ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

A Review on Steganography - Least Significant Bit Algorithm and Discrete Wavelet Transform Algorithm

Vanitha T [1], Anjalin D Souza[2], Rashmi B[3], Sweeta DSouza[4]

Department of Information Technology, ST Aloysius College, AIMIT Mangalore, India[1, 2, 3, 4]

ABSTRACT: The rapid development in the transfer of data through internet made it easier to transfer data accurate and faster to the destination. Security of information is one the important factors of information technology and communication. Steganography is art and science of invisible communication. Steganography is the method through which existence of the message can be kept secret. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. In this paper we are reviewing the two Steganography algorithms- Least Significant Bit and Discrete Wavelet Transformation.

KEYWORDS: LSB ( ), DWT ( ), MSE ( ), PSNR ( )

I. INTRODUCTION

Cryptography is a technique for securing the secrecy of communication. Many different encrypt and decrypt methods have been implemented to maintain the secrecy of the message. , it may also be necessary to keep the existence of the message secret. Steganography is the art and science of invisible communication of messages. It is done by hiding information in other information, i.e. hiding the existence of the communicated information. In image steganography the information is hidden in images. Today steganography is mostly used on computers with digital data being the carriers and networks being the high speed delivery channels. The difference between Steganography and Cryptography is that the cryptography focuses on keeping the message content secret whereas in steganography focus on keeping the existence of a message secret. Steganography and cryptography are the ways for protecting information from unwanted parties. Watermarking and fingerprinting are the other technologies that are closely related to steganography. They are mainly concerned with the protection of intellectual property. In watermarking all of the instances of an object are “marked”. The kind of information hidden in objects when using watermarking is usually a signature to signify origin or ownership for the purpose of copyright protection. On the other hand, different, unique marks are embedded in distinct copies of the carrier object that are supplied to different customers in fingerprinting. With this the intellectual property of owner to identify customers who break their licensing agreement by supplying the property to third parties. This paper reviews the LSB algorithm and DWT algorithm used for image steganography to illustrate the security potential of steganography for business and personal use.[1]

This paper reviews LSB and DWT Steganography algorithm techniques- its major types, introduction on LSB and DWT, Evaluation of Image quality and comparative analysis.

1.1 Types of Steganography:

The sender writes an innocuous message and then conceals a secret message on the same piece of paper. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. The data can be visible in basic formats like: Audio, Video, Text and Images etc. These forms of data are detectable by human hiding, and the ultimate solution was Steganography. The various types of steganography include:

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

a. Image Steganography:

The Image Steganography is technique in which we hide the data in an image so that ther will not be any change in the original image.

b. Audio Steganography:

Audio Steganography can be used to hide the information in an audio file. The audio file should be undetectable.

c. Video Steganography:

Video Steganography can be used to hide the information in video files. The video files should be undetectable by the attacker.

d. Text files Steganography:

Text Steganography is used to hide the information in text files. The general process of steganography i.e., preparing a stego object that will contain no change with that of original object is prepared but using text as a source.[2]

1.2. LSB (Least Significant bit embedding):

LSB technique is implemented in spatial domain. The technique converts image into shaded Gray Scale image. This image will be act as reference image to hide the text. Using this grey scale reference image any text can be hidden. Single character of a text can be represented by 8-bit. If the reference image and the data file are transmitted through network separately, we can achieve the effect of Steganography. Here the image is not at all distorted because said image is only used for referencing. Any huge amount of text material can be hidden using a very small image. Decipher the text is not possible intercepting the image or data file separately. So, it is more secure.

In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by “1”. So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by “3”. This helps in storing extra data. The Least Significant Bit (LSB) steganography is one such technique in which least significant bit of the image is replaced with data bit. As this method is vulnerable to stegano-analysis so as to make it more secure we encrypt the raw data before embedding it in the image. Though the encryption process increases the time complexity, but at the same time provides higher security also. This approach is very simple.

In this method the least significant bits of some or all of the bytes inside an image is replaced with a bits of the secret message. The LSB embedding approach has become the basis of many techniques that hide messages within multimedia carrier data. LSB embedding may even be applied in particular data domains - for example, embedding a hidden message into the color values of RGB bitmap data, or into the frequency coefficients of a JPEG image. LSB embedding can also be applied to a variety of data formats and types. Therefore, LSB embedding is one of the most important steganography techniques in use today. From one of our reference paper we found that in LSB steganography, to conceal the message the least significant bits of the cover media’s digital data are used. The useful feature of the LSB steganography techniques is LSB replacement that makes LSB stegnography as simple. To reflect the message it needs to be hidden, LSB replacement steganography flips the last bit of each of the data values. Consider an 8-bit gray scale bitmap image where each pixel is stored as a byte. And it also representing in a gray scale value. Suppose the first eight pixels of the original image have the following gray scale values: 11010010
01001010
10010111
10001100
00010101
01010111
00100110
01000011
The letter C whose binary value is 1000001. To hide this binary value it can replace the LSBs of these pixels to have the following new gray scale values:
11010011
01001010
10010110

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

10001100
00010100
01010110
00100111
01000011

On an average, only half the LSBs need to be changed. The difference between the cover (i.e. original) image and the stego image is difficult to observe by human eye. The major limitation of LSB is small size of data which can be embedded in such type of images using only LSB. The LSB is extremely vulnerable to attacks. The LSB technique which is implemented to 24 bit format is very difficult to detect contrary to the 8 bit format. Another example of LSB technique is: Considering a grid for 3 pixels which is having 24-bit image and the number 300 is to be embedded using LSB technique. The resulting grid is as follows:

PIXELS: (01010101 01011100 11011000)
(10110110 11111100 00110100)
(11011110 10110010 10110101)

C: 10000011
(01010101 01011100 11011000)
(10110110 11111100 00110100)
(1101111110110011 10110101)

In the above example the number C was embedded into the first 8 bytes of the grid and only the 2 bits need to be changed according to the embedded message .On an average, to hide a secret message using the maximum cover size, only half of the bits in an image will need to be modified.[3]

Algorithm to embed the text message[2]:-

Step 1: Read the cover image and the text message which is to be hidden in the cover image.
Step 2: Convert the text message in binary format.
Step 3: Calculate the LSB of each pixel of the cover image.
Step 4: Replace the cover image of the LSB with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Mean square Error (MSE) and the Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

1.3. Discrete Wavelet Transform:

Discrete Wavelet Transform technique is implemented in frequency domain. Discrete Wavelet transform (DWT) is a mathematical tool for decomposing an image hierarchically. It is used for processing of non-stationary signals. The transform is based on small waves, called wavelets, of varying frequency and limited duration. Wavelet transform provides the image frequency and spatial description. Temporal information is retained in this transformation process unlike conventional Fourier transform. Wavelets are created by translations and dilations of a fixed function called mother wavelet. The frequency domain transform applied in this research is Haar-DWT, the simplest DWT. A 2-dimensional Haar-DWT consists of two operations: One is the horizontal operation and the other one is the vertical. Detailed procedures of a 2-D Haar-DWT are described as follows:

Step 1: First, scan the pixels from left to right in a horizontal direction. And then, perform the addition and subtraction operations on the neighboring pixels. Store the sum on the left and the difference on the right as illustrated in Figure 1. Repeat the operation until all the rows are processed. The pixel sums represent the low frequency part (denoted as symbol L) while the pixel differences represent the high frequency part of the original image (denoted as symbol H).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

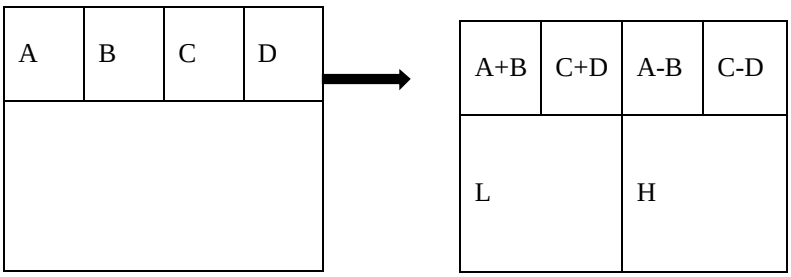

Figure1: The horizontal operation on first row

Step 2: Secondly, it will scan the pixels from top to bottom in vertical direction. It will also perform the addition and subtraction operations on neighboring pixels and then it stores the sum on the top and the difference on the bottom as illustrated in Figure 2. Repeat this operation until all the columns process is complete. Finally we will obtain 4 sub-bands denoted as LL, HL, LH, and HH respectively. The LL sub-band is the low frequency portion and it looks very similar to the original image. The whole procedure described is called the first-order 2-D Haar-DWT.[2]

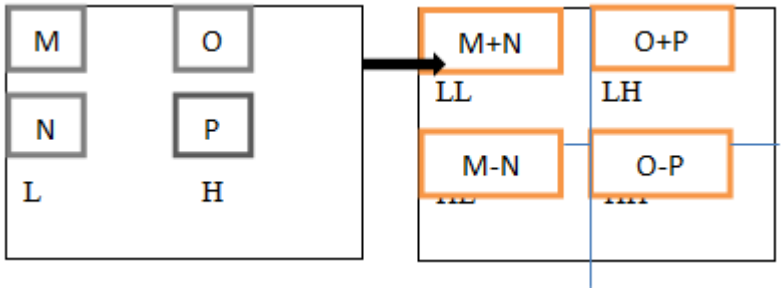

Figure 2: The vertical operation

Algorithm to retrieve the text message:-

Step 1: Read the cover image and text message that has to be hidden in the cover image.
Step 2: Convert the text message into binary. Apply 2D-Haar transform on the cover image.
Step 3: Obtain horizontal and vertical filtering coefficients of the cover image and the cover image is then added with data bits for DWT coefficients.
Step 4: Obtain stego image.
Step 5: Calculate the Mean square Error (MSE) and Peak signal to noise ratio (PSNR) of the stego image.

Algorithm to retrieve text message:-

Step 1: Read the stego image.
Step 2: Obtain horizontal and vertical filtering coefficients of the cover image and then extract the message bit by bit and recomposing the cover image.
Step 3: Convert the data into a message vector and then compare it with original message.[2]

2. Evaluation of Image Quality:

[2] For comparing the stego image with cover results it requires a measure of image quality and the commonly used measures are Mean-Squared Error, Peak Signal-to-Noise Ratio and capacity.

2.1 **Mean-Squared Error:**

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

$MSE = \sum[I1(m,n) - I2(M,N)]^2 \div M * N$

In the above formula M and N are the number of rows and columns in a input images, respectively.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

2.2 Peak Signal-to-Noise Ratio:

Peak Signal-to-Noise Ratio (PSNR) will help to avoid this problem by scaling the MSE according to the given image range: $PSNR = 10\log10\ (256^2 \div MSE\ )$

PSNR is measured in decibels (dB) and it is a good measure for comparing restoration results for the same image.

2.3 Capacity:

It is the size of the data in a cover image. The capacity can be modified without deteriorating the integrity of the cover image. In addition to the cover image perceptual quality a steganography embedding operation needs to preserve the statistical properties of the cover image and therefore capacity depends on the total number of bits per pixel and the number of bits embedded in each pixel of the image. Capacity is represented by bits per pixel (bpp). The Maximum Hiding Capacity (MHC) is represented by terms of percentage.

2.4 Comparative analysis of LSB and DWT steganography:

Comparative analysis of LSB based and DWT based steganography has been done on basis of the parameters like PSNR, MSE, Robustness and Capacity on the different images and the results are evaluated. Images are of best quality if PSNR ratio is high.[2]

(a) Jet (b) Baboon

LSB Substitution Technique:

Table : LSB Substitution Technique

Cover image	PSNR(dB)	MSE(dB)
Jet	52.7869	.58505
Baboon	53.7558	.52329

(a) Jet (b) Baboon

DWT Transform Technique:

Table: DWT transform technique

Cover image	PSNR(dB)	MSE(dB)
Jet	44.76	1.4741
Baboon	44.96	1.4405

Table: Parameter analysis of steganography Methods

Features	LSB	DWT
Invisibility	Low	High
Payload capacity	High	Low
Robustness against image manipulation	Low	High
PSNR	Medium	Low
MSE	Medium	High

III.LITERATURE SURVEY

In [1] authors give a brief idea about the image steganography that make use of Least Significant Bit (LSB) algorithm for hiding the data into image. The proposed approach provides higher security and can protect the message from stego attacks. The image resolution doesn't change much and is negligible when we embed the message into the image and

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

the image is protected with the personal password. So, it is not possible to damage the data by unauthorized personnel. The major limitation of the application is designed for bit map images (.bmp). It accepts only bit map images as a carrier file, and the compression depends on the document size as well as the carrier image size. In [2] authors used using Least Significant Bit (LSB) based Steganography, Discrete Cosine Transform (DCT) based Steganography and Discrete Wavelet Transform (DWT) based Steganography for hiding text in an image file. The LSB algorithm is implemented in spatial domain and the payload bits are embedded into the least significant bits of cover image to derive the stego-image. The DCT & DWT algorithm are implemented in frequency domain and the stego-image is transformed from spatial domain to the frequency domain and the payload bits are embedded into the frequency components of the cover image. The performance and comparison of these three algorithms are evaluated on the basis of the parameters MSE, PSNR, Capacity & Robustness. It is clear that the PSNR of DCT is high as compared to the other two algorithms. This implies that the DCT provides best quality of the image. An embedding algorithm is said to be ROBUST if embedded message can be extracted after the image has been manipulated without being destroyed. A DWT is a highly robust method in which the image is not destroyed on extracting the message hidden in it and it also provides the maximum security.

In [3] authors give an overview of different LSB methods. The implemented a new algorithm called EDGE LEAST SIGNIFICANT BIT EMBEDDING (ELSB). In ELSB, all the edge pixels in an image are used. First the masked image is calculated by masking the two LSB bits in the cover image. Then by identifying the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels,the data is hidden in the LSB bits of the edge pixels only and send the stego object to the receiver. At the receiver, the stego object is again masked at the two LSB bits [12]. Then the canny edge detector is used to identify the edge pixels. The same edge pixels at the sender and receiver are got since the same masked image to calculate the edge pixels are used. Thus the bits where data is hidden are identified. So the data is extracted from the two LSB bits of the identified edge pixels. Thus message is obtained. The least-significant-bit (LSB)-based approach is a popular type of steganographic algorithms in the spatial domain. In [4] authors explain about how the discrete wavelet transform method is used to embed the text message. When the DWT is applied 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, an image is taken as a cover object and another small image as secret message. In embedding process, first cover image is converted in wavelet domain. After the conversion manipulate high frequency component to keep secret image data. These secret image data further retrieved in extraction procedure to serve the purpose of steganography. In [5] authors explains about High Capacity and Security Steganography using Discrete wavelet transform algorithm is proposed. The cover and payload are normalized and the wavelet coefficient is obtained by applying discrete wavelet transform. The approximation band coefficient of payload and wavelet coefficient of cover image are fused based on strength parameters alpha and beta. The capacity of the proposed algorithm is increased as the only approximation band of payload is considered. The Entropy, MSE and Capacity are improved with acceptable PSNR compared to the existing algorithm. The author applies the two level wavelet transform as cover and payload. The payload wavelet coefficients are encrypted and fused with wavelet coefficients of cover image to generate stego coefficients based on the embedding strength parameters alpha and beta. In [6] author tells about the application of Wavelet Transform and Genetic Algorithm in a novel steganography scheme. A genetic algorithm based mapping function is employed to embed data in Discrete Wavelet Transform coefficients in 4x4 blocks on the cover image. The optimal pixel adjustment process is applied after embedding the message. The frequency domain is utilized to improve the robustness of steganography and, Genetic Algorithm is implemented and Optimal Pixel Adjustment Process to obtain an optimal mapping function to reduce the difference error between the cover and the stego-image, therefore improving the hiding capacity with low distortions. The result reveals that the novel scheme outperforms adaptive steganography technique based on wavelet transform in terms of peak signal to noise ratio and capacity, 39.94 dB and 50% respectively. In [7] authors have presented a comparative study of image steganography in the wavelet domain using four different embedding techniques, MSLB, LSB Varying Mode, Fusion Embedding and Threshold embedding. The embedding techniques used have their own applications and importance in terms of what characteristics of image steganography are desired. The authors have done the comparison of proposed algorithms through the imperceptibility measure, PSNR. It is found that Haar wavelet (i.e., IWT) is better option than bi-orthogonal cdf9/7 for the reversible thresholding technique as well as for others. The best choice for image steganography in wavelet domain is based on Fusion method

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol.2, Special Issue 5, October 2014

for color images. For gray image, LSB Varying mode method may be considered a better option as it provides a respectable capacity and satisfactory security along with good imperceptibility. In [8] authors have done a comparison of the DCT and DWT method. DCT and DWT algorithm are implemented in frequency domain in which the cover image is transformed from spatial domain to the frequency domain and the secret image is embedded into the frequency components of the cover image. The performance and comparison of these two techniques is evaluated on the basis of the parameters MSE, PSNR, processing time and capacity. Both the methods have good imperceptibility and also Robustness against statistical attacks. Result shown that decrypted secret image and stego image quality for DCT algorithm is better compared to DWT algorithms, while in the case of capacity and processing time, DWT are good compared to DCT.

IV. CONCLUSION

We have surveyed the two algorithms that are commonly used in the previous paper. From one of previous paper the evaluation done for image quality result states that the PSNR of LSB is high compared to DWT. That proves DWT is highly robust method compared to LSB because the image is not destroyed on extracting the message hidden in it and provides the maximum security. In future we are trying to implement and perform comparative analysis on LSB and DWT algorithm. Considering the parameters like PSNR, MSE, Robustness & Capacity on the different images and the results are evaluated to check best quality of Images having high PSNR ratio.

REFERENCES

[1] Mrs. Kavitha, Kavita Kadam, Ashwini Koshti, Priya Dunghav, “Steganography Using Least Signicant Bit Algorithm” International Journal of Engineering Research and Applications (IJERA)
[2] Stuti Goel,Arun Rana,Manpreet Kaur, “A Review of Comparison Techniques of Image Steganography” IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) , Volume 6, Issue 1 (May. - Jun. 2013), PP 41-48 www.iosrjournals.org
[3] M. Pavani1, S. Naganjaneyulu, C. Nagaraju, “A Survey on LSB Based Steganography Methods” International Journal Of Engineering And Computer Science ISSN:2319-7242
[4] Barnali Gupta Banik, Prof. Samir K. Bandyopadhyay, “A DWT Method for Image Steganography” International Journal of Advanced Research in Computer Science and Software Engineering
[5] H S Manjunatha Reddy, K B Raja, “HIGH CAPACITY AND SECURITY STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM”
[6] Elham Ghasemi, Jamshid Shanbehzadeh, Nima Fassihi, “High Capacity Image Steganography usingWavelet Transform and Genetic Algorithm”
[7] Sushil Kumar1, S.K.Muttoo, “A COMPARATIVE STUDY OF IMAGE STEGANOGRAPHY IN WAVELET DOMAIN” International Journal of Computer Science and Mobile Computing
[8]Jay Desai, Hemalatha S, Shishira SR, “Comparison between DCT and DWT Steganography Algorithms” International Journal of Advanced Information Science and Technology (IJAIST)
[9] *Edu Twin*. (n.d.). Retrieved from www.edutwin.com: http://edutwin.com/t-an-overview-of-image-steganography-full-report.
[10] *Scribd*. (n.d.). Retrieved from www.scribd.com: http://www.scribd.com/doc/52409986/Synopsis-Image-Steganography
[11] *citeseerx*. (n.d.). Retrieved from http://citeseerx.ist.psu.edu/: http://citeseerx.ist.psu.edu/showciting?cid=4344348