IMAGE STEGANOGRAPHY: A CONCEPTUAL STUDY OF DIFFERENT TECHNIQUES

[1]Jyoti Pandey, [2]Kamaldeep Joshi, [3]Harkesh sehrawat, [4]Rainu nandal
[1]M.Tech. Student, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor,
[1]UIET, MDU, Rohtak, India.

Abstract- In the era of internet, a large number of important files is shared through the internet. These files are of great significance from the point of view of privacy. So proper security is needed in order to achieve the secure transfer of files, many different techniques are used so that data in these files can't be intercepted by the third party. To achieve security, different technologies like cryptography and steganography are used. In cryptography, information is encrypted but its existence is not hidden. But in Steganography, the existence of secure information is also hidden. Steganography is the novel and decent technique of embedding important secret information in the cover medium like text, audio, video etc. The main use of steganography is to hide the important information as well as its existence from the third party. This paper discusses image steganography and various techniques used in image steganography. In image steganography, to achieve the secure transfer of information, the message is embedded into an image which acts as a cover image and after applying different steganography techniques, a stego-image is generated that contains the hidden information. There are various techniques of image steganography like Spatial Technique, Transformation Technique, Distortion Domain Technique, Masking and filtering etc.

Keywords- Steganography, stego-image, Spatial Domain Technique, Transform Domain Techniques, Distortion Domain Techniques, Masking and filtering, Magic LSB, Cyclic LSB.

I. INTRODUCTION

The word" Steganography" is originated from Greek word "Steganos" means "cover" and "graphia" means "writing"[1]. In Steganography, presence of information is hidden into other source of information using different cover medium like image, audio and video etc. Images are primarily used for hidden information in image steganography. The information is hidden into an image called cover image. The image in which information is hidden is called stego-image's [2].

The Main objective of steganography is to transfer secret information so that this information is invisible to unauthorized users. In history, there were several secret communications like undetectable ink, microdots, spread spectrum, character organization etc. [3]. But now a days, digital steganography is used achieve secret communications. Description of several image steganography techniques is given in this paper. These techniques have high level of information security and data hiding capacity is very high.

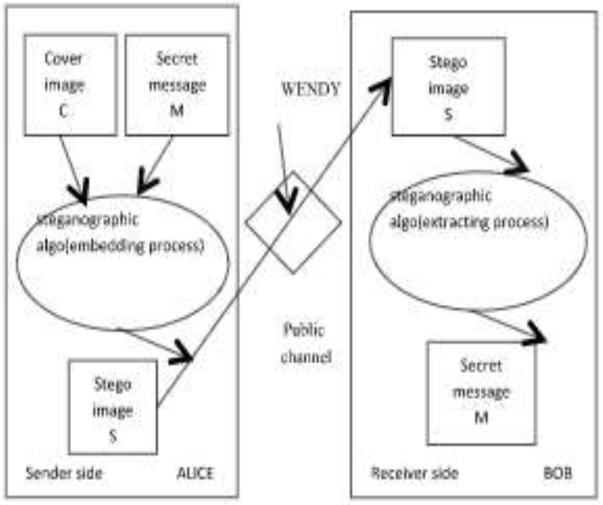
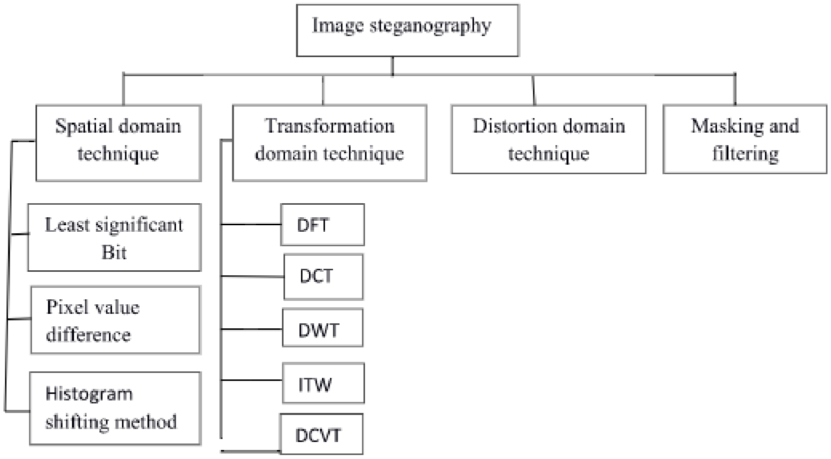


Figure 1: Basic Steganography Model

2. TECHNIQUES OF IMAGE STEGANOGRAPHY

The categorization of the steganography techniques are shown by figure 2:



2.1. SPATIAL DOMAIN TECHNIQUES:

Embedded of secret information into image is done by altering the intensity of various image pixels in this spatial domain techniques. Bits can be embedded simply or randomly. By using this technique, filtering, smoothing filters or unsharp masking can be done to hide the secret information in image. Encoding in spatial domain method is done through Least Significant Bits. LSB of every intensity of pixel is changed and secret data is embedded into the image. Variations in LSB are nearly unnoticeable to human vision [4].

Different methods of Spatial Domain Techniques:

1. Least Significant Bit
2. Pixel Value Difference
3. Histogram Shifting Method
4. Pixel Indicator Technique
5. Cyclic LSB
6. Magic LSB
7. Edges Based Data Hiding Methods
8.

2.1.1. Least Significant Bit:

In this method, first binary value of every pixel of cover image is determined and then its LSB is take .than this LSB is converted into another wait which contains the message to be embedded. Before embedding, the required message, is which has to be transferred, is converted into sequence of bits [5]. If embedding rate is low, then this steganography is detectable. This method is prone to Steganalysis detection and can't withstand against compression.

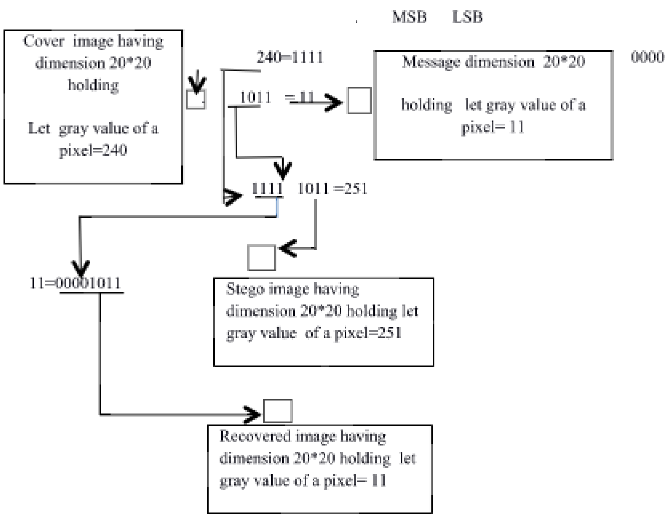

MSB LSB
Cover image having dimension 20*20 holding
Let gray value of a pixel=240
240=1111
1011 =11
Message dimension 20*20
holding let gray value of a pixel= 11
0000
1111 1011 =251
11=00001011
Stego image having dimension 20*20 holding let gray value of a pixel=251
Recovered image having dimension 20*20 holding let gray value of a pixel= 11

Figure 3: LSB technique for Steganography.

Figure 3.1 and 3.2 show the cover image lenna with its stego image.

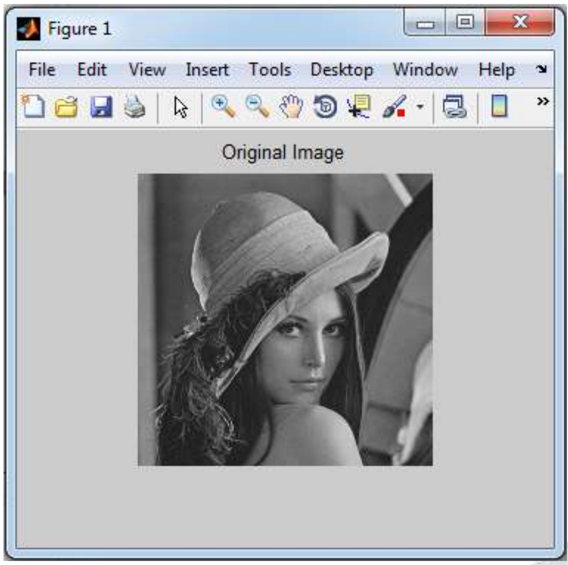


Fig 3.1: Original Image

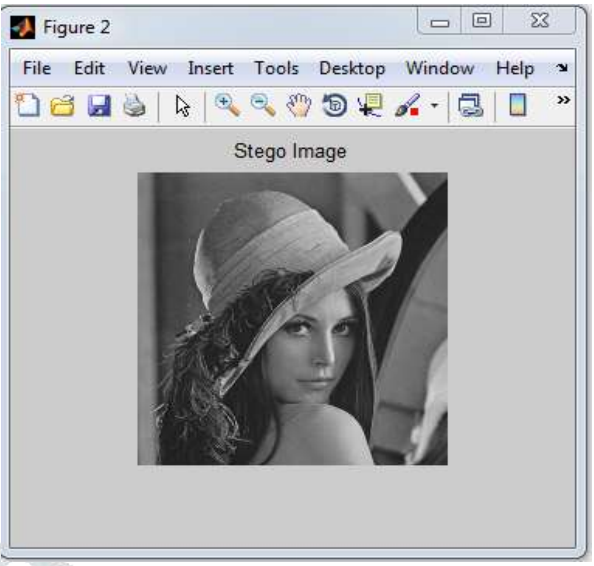


Fig 3.2: Stego Image

2.1.2. Pixel Value Difference:

In the Pixel Value Difference (PVD) method, to find how many bits can be embedded into cover image, difference of two pixels is used. These pixels should be consecutive. The benefit of choosing consecutive pixel is that these pixels will provide high imperceptibility to stego-image [6]. This method is advantageous because nearly all characteristics of original image remain intact in stego-image. PVD is so designed such that the gray scale range interval is not violated by pixel modification.

2.1.3. Histogram Shifting Method:

N. Akhtar et al. 2013 presented image graphically, Histogram are used. Value of pixel as well as its density can be represented by histogram. Distribution of pixel, colors density and tonal distribution can be identified by histogram. Tonal distribution is represented on horizontal axis of histogram whereas numbers of pixel are represented on the vertical axis of histogram. Highest and lowest pixel values of graph can be determined by histogram. In this method, a certain group of pixels of image are modified [7]. These pixels are so modified that they always lie in maxima and minima limit. Maxima and minima are highest and lowest value of histogram respectively.

2.1.4. Pixel Indicator Technique:

K. Muhammad et al. 2014 proposed a LSB and cyclic LSB techniques, the quality of stego image is nearly equal to the original image i.e. stego image have better quality but the main drawback of these techniques is that they have very low payload capacity nearly equal to 1bpp (bits per pixel). Therefore a new technique was developed to increase the payload capacity of LSB techniques [8]. This technique is called Pixel Indicator Technique in which RGB images are used as cover images. In this technique, Channels of RGB are divided into two separate channels which are indicator channel and data channel.

The indicator channel is used to select the data channel for information hiding. This selection process is changed rapidly according to a fixed equation. This rapid change of process results in enhanced security. Using 1st and 2nd LSB of indicator channel, cover image is embedded with data. Data embedding is done according to following table:-

Table 1: Indicator values Based action

Last two LSB	1 Data Channel	2 Data Channel
0 0	No data is hidden	No data is hidden
0 1	No data is hidden	2 LSB of this channel are replaced
1 0	2 LSB of this channel are replaced	No data is hidden
1 1	2 LSB of this channel are replaced	2 LSB of this channel are replaced

Algorithm to select the indicator channel:

1. Find the length of secret message.
2. If length of secret message is even:
    Indicator channel=Red
    Data channel 1= Green for odd parity and Blue for even parity
    Data channel 2=Blue for odd parity and Green for blue parity
3. If length of secret message is prime:
    Indicator channel=Blue
    Data channel 1= Red for odd parity and Green for even parity
    Data channel 2=Green for odd parity and Red for blue parity

4. Else:
    Indicator channel=Green
    Data channel 1= Red for odd parity and Blue for even parity
    Data channel 2=Blue for odd parity and Red for blue parity

Algorithm for hiding the data using Pixel Indicator Technique:

1. Select a cover image.
2. Derive the secret message's length.
3. Store the message length into first 8 bytes of 1st row and in variable remaining message size (RMS).
4. Now, from 2nd row, select the indicator channel from RGB channel and check the 2 LSB of indicator channel:
    4.1 If 2 LSB is equal to 00, then do nothing and move to next pixel
    4.2 If 2 LSB is equal to 01, then hide 2 data bits in 2 LSB of channel 1, decrease the RMS value by 2 and move to next pixel
    4.3 If 2 LSB is equal to 10, then hide 2 data bits in 2 LSB of channel 2, decrease the RMS value by 2 and move to next pixel
    4.4 If 2 LSB is equal to 11,then hide 2 data bits in channel 1 and 2 data bits in channel 2,decrease the RMS value by 4 and move to next pixel
5. Repeat the Step 4, until RMS value is equal to 0.

Algorithm to recover data using Pixel Indicator Technique:

1. Select the cover image.
2. Derive the length of secret message from first 8 bytes of first row of stego image and copy this into variable RMS
3. Now, from 2nd row, select the indicator channel from RGB channel and check the 2 LSB of indicator channel:
    3.1 If 2 LSB is equal to 00, then do nothing and move to next pixel
    3.2 If 2 LSB is equal to 01, then extract 2 data bits in 2 LSB of channel 1, decrease the RMS value by 2 and move to next pixel
    3.3 If 2 LSB is equal to 10, then extract 2 data bits in 2 LSB of channel 2, decrease the RMS value by 2 and move to next pixel
    3.4 If 2 LSB is equal to 11,then extract 2 data bits in channel 1 and 2 data bits in channel 2,decrease the RMS value by 4 and move to next pixel
5. Repeat the Step 4, until RMS value is equal to 0.

2.1.5. CYCLIC LSB:

M. Khan et al. 2015 proposed the original quality of cover image is retained in LSB based techniques. Stego image and cover image have comparable quality. But information hiding using LSB can be easily detected by attackers because these techniques are simple and straightforward. To increment the security of secret information, it has to be scattered into the whole cover image. Therefore, a new LSB technique was developed which allow data dispersion in the whole image.

This method is called cyclic because RGB channels are rotated into cycle i.e. first bit of secret message is hidden into red channel of 1st pixel, second bit is hidden into green channel of next bit, third bit is hidden into blue channel of next pixel and then this cycle is repeated [9].

Algorithm for hiding the data:-

1. Select the cover image as well as secret information.
2. Convert the secret message into 1D array of bits.
3. From the cover image, separate different planes into Red, Green and Blue Channels.
4. Create a Flag named Channel Flag which will be used for determining which channel will be used for information hiding. Initialize Channel Flag with value 1.
5. Check the Value of Channel Flag.
    5.1 If channel Flag==1, Secret message will be embedded into red channel.
    5.2 If channel Flag==2, Secret message will be embedded into green channel.
    5.3 If channel Flag==3, Secret message will be embedded into blue channel.
6. Increase the value of channel Flag by 1.
7. If value of channel Flag is 3, then set channel Flag=1.
8. Repeat Steps 5 to 7 until complete secret message is embedded into cover image.
9. Combine all the channels to form the stego image.

Algorithm for obtain the hidden message:-

1. Select the stego-image.
2. From the cover image, separate different planes into Red, Green and Blue Channels.
4. .Initialize Channel Flag with value 1.
5. Check the Value of Channel Flag.
    5.1 If Channel Flag==1, extraction the secret information from red channel.
    5.2 If Channel Flag==2, extraction the secret information from green channel.
    5.3 If Channel Flag==3, extraction the secret information from blue channel.
6. Increase the value of Channel Flag by 1.
7. If value of Channel Flag is 3, then set Channel Flag=1.
8. Repeat Steps 5 to 7 until all information is extracted from stego-image.

9. Combine all the extracted bits to form the secret message.

2.1.6. MAGIC LSB:

K. Muhammad et al. 2015 Proposed a steganography techniques; encryption is not done when data is embedded into the cover image. No encryption enables the malicious third party user or attacker to extract data easily from the cover image. Not only have that, stego image using different techniques had low quality which can be easily detected by some attacker. To overcome these problems, magic LSB method is used. In this method, data is encrypted using different algorithms. If some malicious attacker knows the embedding algorithm, then still data extraction is not easy because data is further sub-divided into 4 blocks. So, data is more secure in this technique. In this technique transpose of cover image is taken and a transposed image T is formed.

Then, this Transposed image T is taken and its RGB model is converted into HSI model (Hue, Saturation, and Intensity).HSI is more secure than RGB because these planes are not dependent on each other i.e. changing one plane does not disturb the characteristics of other planes, while in RGB model, all planes are inter-related i.e. changing one plane will affect all the other planes. Also, image processing is relatively cost-friendly in HSI plane.

In this technique, a message is implanted into the cover image and for encryption, key K is used. Then, the stego-image S contains the secret information. The message M is encrypted by means of an algorithm using key K which divides the data into four encrypted blocks B1, B2, B3, and B4. The HSI model's intensity plane is then further subdivided into four sub-images. Now, the rotation is done on these sub-images at different angles with the help of key K. After rotation, four images are obtained as I1, I2, I3, and I4.Then embedding of the message is done using Magic LSB technique. At last, these four sub-images are rotated again to form the intensity plane of the final stego-image. To construct the complete stego-image, this intensity plane is then hue and saturation plane. Reverse operations have to be applied by the receiver to extract the secret message from the image. MLEA algorithm is used which divides original media into four sub media using a secret key. In MLEA algorithm, secret data is encrypted first and then it is embedded into cover media.

Example:

Consider a cover image I={40,56,21,55,65,52,44,78,79}. Consider a secret message M= $(01000001)_2$ which is to be embedded in image I. Before embedding, a magic matrix is generated having size same as stego image matrix i.e. if stego image have size 3X3, then dimension of magic matrix is also 3X3.

This magic matrix will determine the position where bits of secret message will be stored.

$$I = \begin{bmatrix} 70 & 56 & 41 \\ 35 & 15 & 52 \\ 94 & 8 & 29 \end{bmatrix} \qquad MGM = \begin{bmatrix} 8 & 3 & 4 \\ 1 & 5 & 9 \\ 6 & 7 & 2 \end{bmatrix} \qquad S = \begin{bmatrix} 71 & 56 & 40 \\ 34 & 14 & 52 \\ 94 & 8 & 29 \end{bmatrix}$$

COVER IMAGE MAGIC MATRIX STEGO IMAGE

According to this magic matrix, the first secret bit will be embedded into 35 of I(2nd row,1st column),second bit in 29(3rd row,3rd column),third bit in 56(1st row,2nd column), 4th bit in 41(1st row,3rd column) and so on. In Stego image matrix, elements which are different from I have been embedded with secret message.

Properties of Magic Matrix:

1. All elements of magic matrix are unique i.e. no two elements are repeated.
2. The elements of matrix cannot be greater than the product of dimension of stego matrix.(Here, every element should be less than 3x3=9)
3.Sum of elements of columns, rows as well as its diagonals should be same.(Here, In sum of row and column is 8+3+4=1+5+9=6+7+2=8+1+6=3+5+7=4+9+2=15.Also sum of elements of diagonals is 8+5+2=6+5+4=15 which is same as sum of row and columns.)

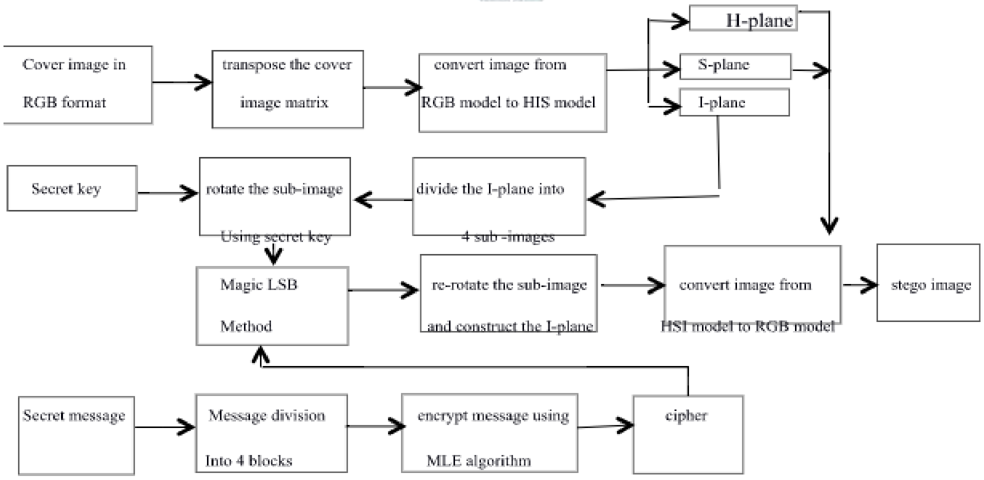

Cover image in RGB format
transpose the cover image matrix
convert image from RGB model to HIS model
H-plane
S-plane
I-plane
Secret key
rotate the sub-image Using secret key
divide the I-plane into 4 sub -images
Magic LSB Method
re-rotate the sub-image and construct the I-plane
convert image from HSI model to RGB model
stego image
Secret message
Message division Into 4 blocks
encrypt message using MLE algorithm
cipher

Figure 4 show the proposed steganographic model:

2.1.7. EDGES BASED DATA HIDING METHODS

K. Muhammad et al. 2015 provided a method; highly secure information is store at the edges of cover image. Pixels at the edges of the cover image can store more secure information better than the remaining part of the image. Also information inside the edges cannot be easily detected by the third-party user.

This technique has a higher payload capacity as compared to LSB and cyclic LSB technique. Payload capacity of this technique can be further increased by combining canny and fuzzy edges of the image. By altering the amount of data in edge and smooth area of the image, payload capacity can be increased significantly. Therefore, 3 bits of secret information are stored in edge pixels, whereas one or two bits of information are stored in smooth pixels. In this technique, traversing of pixels is started from the center of the image after dividing the data into two blocks [10]. This increases the security.

2.2. TRANSFORMATION DOMAIN TECHNIQUE:

In this method, the data is hidden with the help of various transformed like frequency or wavelet. So, unlike spatial domain where data was embedded into direct pixels of image, here data is embedded into transformed image. The images are less prone to cropping, compression or any other image processing method after transforming [11]. The information is not limited to individual pixel but spread over a larger number of pixels in the transformed domain. Thus, information is secured from any attack. This method is more secure in data maintenance although, it is more complex.

Transform Domain can be classified into following categories:

1. (DFT) - Discrete Fourier Transform
2. (DCT)- Discrete Cosine Transform
3. (DWT)- Discrete Wavelet Transform
4. (IWT)- Integer Wavelet Transform
5. (DCVT)- Discrete Curve let Transform

2.2.1. Discrete Cosine Transform:

In this method, image is separated into different parts with each part having different frequency. These frequency bands are mainly divided into three categories:-low, middle and high frequency bands. This watermark is thus easier to insert into image due to different bands. Since scattering of watermark information is least in middle frequency bands, there for middle frequency bends selected mostly. The JPEG formats make use of this type of transform [12].

Equation of DCT is:

$$D(v,w) = \frac{1}{4}\, C(v)C(w) \sum_{x=0}^{7}\sum_{y=0}^{7} d(x,y) \cos\left[\frac{\pi(2x+1)v}{16}\right] \cos\left[\frac{\pi(2y+1)w}{16}\right]$$

2.2.2. Discrete Fourier Transform:

This method is similar to Discrete Cosine Method but instead of utilizing cosine, Fourier transform is used. Use of Fourier transform makes it lack resistance to geometric distortions. In this technique, information based on space and time is converted into information based on frequency.

Image compression and image filtering uses DFT. It constitutes samples which are sufficient to form the image instead of all the frequencies that makes up image.

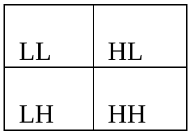
The DFT of Spatial value d (v, w) for image dimension M * N is derived by the equation [13].

Equation of DFT is D (v, w) =$\frac{1}{\sqrt{MN}} \sum_{v=0}^{M-1}\sum_{w=0}^{N-1} F(x,y)e^{-12\pi\frac{VX}{M}+\frac{WY}{M}}$

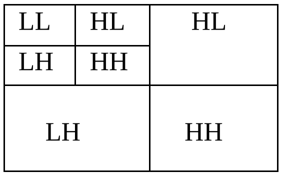
2.2.3. Discrete Wavelet Transform:

A wavelet is a signal wave having its own time domain. A wavelet usually oscillates in its own time domain. Wavelets are functions and the range of these functions can be obtained over a fixed interval in time domain. Average value of these wavelet functions is zero. Multi-resolution Analysis on images is performed by DWT using wavelet function. Multi-resolution Analysis is analyzing of different frequencies with different resolution. DWT has its own space frequency property.

K. Joshi et al. 2015 described a DWT, signal is divided into two frequency domain, one is high and another is low frequency domain. The first part which is of high frequency contains a component and second part is again divided into two parts- low & high. Changes in edges are invisible to human eye in high frequency part. DWT is performed in two directions on this part- first is vertical and second is horizontal. Then, frequency is divided into 4 sub-bands in order to perform second level decomposition.



5(a)



5 (b)

Figure 5(a) One level decomposition, 5(b) Two level decomposition

Figure 5.1, 5.2 and 5.3 show the cover image cameraman with its decomposition image cameraman.

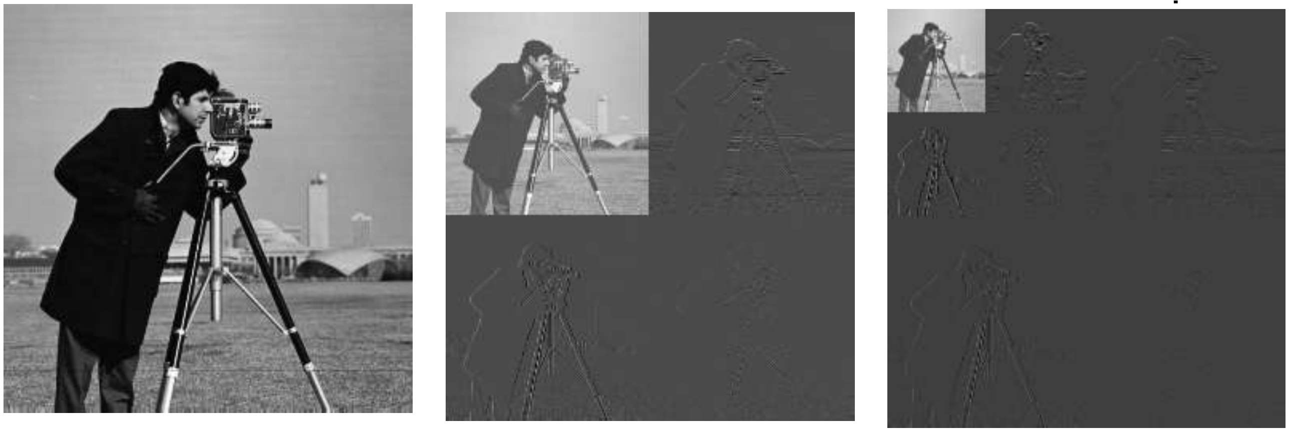


Figure 5.1 original image cameraman, 5.2 one One level decomposition and 5.3 Two level decomposition.

2.2.4. Integer Wavelet Transform:

In Discrete Wavelet Transform, the process of invisible embedding is expected to more effective since it allows separate processing of components. Different components have a little visible interaction between them. But floating point coefficients are present in wavelet filters and DCT [14]. Since in images, input data is mainly consists of series of integers, the output is also expected to be an integer value. But floating point coefficient won't provide integer output. Therefore Integer Wavelet Transform is used since integer output will allow perfect reconstruction of the original image.

2.2.5. Discrete Curve let Transform:

R. Kumar, A.J. Singh 2015 presented a Curve let Transform is a rather new Transform Technique. It is an evolving technique which belongs to the multiscale geometric Transform. Effective Solutions of all the problems are provided using Curve let Transform since edge representation is better in curve let Transform as compared to Wavelets and DCT [15].

2.3. DISTORTION TECHNIQUE:

B. Kaur et al. 2013 proposed a technique; Signal distortion is used for storing secret information. During decoding process, knowledge about original cover image is required. To encode the original image, sequences of modifications are applied to the original cover image. To find the secret information, one has to use decoder functions. Differences between original encoded image and cover image can be measured by using these decoder functions. The purpose of these functions is to find the modifications applied to original image and ultimately, the secret information is recovered by decoding the image [16].

A series of changes are applied to cover image to create a stego object. To encode the message, image pixels are selected pseudo-randomly .The message is bit '1' if, there in some deviation between original image and stego image otherwise value of message bit will be '0'. To prevent changing of statistical properties of image, sender can modify '1' pixel value. A necessary condition to retrieve the message is that the receiver must have original cover image in his possession. This is a limitation of this technique since cover image should not be used more than once to achieve proper security. If some third party user having malicious intention have the cover image, he can retrieve the hidden information from the encoded image easily.

2.4. MASKING & FILTERING:

M. Hussain et al. 2013 Described a Masking is an important concept of data hiding. Although it is a little different form Steganography. In Steganography information is hidden whereas in Masking a watermark is drawn on image which becomes part of the image. So in Masking, marking on image is done. Usually, this marking is done through watermarks. In masking, data of image is extended by masking secret data over original image instead of hiding information inside the data. Masking is integrated into image itself with the help of lousy compression [17]. Due to this, image is not destroyed. Robustness of this method is much greater as compared to LSB. But this technique has a limitation that it can only be applied to grayscale images or 24-bit images.

3. EVALUATION

W. Zhang et al. 2007 described imperceptibility is the most important requirement of a Steganography. The following criteria have been proposed to achieve imperceptibility of a Stenographic Algorithm [18].

1. Invisibility: This is of utmost importance in steganography. A good Stenographic algorithm should remain undetected by human eyes. As soon as a person notices that image has been tempered or changed by any method, the algorithm is compromised and is of no use. Therefore, algorithm should be so designed that the human cannot tell the difference between original image and stego-image.

2. Payload Capacity: Sufficient embedding capacity is required by steganography. Like in watermarking, a small portion of image needs to be embedded in order to maintain original copyright information.

3. Robustness against Statistical attacks: Statistical Analysis is the process of hidden information detection. This is achieved by applying statistical tests on image data. A good Algorithm should have robustness against this type of Statistical attacks. For example, many algorithms leave a signature at the time of embedding of data. These signatures can be easily detected by Statistical Analysis. So this type of algorithm should be avoided.

4. Robustness against image manipulation: Image manipulation is the process of changing the various aspects of image like cropping and rotating. During Information Transfer, an attacker or third party user can try to change the image data or maybe even try to remove the hidden information. This type of attacks will harm the secret information. Therefore, an algorithm should be efficient and robust against this type of malicious image manipulation.

5. **Independent of file format**: An efficient algorithm should have the ability to hide and embed the information in any file format available. If an algorithm is specific to a file format, then it will be of little use if image available is in any other format.

6. **Unsuspicious files:** All the abnormal characteristics of an image can cause suspicion which may result in further checking of the image. For example, abnormal file size, Weird Image resolution. There abnormality should be avoided as much as possible.

Table 2: Comparison of Image Steganography Techniques:

	Invisibility	Payload Capacity	Robustness Against Statistical Attack	Robustness Against Image Manipulation	Independent Of File Format	Unsuspicious Files
JPEG	High	Medium	Medium	Medium	Low	High
LSB in BMP	High	High	Low	Low	Low	Low
LSB in GIF	Medium	Medium	Low	Low	Low	Low
Spread spectrum	High	Medium	High	Medium	High	High

4. APPLICAITION OF STEGANOGRAPHY:

1. Secret Communication: The main purpose of steganography is to achieve proper security in communication. This is done so that two parties can have secure communication. Cryptography can also be used to achieve secret communication but cryptography will leave the traces of its presence. This will draw unwanted attention. Therefore steganography is used since its existence is hidden in cover image [19].

2. Copyright Protection: The owner of any copyright media should be protected against piracy. Therefore, Watermarking is used to embed the secret information in images which will prove that the media is legitimate.

3. Feature Tagging: Any image can carry additional details like captions, name of person in the photo, details of the photographer, location on map where the image was shot etc. These details can be embedded inside the image. If an image is converted into stego-image, then this will also copy all the details too. Users which have decoding key will be able to view these additional features [20].

4. Use by terrorists: To spread Terrorism, innocent cover images can be used by terrorists in which secret messages is hidden. Many publication media have also reported that terrorists are using web encryption and steganography to transfer secret information.

5. Digital Watermarking: Watermarking is one of the best features of steganography. In this, a watermark is embedded into the image. Authenticity of signal can be verified using this watermark. Bank Note authentication and copyright infringements are example of this.

5. COMPARISON OF DIFFERENT STEGANOGRAPHY TECHNIQUES AND FEATURES

Capacity, Security and Robustness are the important aspects by which any information hiding system can be characterized. Amount of information which a cover medium can hide is called capacity, Inability of third party user or eavesdropper to detect hidden information is called security and modifications which a medium can withstand before hidden information is destroyed is called its robustness [20].

Usually, watermarking and steganography are the concepts which are used in information hiding. A high level robustness is achieved through watermarking. Without changing the quality of data, removing the watermark should be impossible, otherwise data will be compromised and neither sender nor receiver will know that it has been tempered. High security and capacity is achieved through Steganography. Even slightest modification to the medium can destroy the information hidden as well as the medium itself.

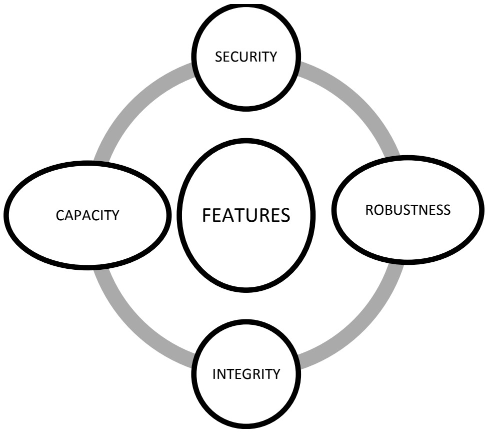


Figure 6: Features for Steganography.

Table 3: Comparisons of Different Steganography Techniques

Technique	Security	Capacity	Transparency	Integrity	Temper resistance	Robustness
Text steganography	High	Low	Low	Low	High	Low
Image steganography	High	High	Low	High	High	High
Audio steganography	Low	Low	Low	Low	High	Low
Video steganography	High	High	High	Low	High	Low

6. CONCLUSION

Steganography is the art and science of information hiding by using different medium. In this paper, Image steganography and its different techniques were studied. In this study, we concluded that there are a large number of techniques are available for embedding data inside image. Each technique has their own importance and use for information hiding in images. All these technique provide different level of security, capacity and robustness. According to the user's requirement, any particular method can be used. Using different algorithms, security and capacity of encryption can also be enhanced. This insight into different techniques of steganography will help us to identify new areas and improve the usage and applications of already existing areas.

REFERENCES

[1] M.Khan, M. Sajjad, I. Mehmood, S. Rho and S. Wook Baik, "A Novel Magic LSB Substitution Method (M-LSB-SM) Using Multi-Level Encryption And Achromatic Component Of An Image" Multimedia Tools And Applications, Volume 3, Issue 2, 2015.

[2]K. Joshi And R. Yadav , "A New LSB-S Image Steganography Method Blend With Cryptography For Secret Communication", In Image Information Processing (ICIIP),Third International Conference On IEEE, Volume ,Issue , 2015.

[3] M. Shelke, A. Dongre and P. Soni "Comparison Of Different Techniques For Steganography In Images " International Journal Of Application Or Innovation In Engineering & Management (IJAIEM) ,Volume 3, Issue 2, 2014 .

[4] K. Joshi, R. Yadav and S. Allwadhi, "PSNR and MSE Based Investigation Of LSB." Computational Techniques In Information And Communication Technologies (ICCTICT), International Conference On. IEEE, Volume ,Issue ,2016.

[5] A. GitHub, "Pixel Indicator Technique for RGB Image Steganography", Article In Journal Of Emerging Technologies In Web Intelligence, Volume 3, Issue 2, 2010.

[6] N. Akhtar, P. Johari and S. Khan, "Enhancing The Security And Quality Of LSB Based Image Steganography", Proceedings Of IEEE International Conference On Computational Intelligence And Communication Networks, Volume 4, Issue 3, 2013.

[7] K. Joshi, R. Yadav And G. Chawla, "An Enhanced Method For Data Hiding Using 2-Bit XOR In Image Steganography", International Journal Of Engineering And Technology, Volume 8, Issue 6, 2017.

[8] Muhammad K, Ahmad J, Farman H and Zubair M "A Novel Image Steganographic Approach For Hiding Text In Color Images Using HSI Color Model". Middle-East J Sci Res, Volume 4, Issue 3, 2015.

[9] M. Hussain and M. Husain, "A Survey Of Image Steganography Techniques", International Journal Of Advanced Science And Technology (IJAST), Volume 4, Issue 4, 2013.

[10] J. Ashok, Y.Raju, S. Munishankaralah and K. Srinivas, "Steganography: An Overview", International Journal Of Engineering Science And Technology (IJEST), Volume 2, Issue 10, 2010.

[11]R. Kumar and A.J. Singh "Understanding Steganography Over Cryptography And Various Steganography Techniques ", IJCSMC, Volume 4, Issue 3, 2015.

[12] B. Kaur, A. Kaur and J. Singh "Steganographic Approach For Hiding Image In Dct Domain", International Journal Of Advances In Engineering & Technology, Volume 4, Issue 3, 2013.

[13] V. Nagaraj,V. Vijayalakshmi and G. Zayaraz, "Modulo Based Image Steganography Technique Against Statistical And Histogram Analysis", IJCA Special, Volume 4, Issue 3, 2011.

[14] S. Roy and P. Venkateswaran, "Online Payment System Using Steganography And Visual Cryptography," Students‟ Conference On Electrical, Electronics and Computer Science, IEEE ,Volume 4, Issue 3,2014.

[15 D. Samidha and D. Agrawal, "Random Image Steganography In Spatial Domain", International Conference In Emerging Trends, VLSI, Embedded System, Nano Electronics And Telecommunication System, IEEE, Volume 4, Issue 3, 2013.

[16] R. amirtharajan and R. akila, "A Comparative Analysis Of Image Steganography", International Journal Of Computer Applications, Volume 2 , Issue 3, 2010.

[17] S. Hemalatha, Acharya, Renuka and P. Kamath, "An Integer Wavelet Transform Based Steganography Technique For Color Images", International Journal Of Information & Computation Technology. Volume 3, Issue 1 , 2013.

[18] A. Ataby and F. Al-Naima, "A Modified High Capacity Image Steganography Technique Based On Wavelet Transform", The International Arab Journal Of Information Technology, Volume 7, Issue 4, 2010.

[19] W. Zhang, S. Wang, And X. Zhang , "Improving Embedding Efficiency Of Covering Codes For Applications In Steganography", IEEE Communications Letters, Volume 11, Issue 4, 2007.

[20] A. Kaur, R. Kaur and N. Kumar "A Review on Image Steganography Techniques", International Journal Of Computer Applications, Volume 123, Issue 4, 2015.