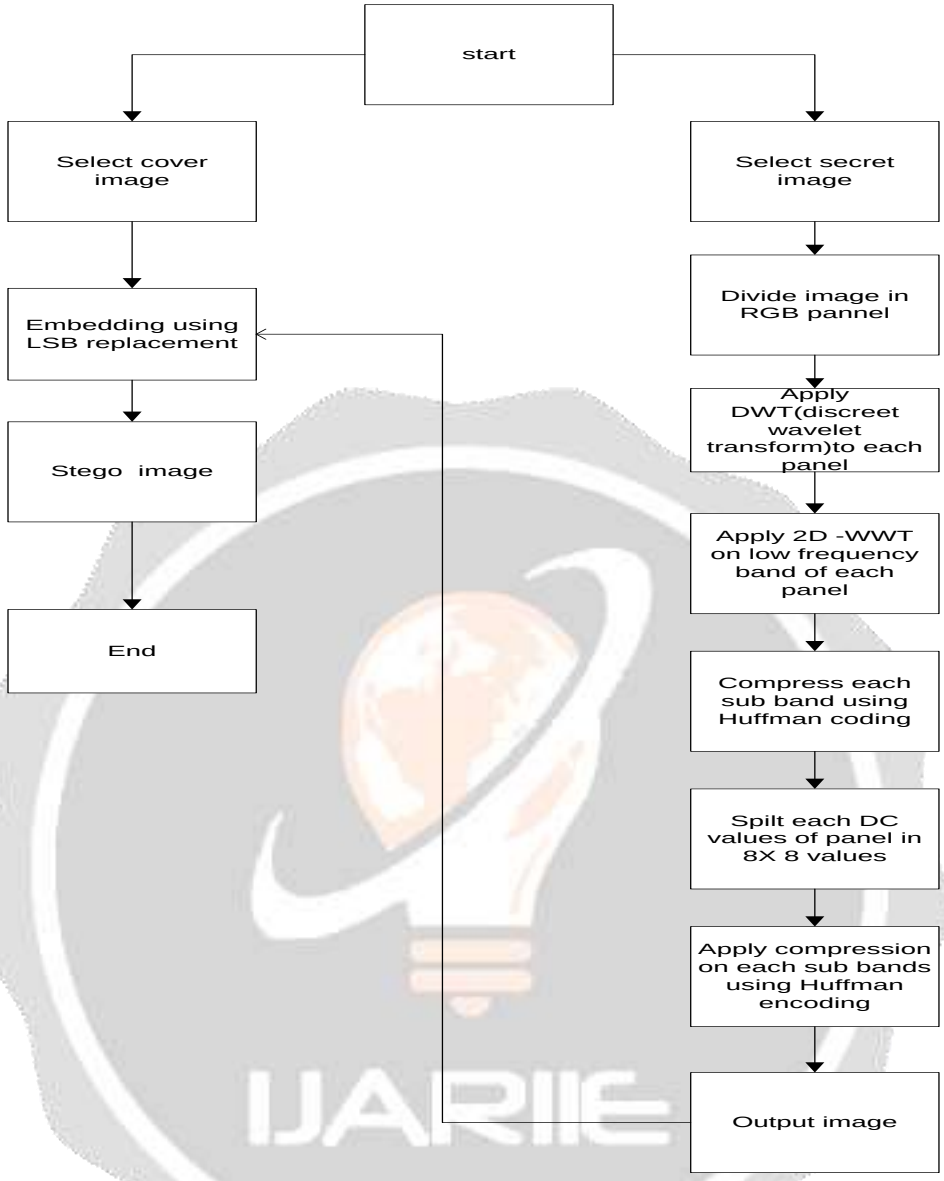


Fig 8: Flow Chart of Embedding Algorithm.

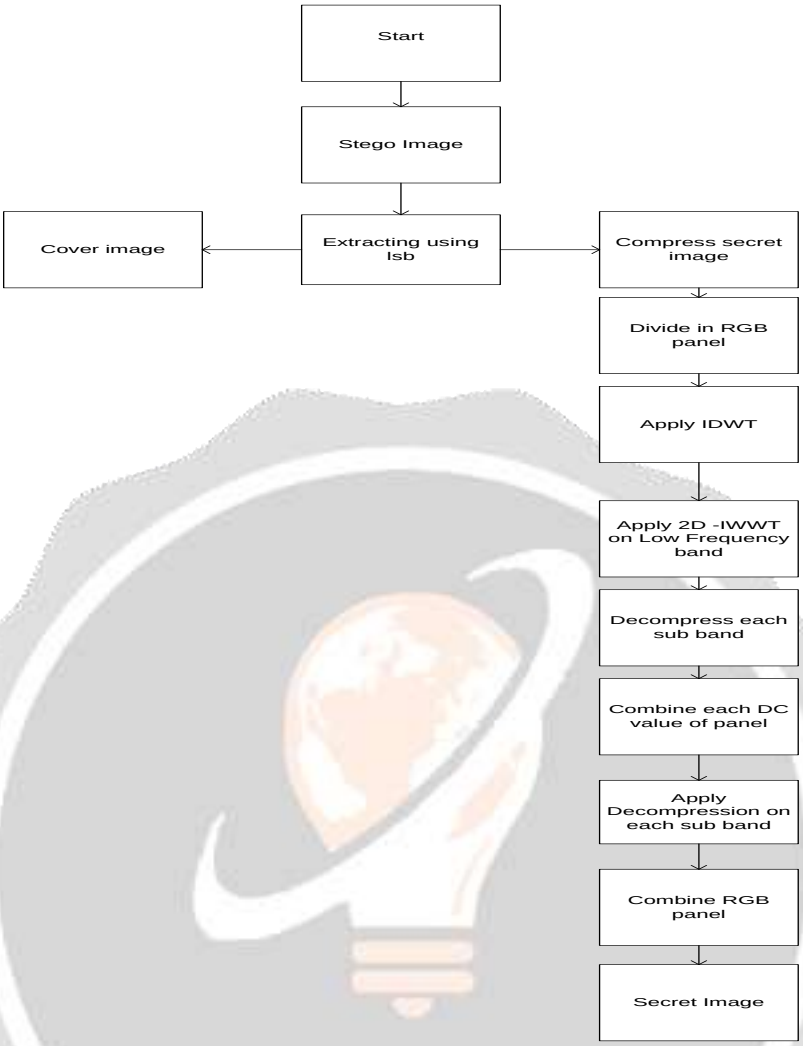


Fig 9: flow chart of recovery algorithm

7. RESULTS AND ANALYSIS

For the performance analysis of the proposed algorithm i first chose the secret image. The image is must be a RGB color image. Then the compression of this image is done the output image of this image hide in the cover image using LSB method. It generated the stego image show that the stego image is look similar as cover image.

Fig 11: select secret image

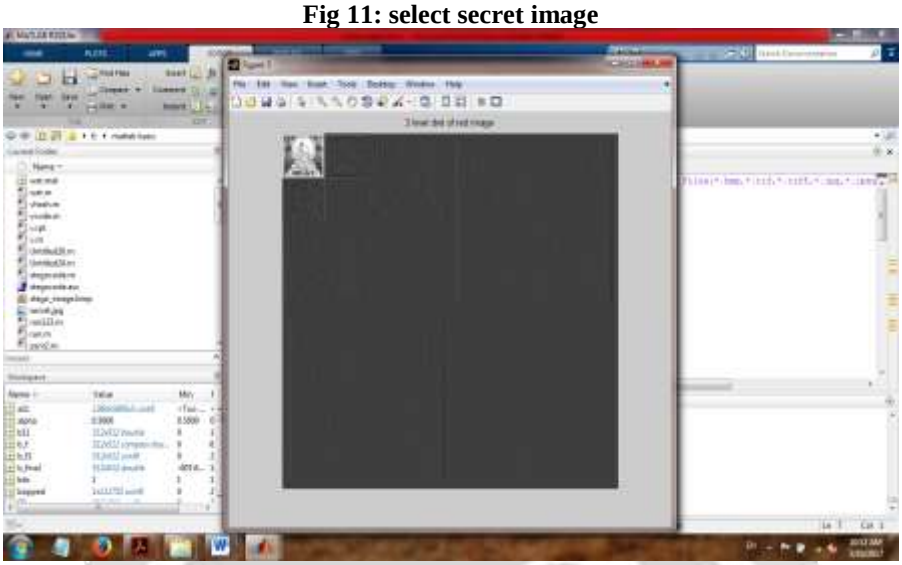


Fig 12: 3 level DWT transformation

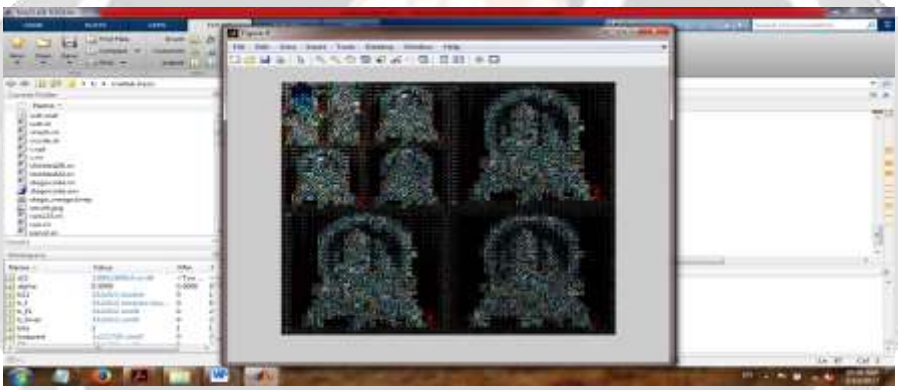


Fig 13: output image of compression method

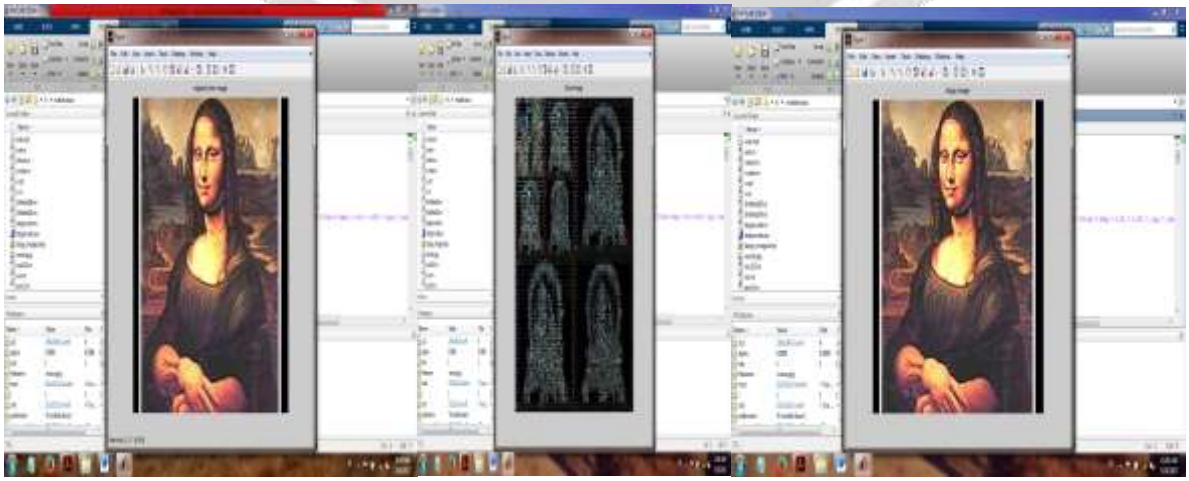


Fig 14: image steganography process

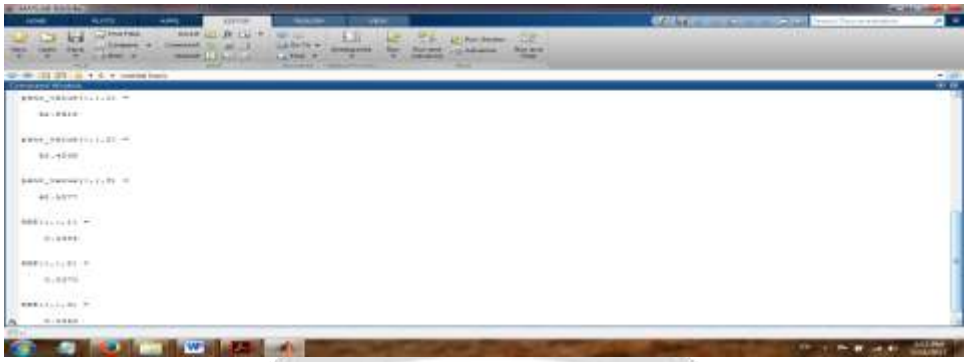


Fig 15: Result of PSNR and MSE

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.

PSNR = 10X log(255 ^2/ MSE)

The mean square error is used to measure the difference between the estimated values and true value for estimated quality.

$$MSE = \frac{1}{NxM} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [X(i,j) - Y(i,j)]^2$$

Table 1. Parameter values of Proposed Method:

Features	Proposed
Security	high
MSE	low
PSNR	high
Imperceptibly	high

7. CONCLUSIONS:

In this paper i work for the image security. i chose the steganography to hide the image. First the secret image compression is done. In this paper the compression method and framework that use Walsh wavelets transform with Huffman coding technique to remove redundancy from image. The steganography is covert communication to protect confidential information.in this paper LSB, DWT and Huffman encoding use. LSB is

simple replacement technique .DWT it is frequency domain method. Huffman encoding is lossless compression technique. The algorithm it enhance the security of image. According to the result the stego image of proposed method are almost same to cover image and it is difficult to differentiate them. It is not easily decode by any person .Security is high due to use of DWT and Huffman encoding.

8. References

1. Nitin Kanzariya, Ashish Nimavat and Hardik Patel, "Security of Digital Images using Steganography Techniques based on LSB, DCT and Huffman Encoding" Elsevier,(Page No.349-359),(ISBN:987-93-5107-184-6).

2.Masour nosrati ,Ronak karimi ,and Mhedi Hariri, "An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011.

3. Nitin Kanzariya and Ashish Nimavat, "A Novel Technique for Image Steganography Techniques Based on LSB and DCT Coefficients" - International Journal for Scientific Research & Development| Vol. 1, Issue 11, 2014 | ISSN: 2321-0613(Page No. 2405-2408).

4.Dr.S.Bhargavi, Anughna.N ,Swetha.T.N," "An Efficient Stenographic Method For Generating Stego Image Based On RSA Algorithm and HASH LSB Technique.International Journal of Research In Science & Engineering, Volume: 1 Special Issue: 2

5.Kanzariya Nitin k, Nimavat Ashish V, Jadeja Vijaysinh K , "highly secure images steganography techniques based on LSB,X-BOX Mapping and Huffman encoding", International Journal of Computer Science Engineeringand Information Technology Research (IJCSEITR),Vol. 4, Issue 6, Dec 2014

6.Anil Kumar , Roshni Sharma," A Secure Image Steganography based on RSA Alorithm and Hash- LSB Techniques",International Journal of Advanced Research in Computer Science and Software enginnring,july 2013.

7.Masour nosrati ,Ronak karimi ,and Mhedi Hariri, "An introduction to steganography methods", World Applied Programming, Vol (1), No (3), August 2011.

8.Rejani. R, Dr DMurugan,deppu V Krishanan , "Comparative study of spatial domain image steganography techniques", Int J Advanced networking and application,volume -07,issue:02,2015.

9.Himanshu Gupta , Dr Soni changlani, and prof Ritesh Kumar , "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging Technology and Advanced Engineering, June 2013.

10.Nitin Kanzariya and Ashish Nimavat, "Comparison of Various Images Steganography Techniques" International Journal of Computer Science and Management Research (Page No. 1213– 1217)(ISSN 2278-733X)

11.Sunil malviya,neelesh gupta,vibhanshu shirvastava "2D-Discrete Walsh Wavelet Transform for Image Compression with Arithmetic Coding" IEEE-31661

12.Nilanjan Dey, Tanmay Bhattacharya, S. R. Bhadra Chaudhuri " A Session based Multiple Image Hiding Technique using DWT and DCT" International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012

13.C.P.Sumathi, T.Santanam, G.Umamaheswari "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

14.Preeti Kumari,Ridhi Kappor ,"Image Steganography for data embedding & extraction using LSB technique", International Journal Computer Applications & Information Technology Vol. 9, Issue 2, July 2016"

15. Shrusti Porwal, Yashi Chaudhary, Jitendra Joshi, Manish Jain"Data Compression Methodologies for Lossless Data and Comparison between Algorithms" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 2, March 2013