Implementation of
Steganography
Techniques Using MATLAB

Haldia Institute of Technology
Department of Computer Science and Engineering
,

A project Report
Under the guidance of
Sri Sabyasachi Pramanik
Asst. Professor
Cse Department
HIT Haldia

Submitted by:

Group Members	**University Roll Number**
Abineshwar Bisoi	**10300112051**
Manav	**10300112099**
Santosh Kumar	**10300112142**
Vikash Kumar	**10300112170**

Acknowledgement

It is not possible to prepare a project synopsis without the assistance &encouragement of other people. This one is certainly no exception. On the very outset of this report, I would like to extend my sincere & heartfelt obligation towards all the personages who have helped me in this endeavour. Without their active guidance, help, cooperation & encouragement, I would not have made headway in the project.
I am ineffably indebted to **Sri Tarun Kr. Ghosh** ,HOD CSE and **Sri Sourav Mondal**,Project Convenor for conscientious guidance and encouragement to accomplish this assignment.
I am extremely thankful and pay my gratitude to my faculty **Sri Sabyasachi Pramanik** for his valuable guidance and support on completion of this project in its presently. I extend my gratitude for giving me this opportunity. I also acknowledge with a deep sense of reverence, my gratitude towards my parents and member of my family, who has always supported me morally as well as economically. At last but not least gratitude goes to all of my friends who directly or indirectly helped me to complete this project report. Any omission in this brief acknowledgement does not mean lack of gratitude.

Thanking You

HALDIA INSTITUTE OF TECHNOLOGY

CERTIFICATE

This is to certify that the project “Implementation of Image Steganography Techniques Using MATLAB” is being

Submitted By:-

Abineshwar Bisoi	10300112051
Manav	10300112099
Santosh Kumar	10300112142
Vikash Kumar	10300112170

Of Computer Science & Engineering Department is absolutely based upon their work under the supervision of Sri Sabyasachi Pramanik ,dept of Computer Science & Engineering, Haldia Institute Of Technology, and the neither this work nor any part of it has been submitted for any degree/diploma or any other academic award anywhere before.

Mr Tarun Kr. Ghosh	Mr. Sourav Mondal	Mr. Sabyasachi Pramanik
Associate Prof &	Convener &	Project Supervisior &
Head of CSE Dept,	Asst. Professor of CSE Dept,	Asst. Professor of CSE Dept,
HIT,Haldia	HIT,Haldia	HIT,Haldia

INDEX

ABSTRACT

Image steganography is an engineering term defining a different and significant discipline for information hiding. This process can be described as hiding of secret information behind an image‟. Discrete Wavelet Transform (DWT) is one of the known methods used in steganography. The focus of the proposed work in this paper is on decreasing the complexity in image hiding through DWT technique while providing better undetectability and lesser distortion in the stego image. This paper proposes the algorithm for embedding and extracting the secret image embedded behind the cover gray scale image. Also, the analysis of performance measurement methods such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), gives us the experimental summary for four different cases where each case spans different sizes of cover and secret image, comparing the cover image and stego image at the sender‟s side and embedded secret and extracted secret at the receiver‟s side. The stego attacks are then applied on the stego image and after each of the attack, the secret image is extracted from the distorted image. For better analysis, this extracted secret is compared with the expected result on the basis of PSNR and MSE.

Keywords

Cover image
DWT Method
Key information
Secret image
Stego image

INTRODUCTION

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means “cover writing” . Generally steganography is known as “invisible” communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today’s steganography systems use multimedia objects like image, audio, video etc. As cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information.

Steganography means is not to alter the structure of the secret message, but hides it inside a cover-object (carrier object). After hiding process cover object and stego-object (carrying hidden information object) are similar. So, steganography (hiding information) and cryptography (protecting information) are totally different from one another. Due to invisibility or hidden factor it is difficult to recover information without known procedure in steganography. Detecting procedure of steganography known as Steganalysis.

Steganography in Digital Mediums

Depending on the type of the cover object there are many suitable steganographic techniques which are followed in order to obtain security. It can be shown in Figure 1.

Network Steganography: When taking cover object as network protocol, such as TCP, UDP, ICMP, IP *etc*, where protocol is used as carrier, is known as network protocol steganography. In the OSI network layer model there exist covert channels where steganography can be achieved in unused header bits of TCP/IP fields [24].

Video Steganography: Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information. Generally discrete cosine transform (DCT) alter values (*e.g.,* 8.667 to 9) which is used to hide the information in each of the images in the video, which is not noticeable by the human eye. Video steganography uses such as H.264, Mp4, MPEG, AVI or other video formats.

Audio Steganography: When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or *etc* for steganography.

Text Steganography: General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code [21] and *etc* is used to achieve information hiding.

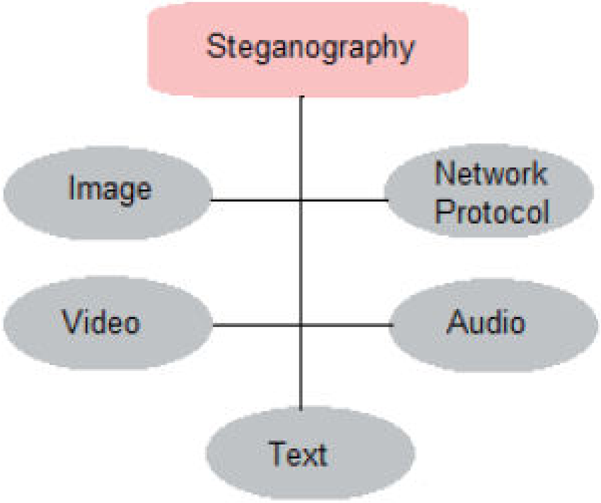


Figure-0. Digital Medium to Achieve Steganography

Image Steganography: Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information. Image steganography has been a vast area of research for many years now. It is a process that hides the secret image behind the cover image in such a way that the presence of the secret image is locked and the cover image appears to be the same [1]. In such a way, the digital information can be embedded and transferred to the destination with minimum risk of detectability. The concept of „undetectability‟ has raised the need of steganography in all dimensions such as commerce, national security services, and banking and other private communication areas. Other information hiding methods such as cryptography, watermarking and digital signature differs from the steganography concept as steganography allows the communication to be hidden and also, provides better quality of the secret image.

Image Steganography Terminologies

Image steganography terminologies are as follows:-

- **Cover-Image**: Original image which is used as a carrier for hidden information.
- **Message**: Actual information which is used to hide into images. Message could be a plain text or some other image.
- **Stego-Image**: After embedding message into cover image is known as stego-image.
- **Stego-Key**: A key is used for embedding or extracting the messages from cover-images and . stego-images.

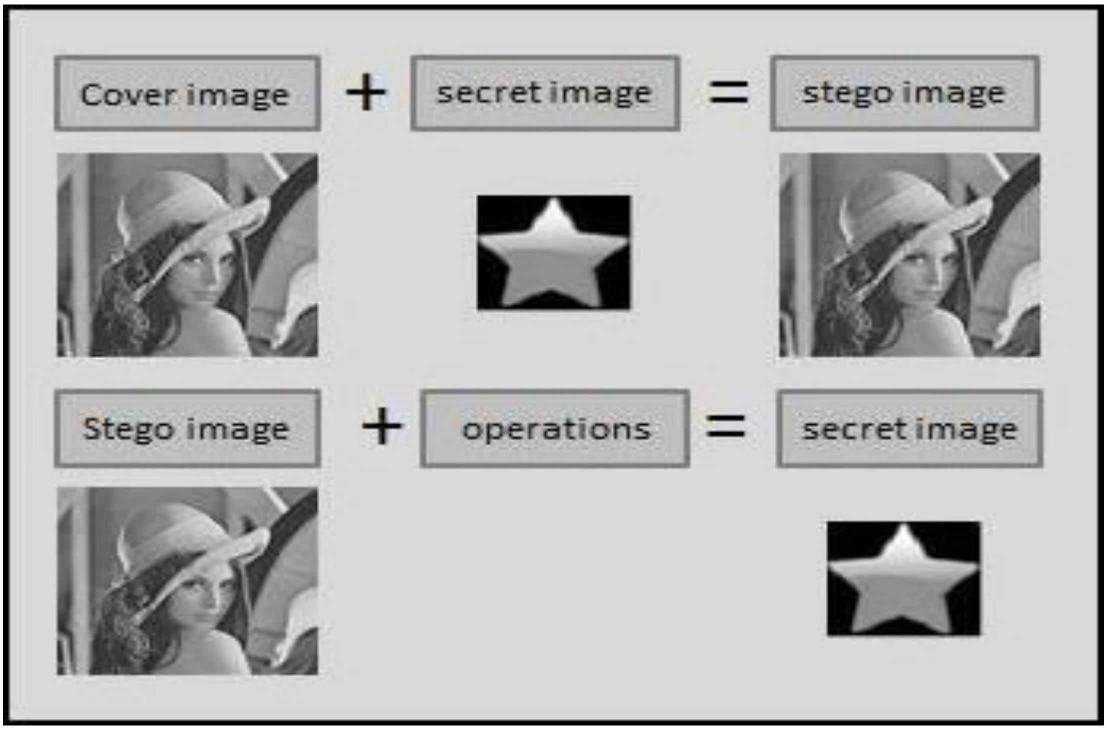


Figure 1. Principles of Steganography

Image Steganography Techniques

Image steganography techniques can be divided into following domains.

Spatial Domain Methods: There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB)-based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without introducing many perceptible distortions. Changes in the value of the LSB are imperceptible for human eyes. Spatial domain techniques are broadly classified into:
1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding method (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method
6. Labelling or connectivity method
7. Pixel intensity based method
8. Texture based method
9. Histogram shifting methods

General advantages of spatial domain LSB technique are:
1. There is less chance for degradation of the original image.
2. More information can be stored in an image.

Disadvantages of LSB technique are:
1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.

Transform Domain Technique: 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. Transform domain embedding can be termed as a domain of embedding techniques for which a number of algorithms have been suggested . The process of embedding data in the frequency domain of a signal is much stronger than embedding principles that operate in the time domain. Most of the strong steganographic systems today operate within the transform domain Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to compression, cropping, and image processing. Some transform domain techniques do not seem dependent on the image format and they may outrun lossless and lossy format conversions.
Transform domain techniques are broadly classified into

1. Discrete Fourier transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete Wavelet transformation technique (DWT).
4. Lossless or reversible method (DCT)
5. Embedding in coefficient bits

Distortion Techniques: Distortion techniques need knowledge of the original cover image during the decoding process where the decoder functions to check for differences between the original cover image and the distorted cover image in order to restore the secret message. The encoder adds a sequence of changes to the cover image. So, information is described as being stored by signal distortion .Using this technique, a stego object is created by applying a sequence of modifications to the cover image. This sequence of modifications is use to match the secret message required to transmit .The message is encoded at pseudo-randomly chosen pixels.

If the stego-image is different from the cover image at the given message pixel, the message bit is a “1.” otherwise, the message bit is a “0.” The encoder can modify the “1” value pixels in such a manner that the statistical properties of the image are not affected. However, the need for sending the cover image limits the benefits of this technique. In any steganographic technique, the cover image should never be used more than once. If an attacker tampers with the stego-image by cropping, scaling or rotating, the receiver can easily detect it. In some cases, if the message is encoded with error correcting information, the change can even be reversed and the original message can be recovered .

DISCRETE WAVELET TRANSFORM (DWT)

Discrete wavelet transforms are used to convert the image in spatial domain to frequency domain, where the wavelet coefficients so generated, are modified to conceal the image. In this kind of transformation the wavelet coefficients separates the high and low frequency information on a pixel to pixel basis . The DWT approach applied in the proposed work is the „Haar DWT‟, simplest of all the wavelet transform approaches. In this transform, time domain is passed through low-pass and high pass filters and the high and low frequency wavelet coefficients are generated by taking the difference and average of the two pixel values respectively . The operation of Haar DWT on the cover image results in the formation of 4 sub-bands, namely the approximate band (LL), horizontal band (HL), vertical band (LH) and the diagonal band (HH). The approximate band contains the most significant information of the spatial domain image and other bands contain the high frequency information such as edge details. Thus, the DWT technique describes the decomposition of the image in four non overlapping sub-bands with multi-resolution. This process can be iterated on one of the sub-band of first level DWT to get the further second level sub bands for better results.

LL	HL
LH	HH

Figure 2. Sub bands formed after applying Haar DWT

Figure 2 shows the 4 sub-bands that are formed after applying 1-level Haar DWT on a 2-dimensional image.

STEGANALYSIS

Steganalysis is an art of identifying stego images that contains a secret image. However it does not consider the successful extraction of the secret image, which is a requirement for cryptanalysis. Steganalysis is a very difficult task as it is based on insecure steganography. Recently, steganalysis has received a lot of attention from the media and the legal world. The attacker either can destroy, disable the secret image or may also add counter information over the original secret image which leads to statistical differences of the secret image.

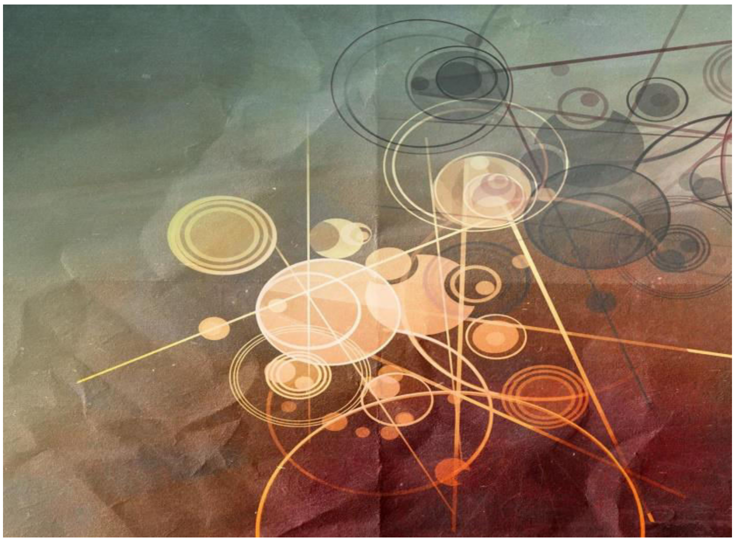
PROPOSED MODEL

If we apply DWT on an image, it divides the image in frequency components. The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image. These detailed coefficients can be used to embed secret image. Here we have taken an image as cover object and another small image as secret message. In embedding process, first we convert cover image in wavelet domain. After the conversion we manipulate high frequency component to keep secret image data. These secret image data further retrieved in extraction procedure to serve the purpose of steganography.
Embedding

Embedding model

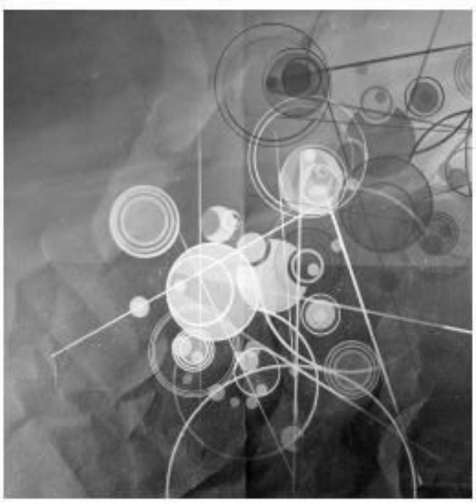
In this step, insertion of secret message onto cover object is carried out. Additional components rather than usual steganographic objects used here is pseudo-random number. Pseudo-random sequences typically exhibit statistical randomness while being generated by an entirely deterministic causal process generator. A pseudo-random number generator is a program that on input a seed, generates a seemingly random sequence of numbers.

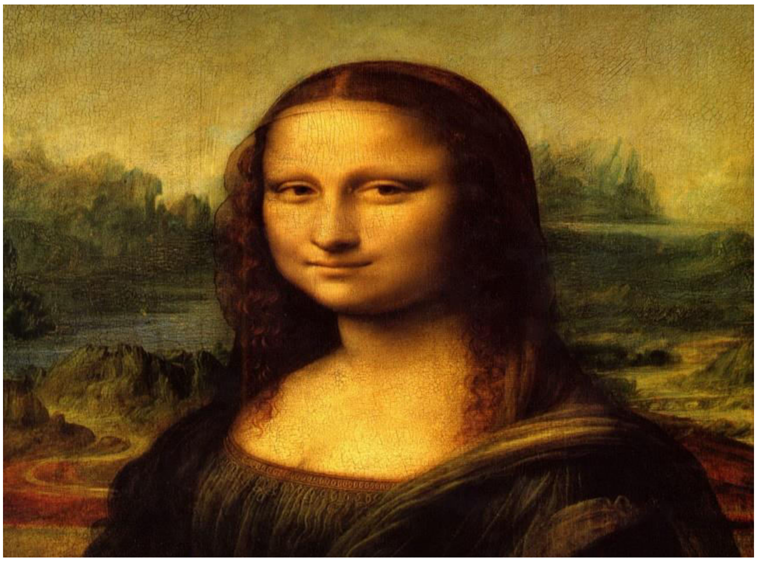
Input: An m × n carrier image and a secret message/image.
Output: An m × n stego-image.
Algorithm:
Steps-
1. Read the cover image (Ic)
2. Calculate the size of Ic
3. Read the secret image (Im)
4. Prepare Im as message vector
5. Decompose the Ic by using Haar wavelet transform
6. Generate pseudo-random number (Pn)
7. Modify detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding Pn when message bit = 0.
8. Apply inverse DWT
9. Prepare stego image to display



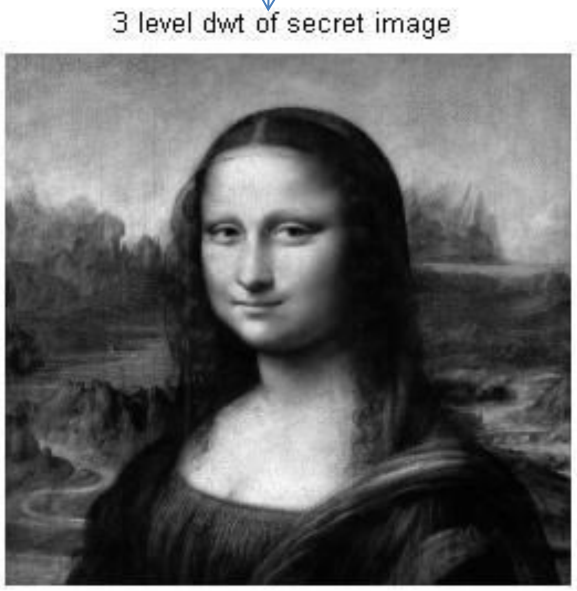
Cover Image

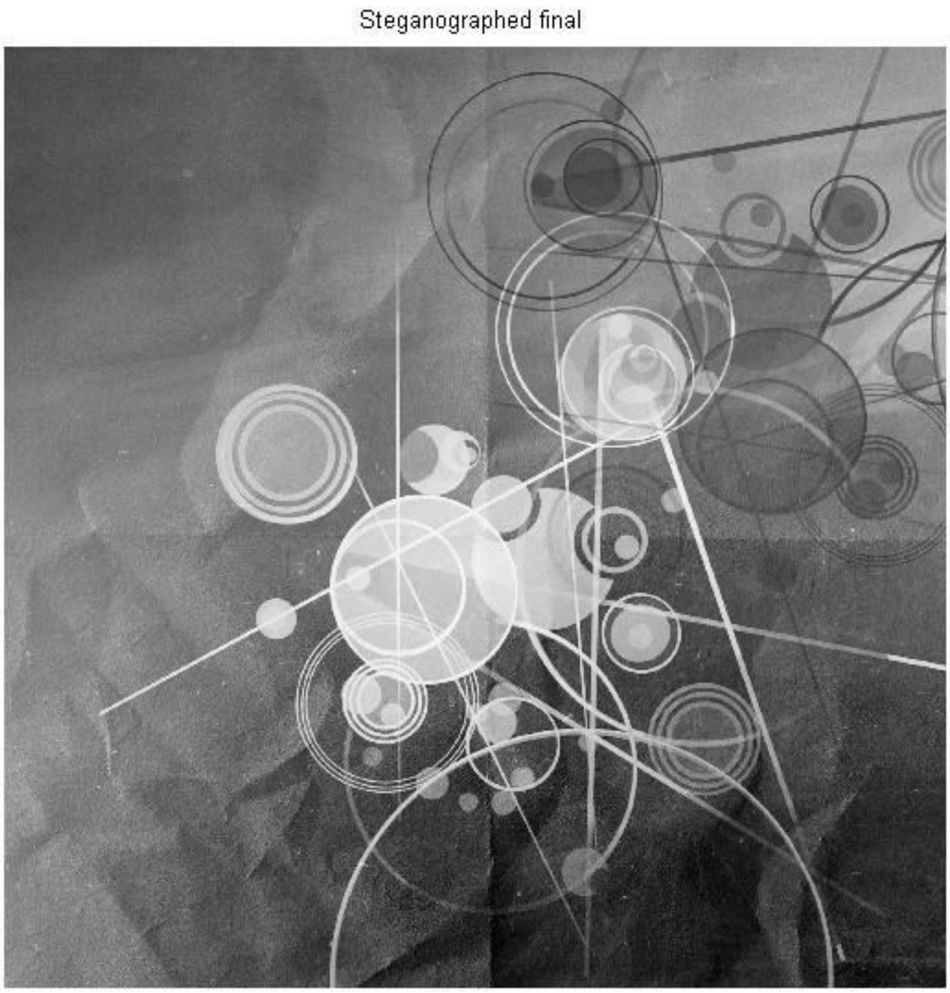
3 level dwt of cover image





Secret Image





Stego Image

Extraction Procedure:

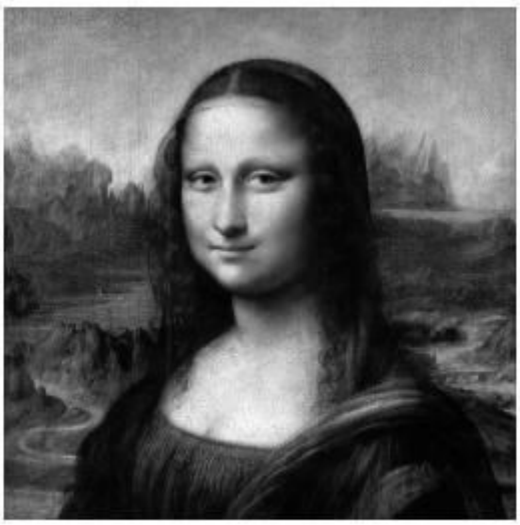
Extraction Procedure In this step extraction of secret message is carried out. Additionally correlation theory is being used. Correlation is the degree to which two or more quantities are linearly associated .The correlation between two same size matrices can be calculated by:

Input: An m × n carrier image and an m × n stego-image.
Output: a secret message/image.

Algorithm:

Steps-
1. Read the cover image (Ic)
2. Read the stego image (Is)
3. Decompose the Ic and Is by using Haar wavelet transform
4. Generate message vector of all ones
5. Find the correlation between the original and modified coefficients
6. Turn the message vector bit to 0 if the correlation value is greater than mean correlation value
7. Prepare message vector to display secret image

extracted secret image



QUALITY MEASUREMENT TECHNIQUES

The quality of the stego image and the extracted secret image is measured by calculation of certain quality measurement metrics. These metrics gives the comparison ratio between the original image and the modified image. The quality may be assessed on the basis of these values. The metrics used in this paper are as follows:

Peak signal to noise ratio (PSNR)

The PSNR depicts the measure of reconstruction of the compressed image. This metric is used for discriminating between the cover and stego image. The easy computation is the advantage of this measure. It is formulated as:

$$\mathrm{PSNR} = 10 \log 255^2 / \mathrm{MSE}$$

A low value of PSNR shows that the constructed image is of poor quality.

Mean square error (MSE)

MSE is one of the most frequently used quality measurement technique followed by PSNR. The MSE [6] can be defined as the measure of average of the squares of the difference between the intensities of the stego image and the cover image. It is popularly used because of the mathematical tractability it offers. It is represented as:

$$\boxed{\mathrm{MSE} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j) - f'(i,j))^2}$$

Where f (i, j) is the original image and f‟ (i, j) is the stego image. A large value for MSE means that the image is of poor quality.

Normalised Correlation (NK)

Normalised Correlation measures the similarity between the two images, i.e. the original image and the stego image. Larger values of NK indicate poorer image quality. Its value tends to one as the difference between the two images tends to zero . Normalised Correlation is formulated as:

$$\boxed{(\mathrm{NK}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[f(i,j).f'(i,j)]}{\sum_{i=1}^{M}\sum_{j=1}^{N}f(i,j)^2}}$$

Normalised absolute error (NAE)

The NAE is the measure of how distant is the modified image from the original image with the value of zero being the perfect fit. The normalised absolute difference can be calculated as:

$$\text{NAE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} \left| [f(i,j).f'(i,j)] \right|}{\sum_{i=1}^{M}\sum_{j=1}^{N} \left| f(i,j) \right|}$$

EXPERIMENTAL SUMMARY

On the basis of the formulae discussed above, various set of cover and secret images are compared. The cover images and the secret image used are shown below in Figure 14 and Figure 15, respectively.

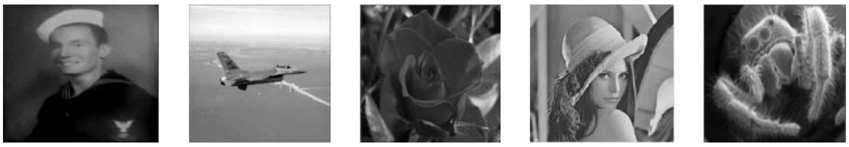


Figure 14. Cover images (.bmp)

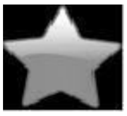
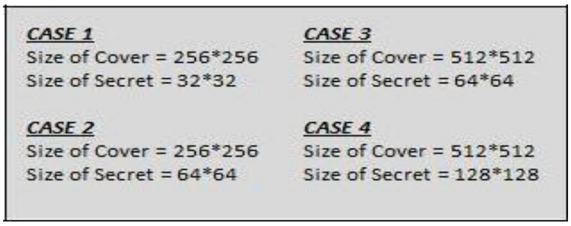


Figure 15. Secret Image embedded (.bmp)



CASE 1
Size of Cover = 256*256
Size of Secret = 32*32

CASE 2
Size of Cover = 256*256
Size of Secret = 64*64

CASE 3
Size of Cover = 512*512
Size of Secret = 64*64

CASE 4
Size of Cover = 512*512
Size of Secret = 128*128

Figure 16. Four cases for various set of sizes of cover and secret image

Technique Used	**PSNR Value**	**MSE**
LSB	44.2542	5.009
DWT	54.4232	3.5269

Comparison With LSB Technique

References

Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radioengineering, vol. 18, no. 4, (2009), pp. 509-516.

S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", *International Journal on Computer Science and Engineering*, IJCSE, vol. 1, no. 3, (2009).

C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "*Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems*", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

Po-Yueh Chen and Hung-Ju Lin, "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering* 2006. Vol 4, No. 3, pp 275-290.

https://en.wikipedia.org/wiki/Steganography

Student Details

IMAGE	Name & Address	Email ID	Phone No
	ABINESHWAR BISOI S/O-SUSANTA BISOI VILL-BULANPUR,Post-BULANPUR,DIST-PASCHIM MEDINIPUR ,West Bengal,Pin-721128	abineshwar.bisoi@gmail.com	8348375874
	SANTOSH KUMAR, S/O-NARESH PRASAD , KISHORE GUNJ ROAD NO.-7, RANCHI ,JHARKHAND, PIN-834001	sntshkmr1992@gmail.com	8513844115
	VIKASH KUMAR, S/O-RAM LALIT SINGH VIKASH NAGAR, MATHURAPUR, ,SAMASTIPUR,Bihar, PIN-848101	vikash.lalit1994@gmail.com	8513845230
	MANAV S/O-DIWAKAR SINGH, KUSHWAHA VATIKA, ISHWAR NAGAR, ISHAKCHAK, BHAGALPUR, BIHAR,PIN-812001	manavmanuprakash@gmail.com	8653153544