International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 3, May-June 2015 ISSN 2278-6856

Steganography Techniques: A Comparative Research Case Study

[1]Musavir Hassan, Er. Muheet Ahmed Butt[2] , Majid Zaman[3]

[1]University of Kashmir, Post Graduate Department of Computer Applications,
Hazratbal, Srinagar 190006, India

[2]University of Kashmir, Post Graduate Department of Computer Applications,
Hazratbal, Srinagar 190006, India

[3]University of Kashmir, Directorate of Information Technology and Support Systems,
Hazratbal, Srinagar 190006, India

Abstract

Steganography is the science and art of hiding information in ways that conceals the existence of embedded data. Information can be transferred from one place to another place through an appropriate multimedia carrier, e.g., image, audio, and video in a covert way. If the feature of secret data is visible, it can attract the attention from eavesdroppers and attackers. To hide secret data in images, there exists a large variety of Steganography techniques some are complicated than others and all of them have respective strong and weak points. The ultimate objectives of steganography are robustness, undetectability and capacity of hidden data. This paper provides a comparative analysis of hiding secret image in a cover image using steganography methods along with some common standards and guidelines drawn from the literature. The effectiveness of these techniques has been estimated on the basis of the parameters MSE, PSNR, Capacity and Robustness. In addition to this a new method for DWM is proposed with normal information loss.

Keywords: Least Significant Bit (LSB), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Mean Square Error, Peak Signal-To-Noise Ratio (PSNR)

1. INTRODUCTION

Steganography is the art and science of hiding the information in a covert way. Steganography improves the concept of Cryptography by hiding an encrypted message so that no one guesses it exists. Anyone scanning your data will fail to know that it contains a secret message. Today in digital age our ability to discover hidden information during our investigations is vital, especially as new and innovative methods continue to evolve. In this modern era, data hiding technologies have sophisticated from limited use to ubiquitous deployment[26][27][28][29][30]. With the rapid advancement in emerging technologies, the need to protect valuable proprietary information has generated a plethora of new methods and technologies for both good and evil [31][32][33][34][35]. Most dangerous among these are those that employ hiding methods along with cryptography, thus providing a way to both conceal the existence of hidden information while strongly protecting the information even if the channel is discovered. Many vendors provide excellent technologies for protecting the privacy of information for the desktop. In addition, many of the latest smart mobile platforms (Android and iPhone) include built-in cryptographic capabilities. What is more dangerous and difficult to discover/decipher are data hiding methods that exploit multimedia and protocol weaknesses to both hide and communicate covertly. These new techniques provide hybrid solutions that combine the best of cryptography with the best of steganography. The interest, innovation, and advancement of these threats continue to go unchecked for the most part. There are four ultimate objectives of steganography viz; Imperceptibility, Security, Capacity and Robustness and the important requirement for steganography system are as follows.

- Security of hidden communication
- Size of payload
- Robustness against harmful and unintentional attacks

The basic flow of processes that takes place in image steganography is shown in Figure1 below. In this steganography process secret message is embedded inside the cover object by a hiding algorithm and is sent to a receiver. The receiver then applies the reverse process on the cover data and reveals the secret data.

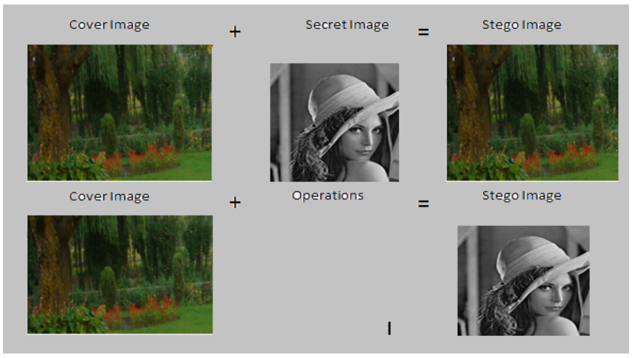


Figure 1: Processing of Steganography

2. TYPES OF STEGANOGRAPHY

Almost all digital file formats can be used for steganography, but the formats that are more suitable are those with a high degree of redundancy. Redundancy can be defined as the bits of an object that provide accuracy far greater than necessary for the objects use and display. The redundant bits of an object are those bits that can be altered without the alteration being detected easily image and audio files especially comply with this requirement, while research has also uncovered other file formats that can be used for information hiding. These are four main categories of file formats that can be used for information hiding. There are four main categories of file formats that can be used for steganography shown in figure2.

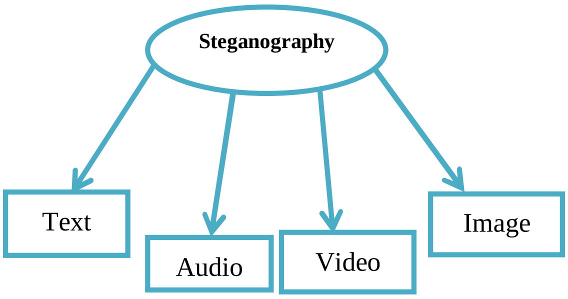


Figure 2: Types of Steganography

Since images are quite popular cover or carrier objects used for steganography. In the domain of digital images many different image file formats exist, most of them for specific application. For these different image file formats, different steganography algorithms exist. Here, in this paper, we will discuss about the image domain steganography methods.

3LITERATURE SURVEY

This paper analyses the various articles on steganography which help to understand the topic in a new perspective.

3.1 Spatial Domain Techniques

Deshpande Neeta,et. al, [1] proposed the Least Significant Bit embedding technique. This paper explains the LSB embedding technique and presents the evaluation results for 2,4,6 Least significant bits for a .pngfile and a .bmp file and also suggests that data can be hidden in the least significant bits of the cover image and the human eye would be unable to notice the hidden image in the cover file.

Aneesh jain et. al, [2] proposed a scheme which hides data in bitmap images, in a way that there is almost no perceptible difference between the original image and this new image and which is also resistant to JPEG compression and retrieve the whole data from an image after hiding it in a raster graphics image.

G.R.Manjula et. al, [3] presents a novel 2-3-3 LSB insertion method in which a quality of a steganographic system is to be less distortive while increasing the size of the secret message.

Aung Tint Phyo, [4] presents a paper Image Steganography Based Audio Security System. This paper proposes the combination of a cryptographic algorithm and a steganographic method to obtain the high level of information security. In this proposed system, secret audio message is encrypted with the help of AES encryption algorithm and then the encrypted audio message is embedded into a cover image by using LSB technique.

In M.B Ould MEDENI et. al's article [5], the authors propose a novel method for hiding information within the spatial domain of the gray scale image. The pixel value differencing(PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block pair(for data embedding. While embedding secret data, each pixel is split into two equal parts. The number of 1's in the most significant part is counted and the secret message is embedded in the least part according to the number of corresponding bits.

In Weiqi Luo et. al's paper [6], the authors propose an edge adaptive scheme which can select the embedding regions according to the size of the secret message and the difference between two consecutive pixels in the cover image. In the data embedding stage, the scheme first initializes some parameters, which are used for estimating the capacity of the selected regions. Finally stego image is obtained after pre-processing. A region adaptive scheme is applied to the spatial LSB domain and the difference between two adjacent pixels is used as a criterion for region selection .

In C.H. Yang et. al.'s article [7]. A predictive method to enhance the histogram-based reversible data hiding approach is proposed. Two interleaving predictive stages are used. Most pixels are predicted by their two neighbourhood pixels and four neighbouring pixels in the column –based and chess-board-based approach. The difference value of each pixel between the original image and the stego image remains within +-1. In interleaving predictions, pixels in odd columns will be predicted by pixels in even columns or vice versa.

[8] presents analysis of Least Significant Bit (LSB) based Steganography and Discrete Cosine Transform (DCT) based Steganography.

In Shamim Ahmed Laskar et. al's [9] method data is embedded into the red plane of the image and the pixel is selected using a random number generator. It is almost impossible to notice the changes in the image. A stego key is used to seed the PRNG(pseudo Random Number Generator) to select pixel locations. This paper focuses on increasing the security of the message and reducing the distortion rate.

In Mamta Juneja et. al's [10] research paper a secured robust approach of information security is proposed. It presents two component based LSB (Least Significant Bit) methods for embedding secret data in the LSB's of blue components and partial green components of random pixel locations in the edge of images. An adaptive LSB based steganography is proposed for embedding data based on data available in MSB's of red, green and blue components of randomly selected pixels across smooth areas. It is more robust as it is integrated with an Advanced Encryption Standard (AES).

In S.Shanmuga Priya et. al's [11]article the authors propose a novel method based on LSB. Data embedding is performed using a pair of pixels as a unit, where LSB of the first pixel carries one bit of information and a function to two pixel values carries another bit of information. The proposed method shows better performance in terms of distortion and resistance against existing steganalysis. Embedding is done in the sharper edge region using a threshold. PSNR value is compared for adaptive and non-adaptive techniques of data hiding in gray scale and color images.

In Jasvinder Kaur et. al's article [12] the authors analyse different steganographic techniques based on digital logic and proposes a new enhanced steganographic technique based on it. The carrier image is selected depending on the information to carry. This technique uses digital operations based on logic gates and shift operators to embed/derive the hidden information from image data. Depending on the size of the information to embed the carrier image is divided into rows and data is embedded using digital operation.

3.2 Transform Domain Methods

NedaRaftari et. al [13] proposed a novel image steganography technique that combines the integer Wavelet Transform(IWT) and Discrete Cosine Transform (DCT) which embeds secret image in frequency domain of cover image with high matching quality.

In the another article Hemalatha. S et. al [14] Integer Wavelet Transform (IWT) have been suggested to hide multiple secret images and keys in a color cover image which is more efficient. The cover image is represented in the YCbCr color space. Two keys are obtained, encrypted and hidden in the cover image using IWT.

In Prosanta Gope et. al.'s article [15], the authors introduce an enhanced JPEG steganography along with a suitable encryption methodology using a symmetric key cryptographic algorithm. The JPEG cover image is broken into 8 x 8 blocks of pixel. DCT is applied to each block and quantization is done and data is encrypted using a new encryption method which uses CRC checking.

In Hemalatha.S et. al's [16] paper, the authors propose a method that uses two gray scale images of size 128 x128 that are used as secret images and embedding is done in RGB and YCbCr domains. The quality of stego images is good in RGB domain by comparing the PSNR values. The authors have used integer Wavelet Transform (IWT) to hide secret images in the color cover image. The authors have compared the PSNR values and image quality when embedding is done in the RGB and YCbCr domains.

In another article of Hemalatha .S et. al, [17] Integer Wavelet Transform(IWT) have been suggested to hide multiple secret images and keys in a color cover image which is more efficient. The cover image is represented in the YCbCr color space. Two keys are obtained, encrypted and hidden in the cover image using IWT.

In S.Arivazhagan et. al.'s work[18] the authors propose method that works in the transform domain and attempts to extract the secret almost as same as the embedded one, maintaining minimal changes to cover image by using techniques like median maintenance , offset and quantization. A modified approach for embedding color images within color images is proposed and it overcomes the limitation in embedding.

Shana T [19] in his paper An Enhanced Security Technique for steganography Using DCT and RSA proposes a DCT- steganography based on encryption to provide high security steganography and cryptography are combined together. This system encrypts secret information before embedding it in the image. The encrypted image is placed in the mid frequency DCT coefficients of cover image, So that embedding done efficiently.

4 IMAGE STEGANOGRAPHY TECHNIQUES

There are two types of domains in which steganography is implemented i.e. spatial domain & frequency domain. In spatial domain, processing is applied directly on the pixel values of the image whereas in frequency domain, pixel values are transformed and then processing is applied on the transformed coefficients. LSB technique is implemented in spatial domain while DCT & DWT technique are implemented in frequency domain. In least significant bit (LSB), each pixel of an image transformed into the binary value and data is hidden into the least significant position of the binary value of the pixels of the image in such a manner that, it doesn't destroy the integrity of the cover image but this scheme is sensitive to a variety of image processing attacks like compression, cropping etc. The discrete cosine transforms (DCT) & discrete wavelet transform (DWT) are mathematical functions that transforms digital image data from the spatial to the frequency domain. In DCT, after transforming the image in frequency domain, the data is embedded in the least significant bits of the medium frequency components and is specified for lossy compression while In DWT, secret messages are embedded in the high frequency coefficients resulted from Discrete Wavelet Transform and provide maximum robustness.

In this section evaluation parameters and proposed embedding and retrieval techniques are discussed.

4.1 Least Significant bit Substitution Technique (LSB)

In LSB Steganography, the least significant bits of the cover media's digital data are used to conceal the message. The simplest of the LSB steganography technique is LSB replacement. LSB replacement steganography flips the last bit of each of the data values to reflect the message that needs to be hidden. Consider an 8-bit gray scale bitmap image where each pixel is stored as a byte representing a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values.

11010010 01001010 10010111 10001100 00010101
01010100 00100110 01000011

To hide the letter C whose binary value is 10000011, we would replace the LSB's of these pixels to have the following new gray scale values:

11010011 01001010 10010110 100001100 00010100
01010110 00100111 01000011

Note that on average, only half the LSB's need to change. The difference between the cover (i.e.; original) image and the stego image will be hardly noticeable to the human eye. However, one of its major limitations is small size of data which can be embedded in such type of images using only LSB.LSB is extremely vulnerable to attacks. LSB techniques implemented to 24 bit formats are difficult to detect contrary to 8 bit format [18]. Another example of LSB technique is: Consider a grid for 3 pixels of a 24 bit image and the number 300 is to be embedded using LSB technique. The resulting grid is as follows:
PIXELS:

$$\begin{pmatrix} 01010101 & 01011100 & 11011000 \\ 10110110 & 11111100 & 00110100 \\ 11011110 & 10110010 & 10110101 \end{pmatrix}$$

Here the number C was embedded into the first 8 bytes of the grid, only 1 bit needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size.

4.2 Discrete Cosine Transform Technique (DCT)

DCT coefficients are used for JPEG compression [20][21]. It separates the image into parts of differing importance. It transforms a signal or image from the spatial domain to the frequency domain. It can separate the image into high, middle and low frequency components. In low frequency sub-band, much of the signal energy lies at low frequency which contains most important visual parts of the image while in high frequency sub-band, high frequency components of the image are usually removed through compression and noise attacks [22]. So the secret message is embedded by modifying the coefficients of the middle frequency sub-band so that the visibility of the image will not be affected. The general equation for a 1D (N data items) DCT is defined by the following equation: [21]

Here, the input image is of size N x M, c (I , j) is the intensity of the pixel in row I and column j; C(u , v) is the DCT coefficient in row u and column v of the DCT matrix. DCT is used in steganography as image is broken into 8 x 8 blocks of pixels. Working from left to right, top to bottom, DCT is applied to each block. Each block is compressed through quantization table to scale the DCT coefficients and message is embedded in DCT coefficients.

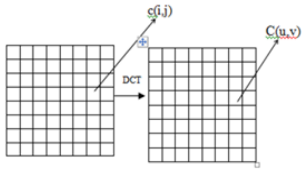


Fig3: Discrete Cosine Transformation of an Image

Figure 3: Discrete Cosine Transformation of an Image

$$C(u) = a(u)\sum_{i=0} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)$$

Where u, v = 0,1,2….N-1
The general equation for a 2D(N by M image) DCT is defined by the following

$$C(u,v) = a(v)\sum_{i=0}^{N-1}[a(u)\sum_{i=0}^{N-1} x_i \cos\left(\frac{(2i+1)u\pi}{2N}\right)] \times \cos\left(\frac{(2i+1)v\pi}{2N}\right)$$

4.2.1 The Middle Band Coefficient Scheme

The middle-Band frequencies (FM) of an 8 x 8 DCT block are shown in Figure 4. In this figure, FL is used to denote the lower frequency components of the block and FH is used to denote the higher frequency components. FM is chosen as embedding region to provide additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. First, 8 x 8 DCT of an original image is taken. Then, two locations DCT (u1,v1) and (u2,v2) are chosen from the FM region for comparison of each 8 x 8 block. These locations are selected based on the recommended JPEG quantization table shown in Table 1. If two locations are chosen such that they have identical quantization values, then any scaling of one coefficient will scale the other by the same factor to preserve their relative strength. It may be observed from Figure 2, that coefficient at location (4, 1) and (3, 2) or (1, 2) and (3, 0) are more suitable candidates for comparison because their quantization values are equal. The DCT block will encode a "1" if DCT (u1, v1) > DCT (u2, v2); otherwise it will encode a "0". The coefficients are swapped if the relative size of coefficients does not agree with the bit that is to be encoded.

Thus, instead of embedding any data, this scheme is hiding watermark data by means of interpreting "0" or "1" with relative values of two fixed locations in middle frequency region.

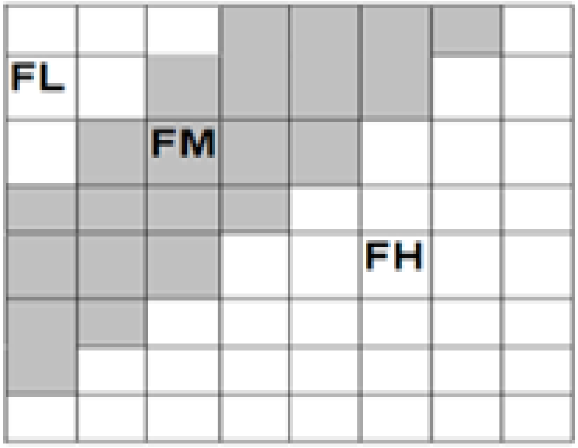


Figure 4: Frequency regions in 8*8 DCT

$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

Quantization Table

4.3 The Discrete Wavelet Transform (DWT)

The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. To analyse a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). Wavelet analysis can be of two types: continuous and discrete. In this paper, discrete wavelet transform technique has been used for image steganography. This method transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object. Human eyes are less sensitive to high frequency details. Here the Haar DWT - simplest type of DWT has been applied. In 1D-DWT average of fine details in small area is recorded. In case of 2D-DWT we first perform one step of the transform on all rows. The left side of the matrix contains down sampled low pass coefficients of each row; the right side contains the high pass coefficients as shown in the Fig5 First stage of step1 wavelet decomposition.

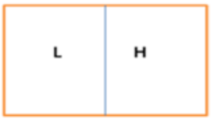


Figure 5: First Stage of Step1 Wavelet Decomposition

Next, we apply one step to all columns. This result in four types of coefficients: LL, HL, LH, HH as follows:

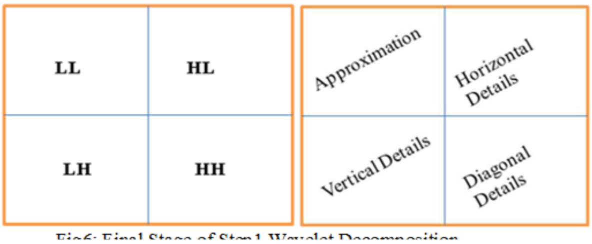


Figure 6: Final Stage of Step1 Wavelet Decomposition

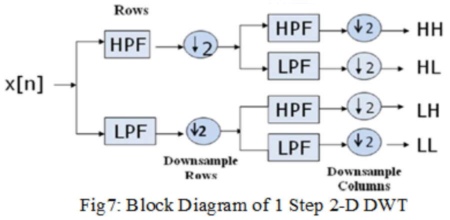


Figure 7: Block Diagram of 1 step 2-D DWT

For example;

Figure 8: Original Image

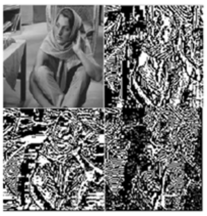


Figure 9: After 1 Step Decomposition by 2D-DWT

The subdivided squares represent the use of the pyramid subdivision algorithm to image processing, as it is used on pixel squares. At each subdivision step the top left-hand square represents averages of nearby pixel numbers, averages taken with respect to the chosen low-pass filter; while the three directions, horizontal, vertical, and diagonal represent detail differences, with the three represented by separate bands and filters. We can continue decomposition of the coefficients from low pass filtering in both directions further in the next step.

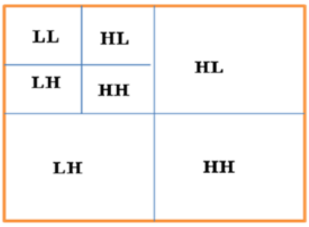


Figure 10: 2 Step Decomposition

5 Metric Evaluation

For comparing stego image with cover results requires a measure of image quality, commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio.

5.1 Mean-Squared Error

The mean-squared error (MSE) between two images I1 (m,n) and I2 (m,n) is:

$$MSE = \frac{\sum_{M,N}[I1(m,n) - I2(M,N)]^2}{M * N}$$

M and N are the number of rows and columns in the input images, respectively. Mean-squared error depends strongly on the image intensity scaling. A mean-squared error of 100.0 for an 8-bit image (with pixel values in the range 0-255) looks dreadful; but a MSE of 100.0 for a 10-bit image (pixel values in [0,1023]) is barely noticeable.

5.2 Peak Signal-to-Noise Ratio

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

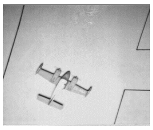
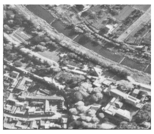
Peak Signal-to-Noise Ratio (PSNR) avoids this problem by scaling the MSE according to the image range.

PSNR is measured in decibels (dB). PSNR is a good measure for comparing restoration results for the same image, but between images comparisons of PSNR are meaningless.

6.Observations

The algorithms are tested in MATLAB. The result with cover image and secret image are shown. The cover image size is 256×256 and secret image size is 32×32. Comparative analysis LSB based, DCT based & DWT based steganography has been done on basis of parameters like PSNR, MSE on images shown below and the results are evaluated. If PSNR ratio is high then images are of best quality.

Table 1: PSNR and MSE Comparison of LSB, DCT, DWT

COVER IMAGE	LSB	DCT	DWT
	PSNR: 22.7209 MSE: 50.2601	PSNR: 34.3621 MSE: 24.0031	PSNR: 24.5075 MSE: 232.1313
	PSNR: 22.7209 MSE: 50.2601	PSNR: 31.1742 MSE: 50.0105	PSNR: 24.5075 MSE: 232.1313
	PSNR: 22.8421 MSE: 40.6178	PSNR: 33.8497 MSE: 27.0089	PSNR: 24.5075 MSE: 232.1313

7.CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself .In this paper, analysis of LSB, DCT & DWT methods has been successfully implemented and results are delivered. The MSE and PSNR of the methods are also compared and also this paper presented a background discussion and implementation on the major algorithms of steganography deployed in digital imaging. The PSNR shows the quality of image after hiding the data. From the results, it is clear that PSNR of DCT is high as compared to the other two techniques. This implies that DCT provides best quality of the image. An embedding algorithm is said to be robust if the embedded message can be extracted after the image has been manipulated without being destroyed. DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and provides maximum security.

References

[1] Deshpande Neeta, KamalapurSnehal, Daisy Jacobs, "Implementation of LSB Steganography and Its Evaluation for Various Bits", 2004.

[2] AneeshJain,IndranilSen.Gupta, "A JPEG Compression Resistant Steganography Scheme for Raster Graphics Images",IEEE-1-4244-1272-2/07/$25.00©2007.

[3] G.R.Manjula and Ajit Danti, A Novel hash based least significant bit (2-3-3) image steganography in spatial domain, International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 4, No 1, February 2015

[4] Aung Tint Phyo, Su Wai Phyo, Image Steganography Based Audio Security System, International journal of scientific research and technological research, Vol.03,Issue.10

[5] M.B.Ould MEDENI and El Mamoun SOUIDI, (2010) "A Generalization of the PVD Steganographic Method", International Journal of Computer Science and Information Security, Vol.8.No.8, pp156-159

[6] Weiqi Luo, Member, IEEE, Fangjun Huang, Member, IEEE, and Jiwu Huang, Senior Member, IEEE, (2010) "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, Vol.5.No.2, pp.201-214.

[7] C.-H. Yang and M.-H. Tsai, (2010) "Improving Histogram-based Reversible Data Hiding by Interleaving Predictions", IET Image Processing, Vol.4. Iss. 4 pp. 223-234.

[8] Vol. 10 Issue 1 (Ver 1.0), April 2010 Global Journal of Computer Science and Technology An Analysis of LSB & DCT based Steganography GJCST Computing Classification *F.2.1 & G.2.m*

[9] Shamim Ahmed Laskar and Kattamanchi Hemachandran, (2013) "Steganography Based On Random Pixel Selection For Efficient Data Hiding", International Journal of Computer Engineering and Technology, Vol.4, Issue 2, pp.31-44.

[10] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No:3, pp.405-424.

[11] S.Shanmuga Priya, K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits in Spatial Domain", International Journal of Engineering Research and Applications,, Vol2, Issue 3, pp. 2632-2637.

[12] Jaswinder Kaur, Inderjeet & Manoj Duhan, (2009) "A Comparative Analysis of Steganographic Techniques", International Journal of Information

Technology and Knowledge Management, Vol. 2, No. 1, pp 191-194.

[13] NedaRaftari and Amir MasoudEftekhariMoghadam, “Digital Image Steganography Based on Assignment Algorithm and Combination of DCT-IWT”, Fourth International Conference on Computational Intelligence, Communication Systems and Networks, 2012.

[14] Hemalatha.S, U.Dinesh Acharya and Renuka.A, Priya.R Kamnath, (2013) “A Secure and High Capacity Image Steganography Technique”, Signal & Image Processing – An International Journal.

[15] Prosanta Gope, Anil Kumar and Gaurav Luthra , (2010) “An Enhanced JPEG Steganography Scheme with Encryption Technique”, International Journal of Computer and Electrical Engineering ,Vol.2.No.5, pp924-930.

[16] Hemalatha.S, U.Dinesh Acharya and Renuka.A, (2013) “Comparison of Secure and High Capacity Color Image Steganography Techniques in RGB and YCBCR domains”, International Journal of Advanced Information Technology, Vol.3, No.3, pp.1-9.

[17] Hemalatha.S, U.Dinesh Acharya and Renuka.A, Priya.R Kamnath, (2013) “A Secure and High Capacity Image Steganography Technique”, Signal & Image Processing – An International Journal,Vol.4, No.1, pp.83-89.

[18] S.Arivazhagan, W.Sylvia Lilly Jebarani, and S.Bagavath (2011) “Colour Image Steganography Using Median Maintenance”, ICTACT Journal on Image and Video Processing, Vol. 2, Iss:01, pp.246-253.

[19] Shahana T (Volume 3, Issue 7, July 2013) An Enhanced Security Technique for Steganography Using DCT and RSA

[20] NageswaraRaoThota, Srinivasa Kumar Devireddy, “Image Compression Using Discrete Cosine Transform”, Georgian Electronic Scientific Journal: Computer Science and Telecommunications, No.3 (17), 2008. Encryption”, International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[21] Dr. EktaWalia, Payal Jain, Navdeep, “An Analysis of LSB & DCT based Steganography” ,Global Journal of Computer science & technology, Vol. 10 Issue 1 (Ver 1.0), April 2010.

[22] K.B.ShivaKumar,K.B.Raja, R.K.Chhotaray, Sabyasachi Pattnaik, “Coherent Steganography using Segmentation and DCT”,IEEE-978-1-4244-5967-4/10/$26.00 ©2010.

[23] Butt, Muheet Ahmed, and Majid Zaman. "Assessment Model based Data Warehouse: A Qualitative Approach." International Journal of Computer Applications 62.10 (2013).

[24] Zaman, Majid, and Muheet Ahmed Butt. "Enterprise Data Backup & Recovery: A Generic Approach." International Organization of Scientific Research Journal of Engineering (IOSRJEN) (2013): 2278-4721.

[25] Maqbool Rao, Nouman, et al. "Distributed Data Warehouse Architecture: An Efficient Priority Allocation Mechanism for Query Formulation."

[26] Butt, Muheet Ahmed. "Implementing ICT Practices of Effective Tourism Management: A Case Study." Journal of Global Research in Computer Science4.4 (2013): 192-194.

[27] Zaman, Majid, and Muheet Ahmed Butt. "Warehouse Creator: A Generic Enterprise Solution." International Journal of Engineering Science (IJES) 2.11.

[28] Butt, Muheet Ahmed. "COGNITIVE RADIO NETWORK: SECURITY ENHANCEMENTS." Journal of Global Research in Computer Science 4.2 (2013): 36-41.

[29] Butt, M. A., and M. Zaman. "Data Quality Tools for Data Warehousing: Enterprise Case Study." IOSR Journal of Engineering 3.1 (2013): 75-76.

[30] Butt, Er Muheet Ahmed, and Er Majid Zaman. "Data Quality Tools for Data Warehousing: Enterprise Case Study."

[31] Zaman, Majid, S. MK Quadri, and Muheet Ahmed Butt. "Generic Search Optimization for Heterogeneous Data Sources." International Journal of Computer Applications 44.5 (2012): 14-17.

[32] Butt, Muheet Ahmed. "COGNITIVE WAY OF CLASSIFYING DOCUMENTS: A PRACTITIONER APPROACH." Journal of Global Research in Computer Science 4.4 (2013): 108-111.

[33] Zaman, Majid, and Muheet Ahmed Butt. "Enterprise Data Backup & Recovery: A Generic Approach." International Organization of Scientific Research Journal of Engineering (IOSRJEN) (2013): 2278-4721.

[34] Butt, Muheet Ahmed. "Implementing ICT Practices of Effective Tourism Management: A Case Study." Journal of Global Research in Computer Science4.4 (2013): 192-194.

[35] Butt, Muheet Ahmed, and Majid Zaman. "Assessment Model based Data Warehouse: A Qualitative Approach." International Journal of Computer Applications 62.10 (2013).