Covert Communication: A Steganography Algorithm

Shrikrishna Narvekar, Dr. Aisha Fernandes,

ME Student, Associate professor,
Information Technology Department,
Goa College of Engineering, Goa, India

Abstract : Data transmission secrecy is important as more and more people are joining the online world. The focus behind data security is to ensure privacy while protecting personal or business data. This demands the need to revamp techniques in the ancient science of steganography. Steganography is the art of concealing data in a manner that its existence itself cannot be detected. This demands the need to revamp techniques in the ancient science of steganography. This Proposed method aims to hide text data within an image, popularly known as image steganography. Transform domain technique is selected for hiding data taking into consideration its advantages over spatial domain image steganography. Our objective is to build stego-image that shouldn't be susceptible to Steganalysis. Once user enters the secret data to be hidden it gets convert into secret image. Text data within this secret image is not visible to the naked eyes. This secret image is further hidden into cover image which ultimately gives stego-image. Performance metrics were used to evaluate the quality of the stego-image as well as the extracted secret data. Experimental results indicate that the proposed techniques produce stego- images that are highly imperceptible.

***IndexTerms* - Discrete Wavelet Transform, Mean Square Error, Optical Character Recognition, Peak Signal to Noise Ratio.**

I. INTRODUCTION

In todays world one cannot survive without internet. There are approximately 4 billion internet users in the world. We browse everyday, do online shopping, perform many transactions online, people also communicate over internet. Concept of steganography is being widely used wherein there is a need to transport sensitive information from one point to another. When we think of covert communication security is a major issue that should be looked upon. The issue of security is taken care by two terms named Cryptography and Steganography. Cryptography is process of secret data transmission wherein sender encrypts the data and sends it to receiver. Receiver then decrypts the data. There are three types of cryptographic techniques: Symmetric- key cryptography, Hash functions and Public-key cryptography Symmetric-key cryptography: In this type of cryptographic techniques encryption and decryption takes place with the help of single key. Receiver uses same keys to decrypt the message that is being used by sender to encrypt message[1]. Hash functions: IN this technique a fixed length hash is computed per plain text as a result of which it is impossible to recover the content of plaintext[1]. Public key cryptography: This technique involves a pair of keys known as public key and private key. Encryption at the sender side takes place with the help of public key which is public and to everyone and decryption takes place only with the help of corresponding private key of the intended receiver[1].
Steganography is a concept of hiding a message within a cover medium as shown in the **figure I.1** below

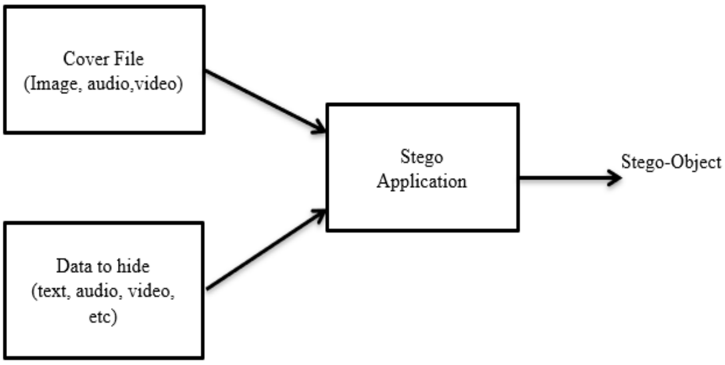


Fig. I.1. Process of Steganography

Steganography in image: When we talk about image steganography digital images where usually used earlier. An image as a whole is a collection of pixels containing different light intensities in its different areas. In an image steganography typically 8-bit and 24-bit images where used. Both this type of images have advantages as well as disadvantages. The advantage of 8-bit image is that it is of small size but it also has a drawback that only 256 colors are possible which is a potential problem due to encoding. When 24-bit images are used for steganography large number of colors can be used for beyond Human Visual System(HVS), which makes it hard to detect once a secret message, has been encoded. The heavy size of 24-bit images is a drawback which makes it suspicious over internet.[2] In general the characteristics of data hiding can be explained using **figure I.1.2** Imperceptibility, robustness to attacks, and the insertion capacity are in the corners of the magic triangle. This model is convenient for a visual representation of the required trade-offs between the capacity of the embedded data and the robustness to certain attacks, while keeping the perceptual quality of the stego-medium at an acceptable level.

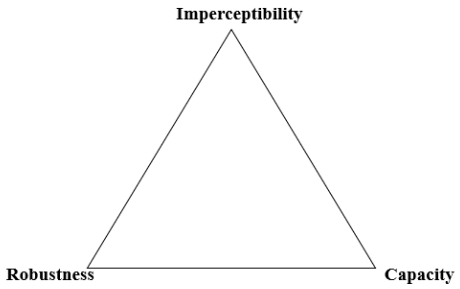


Fig. I.2. Characteristics of steganography

It is not possible to attain high robustness to signal modifications and high insertion capacity at the same time. Some of the differences between cryptography and steganography is that in case of cryptography message is encoded with the help of key and decryption takes place at receiver side. In this entire process attacker is aware that some secret communication is going on but in case of steganography is hard to detect presence of communication. The main goal to cryptography is data protection whereas that of steganography is data protection. Cryptography can be implemented only on text whereas steganography can be implemented on audio,video, image and text. Attack on cryptography is cryptanalysis wherein attacker tries to defeat or weaken the cipher text. Steganalysis is the art of discovering the fact some secret communication is taking place. Steganography is implemented in two domains: Spatial domain steganography and Transform domain Steganography In spatial domain technique pixel of an image are used directly to encode message within them. This technique is one of the simplest scheme in terms of embedding and extraction but has many drawbacks. When filtering is applied on stego-image some of the bits are lost which violates properties of steganography. There is also limitations on number of bits that can be hidden.[3] Transform domain is a complicated technique of steganography but it is much better in performance compared to spatial domain. In this technique message bits are embedded into coefficients which are calculated from cover image. Since secret data is in significant areas of cover image it is very difficult to detect presence of data. Message bits are not lost in case of transform domain steganography since it has ability to hold message even when image processing techniques are applied.[3] Taking into consideration advantages of transform domain techniques over spatial domain techniques we have selected transform domain technique in order to perform steganography. Transform domain techniques
are further divided into three types:
Discrete Fourier transforms technique (DFT)
Discrete cosine transforms technique (DCT)
Discrete Wavelet transforms technique (DWT)
All this three techniques mentioned above have their advantages as well as disadvantages. I have selected DWT technique since in DWT it is possible to extract message without destroying it.

II. LITERATURE REVIEW

A. Background

Information hiding is a domain which covers different methods which used not only in order to make data difficult
to read but also to hide its presence. The main aim of steganography is secret communication i.e. unauthorized person should not be aware of existence of message. In many organizations steganography is used to hide plans of new inventions. It is used in military and government messages. Apart from good usage of steganography application they can used for bad purpose also. People many also share the trade secrets of one company to other company without anyone being aware of it.Terrorist can also make use of steganography in order to keep their communication secret[4]. Nowadays researches have found out many new approaches in order to perform covert communication. Steganography concept in general terms is nothing but a covert communication which involves two terms i.e. cover object and stego object. Cover object is cover within which data is hidden and once data is hidden within an object we call it as stego object. The main principle behind steganography is a secrecy i.e. no one should be aware that some secret data is being transferred. With the purpose of adding more security some researcher encrypt the text and then embed it within the cover object. When we build a stego object it has
to obey properties of steganogrphy. Some of the important properties of steganography are:

1.Hiding Capacity: It refers to the amount of data that can be hidden in terms of bytes in such a way that carrier image within which data is hidden should not get distorted. The main aim of steganography is to hide maximum amount if data in such a way that carrier image should not get distorted. This is a key factor in making hidden data imperceptible and carrier image innocent and unsuspicious[5].

2.Imperceptibility: It means that data should be hidden in an undetectable way so that no one can see any visible artifacts or distortions in the carrier file. Therefore avoids the worries about any secret communication is taking place[5].

3.Irrecoverability: If a carrier file is intercepted then eavesdropper should not be able to decoded it and so as to extract the data hidden inside it. An irrecoverable steganography algorithm makes it hard for eavesdroppers and unauthorized third parties to recover the hidden data from the carrier despite knowing that steganography has been employed[5].

4.Robustness: It is the ability of the hidden message to remain undamaged even if stego-media undergoes transformation, sharpening, linear, and non-linear filtering, scaling ,blurring and various other techniques.[5]

B. Libraries used

1.OpenCv2: OpenCV was started at Intel in 1999 by Gary Bradsky and the first release came out in 2000. OpenCV supports wide variety of programming languages such as C++, Python, Java etc and it is available on different platforms such as Windows, Linux, OS X, Android, iOS etc. OpenCv python is the Python API of OpenCV. Python is programming language which became very popular because of its readability and simplicity. Python has many modules which can be used whenever required.We can perform big task by just calling this modules rather than writing those multiple lines of code[6]. opencv can be installed using
pip or commands through command prompt. The following command is used to install opencv**. pip install opencv**
If your system ask to upgrade then upgrade pip version by using following command **pip install upgrade pip**
If we are using anaconda navigator then we can directly in search package option.

2.Easygui: It is used for simple GUI programming in python.EasyGUI is different from other GUI generators in that EasyGUI is NOT event-driven. Instead, all GUI interactions are invoked by simple function calls.EasyGui provides an easy-to-use interface for simple GUI interaction with a user. It does not require the programmer to know anything about tkinter, frames, widgets, callbacks or lambda.EasyGUI runs on python 2 and python 3,and does not have any dependencies[9]. The reason of using this module is to create a dialogue box which can ask user to enter cover image, enter a text to be hidden etc. Once user selects image then we can observe the final results[7].

pip install easygui

3.Pywt: PyWavelet is open source wavelet transform software for Python.It combines a simple high level interface with low level C and Cython performance. The main features of PyWavelets are:

1.1D,2D and nD Forward and Inverse Discrete Wavelet Transform (DWT and IDWT)
2.1D,2D and nD Multilevel DWT and IDWT
3.1D and 2D Wavelet Packet decomposition and reconstruction

The new version pf pywavelets is 0.2. This version includes many new improvements and new features. One of such new feature is a two dimensional wavelet packet transform structure that is almost completely sharing programming interface with the one-dimensional tree structure.The way of installing pywavelets is we can directly search in package option and install or we can install it by using following command[8]

pip install Pywavelets

4.Pytesseract-OCR: Earlier digitization of document was achieved by manually typing the text on the computer but nowadays if we want to convert printed article into computer document then we can use scanner or Optical character recognition software. If you have a document scanner on your phone, such as Adobe Scan, you have probably encountered OCR technology in use. As an human being we all have eyes that can recognize pattern of light and dark that make up a characters. Similarly, computers can also do so with the help of OCR. Once we convert printed article into computer readable format then we can do all editing on it.Tesseract is an optical character recognition engine for various operating system. It can recognize more than hundred languages[9].

5.Pil: Pillow is the friendly PIL fork by Alex Clark and Contributors. PIL is the Python Imaging Library by Fredrik Lundh and Contributors. It is free library for python programming language which adds support for opening, manipulating and saving different image formats. It is available for windows, Mac OS x and Linux[10].

C. Related Work

L.Baby Victoria et al., (2017) has done study on spatial domain and transform domain steganography used in image hiding. In this paper they have done analysis on spatial and transform domain techniques and compared finally stating its advantages and disadvantages. They have done review of different papers who have worked in spatial domain i.e. LSB steganography, plane bit substitution method, LSB insertion mechanism using random number generation and application of noise filtering before embedding encrypted data. They have also worked on transform domain techniques such as discrete cosine transform and discrete wavelet transform. On comparing the performance of two techniques it was found that transform domain techniques are much more complicated then spatial domain techniques but very robust and offer high security[3].

Sanjay Yadav et al.,(2017)has done comparative analysis of canny edge based image steganography with RSA encryption. In this paper they have explained different types of steganography like text steganography, image steganography, audio steganography and protocol steganography. The properties of steganography were explained which needs to be taken into consideration while developing steganography application . In the further section they have explained different methods of steganography and explained RSA encryption. Further they have compared different techniques stating advantages and disadvantages of each one[5].

Biswarup Nandi et al.,(2017)has proposed approach of hiding encrypted text within a cover image using LSB algorithm for steganography. In this paper secret data is encrypted and then embedded into cover image. At the extraction phase embedded data is extracted into and decrypted using decryption algorithm. LSB technique is used to embed data in a image. In LSB method secret bit values of secret data are hidden in the least significant bit of the pixel values of the cover image[11].

Aisha Fernandes et al., (2015)has proposed covert communication techniques where she has hidden secret image within an edge of an image. To detect edges of image , modified Canny edge detection algorithm is used. Compressed secret image is hidden within a color pixel using 2 significant bits of 24 bit image. Further she has used logical operators for hiding and retrieving data. Bits of image which are not used for hiding are erased by using bit mask operators. Optimization criteria is used in order to minimize the bit storage[12].

Ronak Doshi et al. ,(2012) has done review on implementation of different techniques of text steganography , image steganography, audio steganography, as well as video steganography. In text steganography they have explained about LSB coding as well as masking and filtering. In audio steganography they have explained about LSB coding, parity coding, phase coding, spread spectrum as well as echo coding. Video is the collection images and sound so all the techniques mentioned for audio as well as image steganography are applicable for video steganography[13].

Tushara M et al.,(2016) has done review of image steganography using discrete wavelet transform. They have applied DWT on a cover image by splitting it first into single level DWT and further subsequently splitting it into two level and three level DWT. Embedding into the low frequency bands makes image more resistant to various attacks with equal possibility of stego image getting distorted. High frequency bands are used for embedding since they are less sensitive to human visual system. Finally it is concluded that DWT is less prone to attacks since coefficients of transform domain are altered. The amount of data hidden is less compared to spatial domain technique[14]

Sudhanshi Sharma et al. ,(2013)proposed review of transform domain techniques for image steganography. They have selected transform domain technique and within that they have selected two techniques i.e. discrete wavelet transform and discrete cosine transform are implemented and their performance is being evaluated with respect to performance evaluation parameters. DCT was found better in performance to DWT but when it comes to robustness DWT was found to be more robust compared to DCT. Extraction of message without destroying it was possible in DWT and hence offers maximum security[15].

Swapnali Zagade et al.,(2014) has proposed data hiding in an image using DWT technique. They have taken image of a small baby and hidden data within the skin region of that image. Once data is hidden image is cropped and DWT is applied on the cropped image. This increases quality of stego image. This increases quality of stego image. This stego image acts as an input to the extraction phase. Here, cropped value is required to retrieve the data. Once cropped value is obtained necessary data is retrieved using DWT[16].

Shashank gupta et al. (2015)[6] has proposed an innovative method for text steganography. They have taken cover image and applied DWT onto it. Further they have chosen low frequency components and hidden data within the low frequency component. At the receiver side they have used inverse discrete wavelet transform for recovery of original image. The algorithm has good security, good invisibility and good strength against lot of hidden attacks[17]

Noman Islam et al. ,(2016) has done survey on optical character recognition system. Optical character recognition converts printed text into images. There has been lot of research done in optical character recognition system as a result of which many systems have emerged.Based on the type of input, the OCR systems can be categorized as handwriting recognition and machine printed character recognition. It is found that handwriting character recognition is a tough job because many users have different ways of writing same character. Handwritten character recognition was classified into two sub categories as online and offline. Further different phases involved in OCR like Image acquisition, preprocessing,character segmentation etc were studied. Despite of there being many research carried out in OCR some languages like Arabic, Sindhi and Urdu are still not supported by OCR[18].

Riya. P. Ahuja et al. ,(2015) has done secure data transmission using data hiding technology.The document which being transmitted securely is converted into soft copy. This soft copy is encrypted into an image using LSB steganography. The hard copy docuement is converted into soft copy using OCR. Once a stego-image is obtained then it is send to the receiver. At the receiver end stego-image is passed through decryption module to obtain original text[19].

III. DESIGN

A. Conceptual Design

The outline of working of a application is mentioned in this section. Entire process runs in the following steps:

1. User gets dialogue box once he/she clicks on run asking whether to continue or not.
2. Once yes is clicked then user can select cover image.
3. Once cover image is selected then user enter text to be embedded(secret data).
4. This text is being converted into image which is known as secret image.
5. When secret image is stored within a cover image he will get a stego-image.

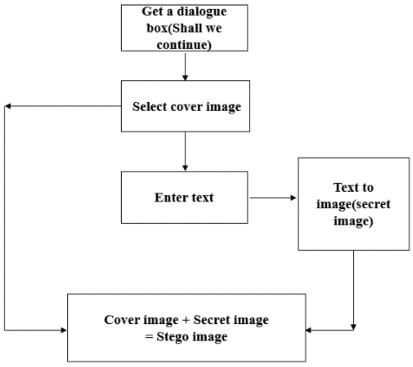

Get a dialogue box(Shall we continue)
Select cover image
Enter text
Text to image(secret image)
Cover image + Secret image = Stego image

Fig. III.1. Outline of stego image

Once receiver get image he has to perform following task

1. Retrieve secret-image from stego-image.
2. Extract secret text from stego-image.

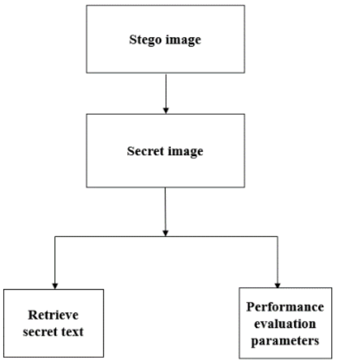


Fig. III.2. Outline of retrieving text from stego image

B. Detailed Design

In detailed design intermediate steps which will be discussed in detail. Above mentioned is the overview of the entire working process. I have faced many challenges at the time of building this application. Hiding part is easy but retrieval of text without loss is most difficult. At initial phase I found challenges in retrieving text. Some of the bits were lost at first retrieval. In order to overcome this problem i have converted text to image and then hidden this image within the cover image. Initially i tried hiding some six to seven characters. It was possible to retrieve all those characters without any loss but when i tried with big sentence i found that some characters were lost or got replaced. In order to solve this problem one experiment was conducted taking different font sizes and font styles and it was found that one particular font size with its style was more suitable.

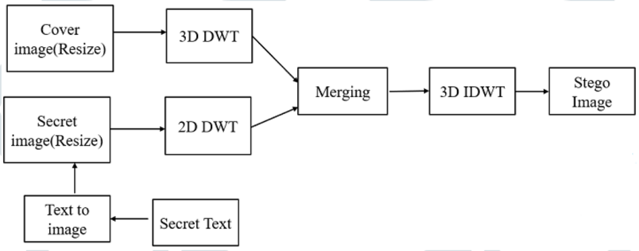


Fig. III.3. Detail procedure for obtaining stego image for hiding

For hiding text in an image

1. Input Cover Image and Secret Text.
2. Using OCR convert text to image.
3. Use the image as secret image.
4. Generate 3D DWT for Cover Image, 2D DWT for secret image.
5. Merge the two transformed images.
6. Get 3D IDWT of the merged image.
7. Generate Stego Image.

I have done resizing in order to make sure that images should not go out of index when performing DWT operations. If small image is selected then it wont be suitable to hide much amount of text. All the dwt operations are carried out using pywavelets library.

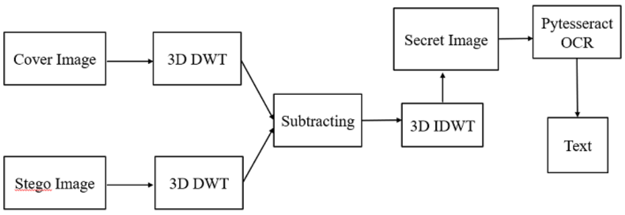


Fig. III.4. Detail procedure for obtaining cover image For hiding

For retrieving text in an image

1. Input Cover Image and Stego Image
2. Generate 3D DWT for both Images
3. Subtract the two transformed images, (secret = Stego - cover)
4. Get 2D IDWT of the secret image
5. Generate secret Image
6. Input the image in Pytesseract-OCR to be scanned
7. Generate secret text

C. Hiding Mechanism

Whenever a cover image is being selected the next step is performing 3D wavelet transform on it we divide the cover image by 255. The reason for dividing the cover image by 255 is that there are altogather 256 colors ranging from 0- 255 which are integer values. When we divide our image by 255 the RGB values are scaled from 0-1. The only reason for scaling the values from 0-1 is to avoid complexity in calculation. The background color of secret image we have choosen as gray and that of text as black.It is not possible for naked eye to figure out that some text is being hidden in cover image. At the extraction phase we have OCR which can detect color change and extract text from image.

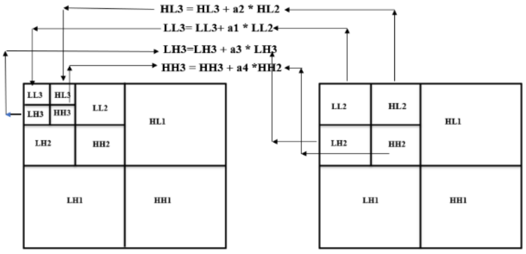


Fig. III.5. Hide secret text in a cover image

More often, steganography is performed on digital images. The technique proposed can work with RGB images too. Usually when DWT technique is applied on the color images they get converted into grayscale. This was one of the challenge faced by me when tried to use RGB images as a cover image. Initially i got grayscale colored image for RGB image which was very suspicious. I have tackled this issue in the following way:

secret data is hidden in the R band Stego image is obtained which is grayscale. Once a grayscale stego image is obtained then G and B bands of cover image are added to it in order to make it a RGB stego image.

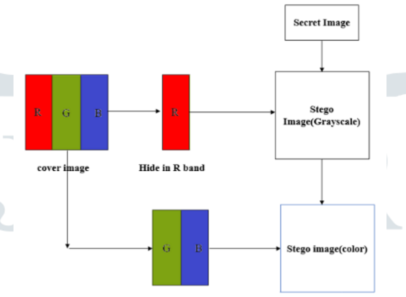
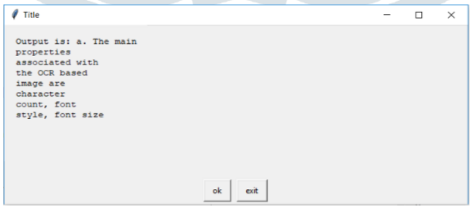


Fig. III.6. Obtain RGB stego image

IV. IMPLEMENTATION

When user runs an application a dialogue box appears asking user whether to proceed or not. Once he click on yes button get a dialogue box appears to select cover image. Once cover image is selected then user is allowed to enter text to be hidden in an image. This text gets converted into image which acts as a secret image. This secret Image is hidden within the cover image. In order to retrieve text from stego-image we need to first extract secret image from stego image. Once secret image is extracted then secret text can also be extracted from it. The obtained stego image and retrieved text is shown in the figure below.

Fig. IV.1. Obtained stego image



```
Output is: a. The main
properties
associated with
the OCR based
image are
character
count, font
style, font size
```

Fig. IV.2. Retrieved Text

V. RESULT

The proposed technique was tested on 25 images of different format like jpeg, png etc. Image clicked from mobile camera as well as online images are used as used as a cover images. Some of the images that were used as a cover are shown in the figure below.The resolution of cover images varied from 72*72 ,150*150 pixels to higher resolutions. The bits of data that can be stored varies. Samples of the original images analysed for study are shown in figure. The performance is finally measured with respect to performance evaluation parameters. Samples of images used as a cover image and stego image are shown below.

Fig. V.1. Cover image 1

Fig. V.2. Stego image 1

Fig. V.3. Cover image 2

Fig. V.4. Stego image 2

A. Performance Evaluation

The performance Evaluation can be done with respect to performance evaluation parameters shown below

1) Mean Square Error: As a performance measurement for image distortion, mean square error and the peak signal to noise ratio could be used as the key measures. MSE refers to the cumulative squared error between the modified and the original image. MSE is computed by performing byte by byte comparisons of the two images, since a pixel is represented by 8 bits and hence 256 levels are available to represent the various gray levels. Assuming I(i,j) to be the original image and I(i,j) to be the modified image, the MSE is computed as shown in equation 1 below

$$MSE = \frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[\, I(i,j) - I'(i,j)\ ] \qquad (1)$$

Where i and j are the image coordinates and M and N are the dimensions of the image.

2) Peak signal to noise ratio: The PSNR metric, measured in decibels (dB), expresses the degree of noise introduced after embedding the secret data, by comparing the original against the modified (compressed image or stego image). As the PSNR value increases stego image looks nearly same as original image. Human visual system is unable to distinguish images with PSNR more than 35 .PSNR value is inversely proportional to MSE value. If MSE is zero, PSNR becomes infinite, means no distortion occurs after embedding.PSNR is computed as shown in the equation 2 below

$$PSNR = 10 \times Log_{10}\ [\frac{Cmax^2}{MSE}] \qquad (2)$$

The MSE and PSNR Values for ten different images is shown in the Table 1 given below. PSNR values obtained are above 40 which a good value.

TABLE I
PERFORMANCE EVALUATION TABLE

Sr.No.	Images	MSE	PSNR(db)
1	Fabric.png(901kb)	0.8460	48.8567
2	Hands2.jpeg(226kb)	0.7988	49.1064
3	Car1.jpeg (23,981kb)	0.8511	48.8308
4	kids.tif(374kb)	0.8370	48.9032
5	forest.tif(396kb)	0.8177	49.0048
6	lighthouse.png(904kb)	0.8389	48.8934
7	green.jpeg(440kb)	0.8119	49.0356
8	canoe.tif(211kb)	0.8481	48.8463
9	pears.png(1043kb)	0.8502	48.8353
10	coins.png(217kb)	0.8127	49.0312

B. Experiment conducted

In order to check the nature of variation of PSNR with respect to hiding capacity one experiment is being conducted. I have taken same image as a cover image and varied amount data in bits to be hidden and obtained the results as shown in Figure below

TABLE II
VARYING PSNR VALUES VS VARYING DATA EMBEDDING

Sr.No	Cover Image	Secret Data	MSE	PSNR(db)
1	Autonm.tiff(209kb)	640	0.8276	48.9525
2	Autonm.tiff(209kb)	664	0.8278	48.9512
3	Autonm.tiff(209kb)	992	0.8283	48.9489
4	Autonm.tiff(209kb)	1112	0.8298	48.9416
5	Autonm.tiff(209kb)	1824	0.8305	48.9372

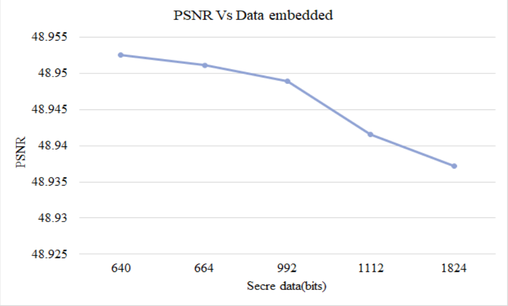


Fig. V.5. Performance (PSNR vs Data Embedded)

VI. Conclusion

In order to hide text data within an image transform domain steganography is effectively used. The objectives over here was to hide as much data as possible without being noticed. keeping in the mind the hiding capacity it is necessary to cross the limit of PSNR value above 35. The ultimate aim of steganography is to perform secret communication for which there should not be any difference in cover as well as stego-image. As can be seen from the results the difference between the cover and stego images was negligible. Secret image was not visible to naked eye. With the help of python as a programming language final code is optimised with faster processing. Anaconda navigator provides in built GPU support. It is not possible to hide a full paragraph of 100 to 200 words and OCR cannot detect difference between 0 and o so they get replaced with each other. In the future by using all the three color spaces i.e. RGB data can be hidden so that it hiding capacity will increase three times to the original capacity. In order to get better invisibility, make the background color of secret image as the average color of cover image.

VII. Acknowledgment

An endeavour over a period of time can be successful only with the constant support and guidance of our well wishers, hence I take this opportunity to express my gratitude to all those who encouraged me in getting a head start on my project work. I am immensely grateful to our principal Dr. Krupashankar M. S. who assured me every support from the college. I would like to thank our H.O.D. Dr. Nilesh B. Fal Dessai and our project coordinator as well as my guide Dr. Aisha Fernandes for providing me with excellent guidance, direction and constant support for successfully performing this project. Besides I am also grateful to all my friends and family for constantly being at my side. Lastly, I am grateful to the entire staff of the Information Technology department for providing me with the lab facilities and cooperation for my project work.

References

[1] Shashank(2019).What is cryptography?- An Introduction to Cryptographic Algorithms.
[2] Essays, UK(2018). Types and Techniques of steganography computer science, (17 pages) Essay in computer science.
[3] L.Baby Victoria, Dr.S.Sathappan , Swarup Biswas, (2015). A Study on Spatial Domain and Transform Domain Steganography Techniques used in Image Hiding ,International Journal Of Innovative Technology and Creative Engineering(ISSN:2045-8711)VOL.5.
[4] Ronak Doshi, Pratik Jain,Lalit Gupta (2012).Steganography and Its Applications in Security,International Journal of Modern Engineering Research (IJMER),Vol.2.
[5] Sanjay Yadav1 and A. K. Thripati2 (2017). Comparative Analysis of Canny Edge based Image Steganography with RSA Encryption, International Journal of Advanced Science and Technology Vol.104
[6] Alexander Mordvintsev and Abid K (2017). OpenCv- Python Tutorials Documentation.
[7] easygui dev team (2018). easygui Documentation.
[8] The PyWavelets Developers (2019). Pywavelets Documentation.
[9] Robley Gori(2019). PyTesseract: Simple Python Optical Character Recognition
[10] Alex Clark (2019).Pillow (PIL Fork) Documentation.
[11] Biswarup Nandi, Mousumi Ghanti (2017). Lossless] Steganography: An Approach for Hiding Text under Image Cover, Proceedings of the International Conference on Inventive Computing and Informatics (ICICI).
[12] Aisha Fernandes, Wilson Jeberson (2015). Covert Communication Using Arithmetic Division Operation, International Conference on Advanced Computing Technologies and Applications (ICACTA).
[13] Ronak Doshi, Pratik Jain,Lalit Gupta (2012). Steganography and Its Applications in Security, International Journal of Modern Engineering Research (IJMER),Vol.2.
[14] Tushara M1, K. A. Navas2,(2016). Image Steganography Using Discrete Wavelet Transform A Review, International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering, Vol. 3,
[15] Sudhanshi Sharma1, Umesh Kumar2 (2015). Review of Transform Domain Techniques for Image Steganography, International Journal of Science and Research (IJSR),Volume 4 Issue 5.
[16] Swapnali Zagade, Smita Bhosale(2014). Secret Data Hiding in Images by using DWT Techniques, International Journal of Engineering and Advanced Technology (IJEAT), Volume-3, Issue-5.
[17] Shashank gupta, Rachit Jain(2015). An Innovative Method of Text Steganography, Third International Conference on Image Information Processing.
[18] Noman Islam, Zeeshan Islam , Nazia Noor (2016). A Survey on Optical Character Recognition System, Journal of Information and Communication Technology- JICT Vol. 10.
[19] Riya. P. Ahuja, Mohini. R. Pasalkar, Ameya. J. Jadhav, Swati Shirke (2016). Secure Transmission of Hard Copy to Soft Copy Using OCR and Data Hiding Technology ,Journal of Information and Communication Technology-JICT Vol. 10.