ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 7, July 2015*

# Research Paper on Fuzzy Based Selection of Wavelets for Image Steganography

**Manika Bhatt**

M.Tech, Computer Science & Engg., Shree Siddhivinayak Group of Institutions , Yamuna Nagar, India

**Abstract**: Steganography refers to the practice of hiding secret messages in communications over a public channel so that an eavesdropper (who listens to all communications) cannot even tell that a secret messages are being sent. We give a precise model of a communication channel and a rigorous definition of steganographic security and prove that relative to a channel oraclesecure steganography exists if and only if one way exist function. We are given tightly matching upper and lower bounds on the maximum rate of any secure stego system. We introduce the concept of steganographic key exchange and public-key steganographyand show that provably secure protocols for these objectives exist under a variety of standard number-theoretic assumptions. We extend the concept of steganography as covert communication to include the more general concept of covert computation.

**Keywords**: Discrete Cosine Transformation, Graphics Interchange Format, Joint Photographic Experts Group.

## I. INTRODUCTION

Data security means to protect a database from destructive forces and the unwanted actions of unauthorize user. Huge amount of confidential informations is being exchanged over the Internet (publicly open medium) as this is the most cost-effective and widely available way. This technological progress has also made digital data very much vulnerable to interception and then possible unauthorized access/use and has caused significant economical losses for the content producers and rights holders. For protect data on public channels, the security measures need to be incorporated into data communication systems over the Internet.

## II. STEGANOGRAPHIC FRAMEWORK

A secret message will be concealed in a cover by applying an embedding algorithm to produce a stego_image. This stegomedium will then be transmitted by a communication channel like internet. For receiving the secret message which sent by the sender, receiver needs to use a recovering algorithm which is parameterised by stego_key to extract the message. A stego_key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to parties who know it. Figure 1.1 blew shows a generalized steganographic framework.

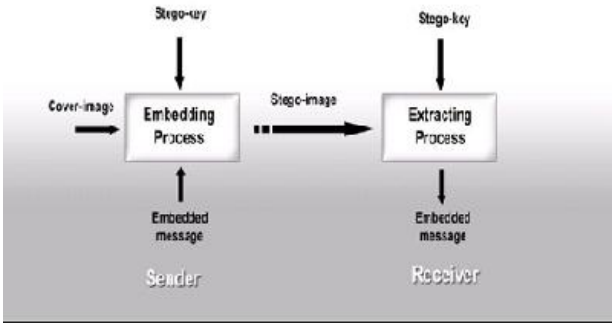



Figure.1.1: A generalized steganographic framework

The following formula provides a very generic description of the pieces of the steganographic process [4]:

cover_medium+ hidden data + stego_key = stego_medium

In this context, the cover_medium is the file in which is used to hide the hidden_data, which may be encrypted using the stego_key. The resultant file is the stego_medium (which will, of course. be the same type of file as the cover_medium).

## III. TECHNICAL BACKGROUND OF STEGANOGRAPHY

Steganographic methods primarily use image or audio files to hide encrypted data, thus enhancing overall security. Encrypted data on its own can attract the attention of hackers through its mere existence. . Using steganographic techniques, the information that needs to be concealed is dispersed within the least significant bits of a carrier file (e.g., image or audio file), which serves as a hiding place. It is important that the carrier files not lose their actual appearance during the embedding process. Steganos Security Suite, enable users to create suitable image or audio files, or to search their computers for available files. Most suitable are digital files with 24-bit color depth GIF and BMP files can safely be used for steganography.

There are two common compression techniques used to shrink the file size of a bitmap.

### A. GIF

The first is the GIF (Graphics Interchange Format) format, which will decrease the number of bits used to represent each pixel from 24 to 8. This is a lossless compression technique and the data hidden in the message can be recovered without a problem.

### B. JPEG

The JPEG (Joint Photographic Experts Group) is a form of lossy compression. It does a very nice job of decreasing the file size of the image and retaining a great deal of its quality. The JPEG transformation takes eight pixels by eight pixel blocks and performs a 64 bit DCT (Discrete

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 7, July 2015*

Cosine Transformation) does not compute to exact values. With continuing transforms, the precision of the calculation is decreased and the amount of error increases. Two methods used to perform a DCT are the Fast Fourier and wavelet transforms. The downside to JPEG compression is that it may corrupt hidden data.

## IV. RELATED WORK

In this thesis work a new algorithm is proposed for better data security and transferring of data from source to destination. A good approach to Image steganography using multi scale wavelet transform should aim at concealing the highest amount of data possible in a cover image while maintaining imperceptibility, that is, an acceptable level of visual quality for the stego image. The least significant bit scheme is one of the simplest and easily applicable data hiding methods, which directly embeds bits of secret data in the least significant bits of each image pixel. For, transform domain techniques discrete wavelets transform technique (DWT) and Discrete cosine transform (DCT) are used to protect the secret message.

[21] **Lisa M. Marvel, Member**, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, "Spread Spectrum Image Steganography" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999 1075.In this paper**, they present a new method of digital steganography, entitled spread spectrum image steganography (SSIS).** Steganography, which means "covered writing" in Greek, is the science of communicating in a hidden manner. Following a discussion of steganographic communication theory and review of existing techniques, the new method, SSIS, is introduced. This system hides and recovers a message of substantial length within digital imagery while maintaining the original image size and dynamic range. The hidden message can be recovered using appropriate keys without any knowledge of the original image.

[22] **Kevin Curran**, Internet Technologies Research Group, University of Ulster, Karen Bailey, Institute of Technology, Letterkenny, Ireland, "An Evaluation of Image Based Steganography Methods" International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, In this paper, **they studied seven stegnography methods in respect of their weakness and strength, they were evaluated to store maximum size of message in images.** Steganography is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message. This is a process, which can be used for example by civil rights organisations in repressive states to communicate their message to the outside world without their own government being aware of it. Less virtuously it can be used by terrorists to communicate with one another without anyone else's knowledge. In both cases the objective is not to make it difficult to read the message as cryptography does, it is to hide the existence of the message in the first place possibly to protect the courier. The initial aim of this study was to investigate steganography and how it is implemented. Based on this work a number of common methods of steganography could then be implemented and evaluated. The strengths and weaknesses of the chosen methods can then be analysed. To provide a common frame of reference all of the steganography methods implemented and analysed used GIF images. Seven steganography methods were implemented. The methods were chosen for their different strengths in terms of resistance to different types of steganalysis or their ability to maximize the size of the message they could store. All of the methods used were based on the manipulation of the least significant bits of pixel values or the rearrangement of colors to create least significant bit or parity bit patterns, which correspond to the message being hidden.

[23] **Kefa Rabah**, Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey, "Steganography-The Art of Hiding Data", Information Technology Journal 3 (3): 245-269, 2004,ISSN 1682-6027,Given the shear volume of data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved. One lesser-known but rapidly growing method is steganography, the art and science of hiding information so that it does not even appear to exist.
Moreover, in an ideal world we would all be able to openly send encrypted email or files to each other with no fear of reprisals. However, there are often cases when this is not possible, either because you are working for a company that does not allow encrypted emails or perhaps the local government does not approve of encrypted communication. This is one of the cases where Steganography can help hide the encrypted messages, images, keys, secret data, etc.
**This paper discusses the purpose of steganography. Explains how steganography is related to cryptography as well as what it can and cannot be used for. It also discusses a brief history of steganography.** In addition, some of the tools and software used in steganography are demonstrated and including some discussion of the most popular algorithms involved in these tools. This paper further explains the advantages and disadvantages, as well as, strengths and weaknesses in the use of steganography.

[24] **Hsien-Wen Tseng and Chin-Chen Chang**, Department of Computer Science and Information Engineering National Chung Cheng University, Chaiyi, Taiwan , "Steganography Using JPEG-Compressed Images" Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'2004). Sept. 2004 In this paper, a novel steganographic method based on JPEG is proposed. they take advantage of the quantization error resulting from processing the JPEG-compressed image with two different scaling factors. One of the scaling factors is used to control the bit rate of the stego-image while the other is used to guarantee the quality of the stego-image. Our experimental results show that the proposed

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 7, July 2015*

steganographic method can provide a high information hiding capacity and successfully control the compression ratio and distortion of the stegoimage.

## V. SIMULATION SETUP AND PERFORMANCE METRICS

### 5.1 SIMULATION SETUP

During this work we required MATLAB. MATLAB is a software package that lets you do mathematics and computation, analyse data, develop algorithms, do simulation and modelling, and produce graphical displays and graphical user interfaces. MATLAB contains built-in functionality to help you create your GUI programmatically. These include dialog boxes, user interface controls (such as push buttons and sliders), containers (such as panels and button groups), and ActiveX controls for Windows users. A GUI (graphical user interface) allows users to perform tasks interactively through controls such as buttons and sliders. Within MATLAB, GUI tools enable you to perform tasks such as plotting the graph and manipulating graphs.

You can also create custom GUIs for others to use either by running them in MATLAB or as standalone applications.

| Operating Systems | Processors | Disk Space | RAM |
|---|---|---|---|
| 32-Bit and 64-Bit MATLAB and Simulink Product Families | | | |
| Windows 7 or Service Pack 1<br>Windows Vista Service Pack 2 | Any Intel or AMD x86 processor supporting SSE2 | 1 GB for MATLAB only, 3–4 GB for a typical installation | 1024 MB (At least 2048 MB recommended) |

Table 4.1 Shows the MATLAB requirement for Windows

**Strengths of MATLAB**

- Easy to learn.
- Relatively quick to perform Matrix operation
- Behaves as a calculator and programming language

**Basic Areas-**

- Electrical circuits
- Control system
- Bio-informatics
- Image processing
- Mechanics

### 5.2 PERFORMANCE METRICS

PSNR (Peak Signal-to-Noise Ratio) of cover and watermarked videos. MSE (Mean Square Error) of cover and watermarked videos.The **PSNR (peak signal to noise ratio)** is used to measure the quality of stego Image compared to the cover image. It is calculated using equation 3.1, where MSE defined in 3.2 refers to mean square error.

$$PSNR = 20 \log_{10} \left( \frac{255}{RMSE} \right) \quad \ldots.3.1$$

Where RMSE is **Mean Square Error**, f (i,j) is pixel value of original image F(i,j) of stego image and its logarithmic unit is dB Given by Formula:

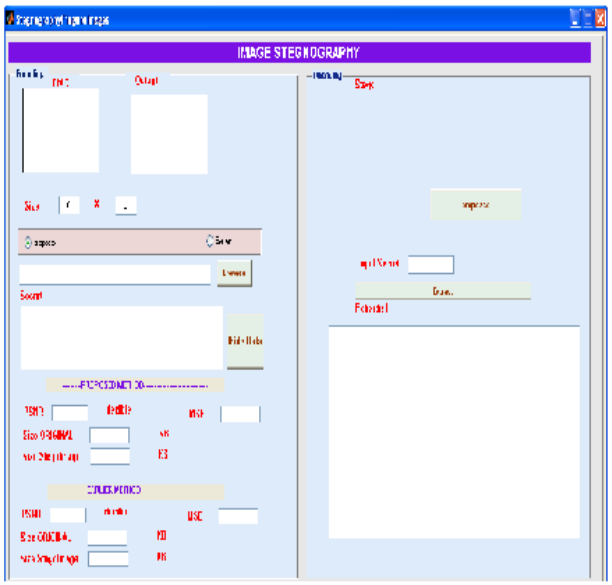
$$MSE = \frac{\sum [f(i,j) - F(i,j)]^2}{N^2} \quad \ldots.3.2$$

The quality of the image is higher if the PSNR value of the image is high. Since PSNR is inversely proportional to MSE value of the image, the higher the PSNR value is, the lower the MSE value will be. Therefore the better the stego image quality is the lower the MSE value will be.

## VI. RESULT

In this, results of all the intermediate steps of the proposed methods are highlighted. Implementation is done on MATLAB. Experimental results of intermediate steps show the efficiency of the proposed approach**.** Figure 6.1 shows encoding part, to embed/hide a secret message on image (initial GUI interface) select proposed method radio button for performing steganography using proposed method.

Figure 5.1: Opening GUI.




**Step 2:** load a cover image which is used to hide a secret message with the help of "Browse" button. In figure 4.2 input cover image is loaded.

**Step3:** Secret message is entered in secret message text box. Secret message "hello it is a secret message" is added.

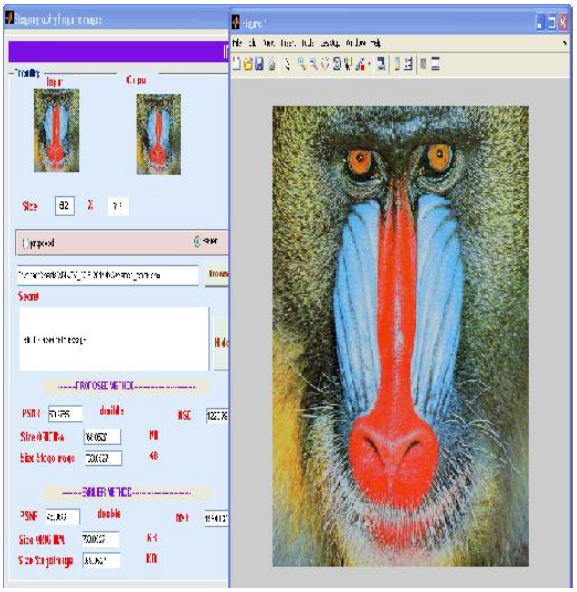
**Step 4:** Steganography is applied. After entering secret message, click on the "Hide Data" button. In this, Image is decomposed using HAAR Transform and data is embedded on the finest scale. First of all, the secret message "hello it is a secret message" is converted into bits, and then these bits embed into the cover image.

Steganography is applied. In the earlier method hide the same data on the same image using DWT technique. After entering secret message, click on the "Hide Data" button. First of all, the secret message "hello it is a secret message" is converted into bits, and then these bits embed

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 7, July 2015*

into the cover image. In text box, "Data has been added to the image" .



Select earlier radio button for performing steganography using earlier method.

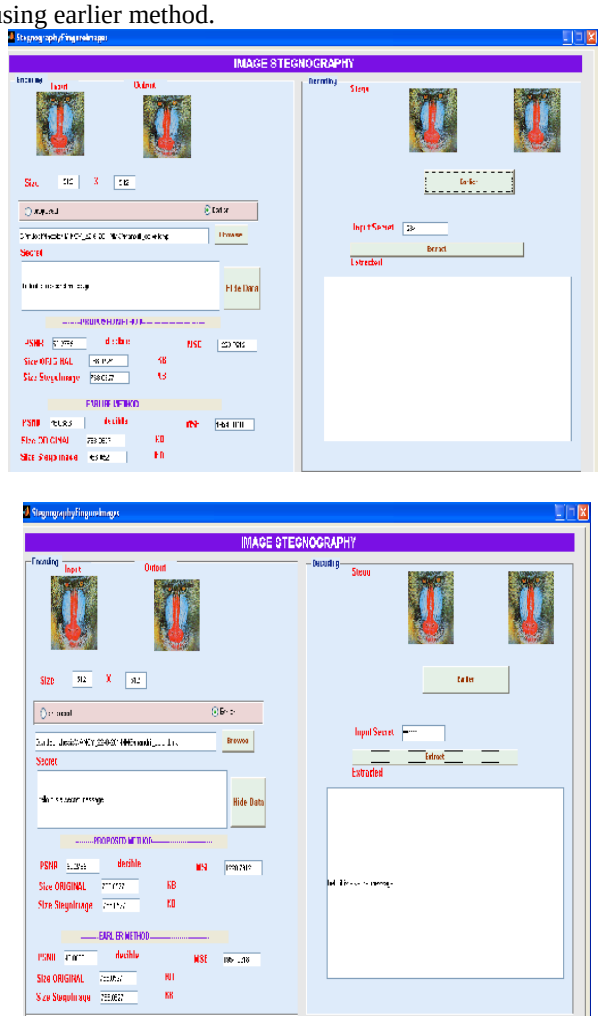



Figure 6.2 Decoding Phase (a) processed image (b) secret key (c) Secret message is extracted

The above figures show the results of the proposed and earlier work on an image. In the earlier method the value of PSNR is low and value of MSE is high. The results obtained using the proposed method are best as compared to earlier technique.

Table 6.1 Comparison of the values of PSNR and MSE for different Techniques applied on different images

| Name of File | Metrics | Size of image (KB) | | Earlier Method using DWT | Proposed Method |
|---|---|---|---|---|---|
| | | Original image | Stego image | | |
| Cameraman.bmp | PSNR | 768.05 | 768.05 | 46.115 | **59.60** |
| | MSE | 768.05 | 768.05 | 1963.1 | **1261.** |
| Lena_color_256.bmp | PSNR (decibel) | 192.05 | 192.05 | 32.148 | **44.72** |
| | MSE | 192.05 | 192.05 | 485.81 | **291.0** |
| Lena_gray_256.bmp | PSNR (decibel) | 192.05 | 192.05 | 32.264 | **45.75** |
| | MSE | 192.0 | 192.05 | 491.40 | **315.6** |
| Livingroom.bmp | PSNR (decibel) | 768.05 | 768.05 | 46.126 | **59.92** |
| | MSE | 768.05 | 768.05 | 1965.4 | **1302** |
| Mandril_color.bmp | PSNR (decibel) | 768.05 | 768.05 | 46.068 | **59.27** |
| | MSE | 768.05 | 768.05 | 1954.0 | **1220.** |
| Woman_darkhair.bmp | PSNR (decibel) | 768.05 | 768.05 | 45.998 | **59.25** |
| | MSE | 768.05 | 768.05 | 1940.4 | **1217.** |

## VII. CONCLUSION

The work accomplished during this thesis can be summarized with the following points: In this thesis we have presented a new system of Steganography using multi scale wavelet transform which could be proven as a highly secured method for data communication in future. Steganography is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the place. The proposed methods provides acceptable image quality with very little distortion in the image. The main advantage of this system is to provide high security for key informations exchanging. This system finds applications in medicine by doctors to combine explanatory informations within X--ray images.

It can be useful in communications for codes self error correction. It can embed corrective audio or image data in case corruption occurs due to poor connection or transmission.


DOI 10.17148/IJARCCE.2015.4782

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 4, Issue 7, July 2015*

The proposed High secured system using steganography was tested by taking message and hiding them in the input image. The experimental results showed that the proposed algorithm maintains the quality of the image ,appropriate,more efficient, simple and accurate than other algorithms as well as it makes the secret message more secure.

The results that are obtained from these experiments are recorded.

### 7.1 FUTURE SCOPE

For future work, this algorithm can be extended through the use of other quality matrics to judge the performance of this algorithm. Furthermore, this algorithm can be made faster in terms of execution. Further enhancement of results by applying some other algorithm than used in this thesis.

## REFERENCES

[1] Lisa M. Marvel, Member, IEEE, Charles G. Boncelet, Jr., Member, IEEE, and Charles T. Retter, Member, IEEE, "Spread Spectrum Image Steganography", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 8, AUGUST 1999.

[2] Kevin Curran, Internet Technologies Research Group, University of Ulster, Karen Bailey, Institute of Technology, Letterkenny, Ireland," An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2

[3] Kefa Rabah, Department of Physics, Eastern Mediterranean University, Gazimagusa, North Cyprus, Turkey," Steganography-The Art of Hiding Data", Information Technology Journal 3 (3): 245-269, 2004,ISSN 1682-6027

[4] Hsien-Wen Tseng and Chin-Chen Chang, Department of Computer Science and Information Engineering National Chung Cheng University, Chaiyi, Taiwan," Steganography Using JPEG-Compressed Images", Proceedings of the Fourth International Conference on Computer and Information Technology (CIT'2004). Sept. 2004

[5] H.-C. Wu, N.-I. Wu, C.-S. Tsai and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEEE Proc.-Vis. Image Signal Process., Vol. 152, No. 5, October 2005.

[6] S .K. Moon , R.S. Kawitkar, PICT, Pune and SCOE, Pune, INDIA," Data Security using Data Hiding", International Conference on Computational Intelligence and Multimedia Applications 2007.

[7] Nameer N. EL-Emam, Applied Computer Science Department, Faculty of Information Technology, Philadelphia University, Jordan," Hiding a Large Amount of Data with High Security Using Steganography Algorithm", Journal of Computer Science 3 (4): 223-232, 2007,ISSN 1549-3636 2007 Science Publications

[8] Sayuthi Jaafar1 and Azizah Abdul Manaf2,Ministry of Defense Malaysia," Code Generated Secret Steganography System (CGS3)", Postgraduate Annual Research Seminar 2007 (3-4 July 2007).

[9] G. Sahoo1 and R. K. Tiwari2, 1 Department of Computer Science &Engineering. , B.I.T., Mesra, Ranchi, Jharkhand, India, 2 Department of Computer Science &Engineering, R.V.S. College of Engg. & Tech., Jamshedpur, Jharkhand, India,," Designing an Embedded Algorithm for Data Hiding using Steganographic Technique by File Hybridization", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008.

[10] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain (2011) "*A New Approach for LSB Based Image Steganography using Secret Key*" IEEE.

[11] Jayeeta Majumder, Sweta Mangal (2012) "*An Overview of Image Steganography using LSB Technique* "IJCA.

[12] Baluram Nagaria, Ashish Parikh ,Sandeep Mandliya , Neeraj shrivastav4 (2012) "*Steganographic Approach for Data Hiding using LSB Techniques*". IJCR vol.2 issue 6.

[13] Shaveta Mahajan, Arpinder Singh (2012) "*A Review of Methods and Approach for Secure Stegnography"* IJARCSSE Vol. 2 issue 10.

[14] Mohammad Javad Khosravi , Ahmad Reza Naghsh-Nilchi. Department of Computer Engineering,University of Isfahan, Isfahan, Iran. "A novel joint secret image sharing and robust steganography method using wavelet" Multimedia Systems DOI 10.1007/s00530-013-0341-1©Springer-Verlag Berlin Heidelberg , October 2013