Text Security through Steganography using Discrete Wavelet Transform and Modified Least Significant Bit

Saurabh Singh[1], Prof. Satyarth Tiwari[2]
M. Tech. Scholar, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[1]
Guide, Department of Electronics and Communication, Bhabha Engineering Research Institute, Bhopal[2]

Abstract—"Steganography" is a procedure that defeats unapproved clients to approach the pivotal information, to invisibility and payload capacity using the different technique like discrete cosine transform (DCT) and discrete wavelet transform (DWT).The available methods till date result in good robustness but they are not independent of file format. The aim of this research work is to develop an independent of file format and secure hiding data scheme. The independent of file format and secure hiding data scheme in increased by combining DWT and modified least significant bits (LSB) technique. Accordingly an efficient scheme is developed here that are having better BER and PSNR against different characters.

Keywords— DWT, MLSB, BER, PSNR

I. INTRODUCTION

Since the beginning of life, people have been looking for safety in all areas of their lives from the natural dangers, human dangers or any danger they face. "Security" means the state of being safe and the measures adopted to ensure the safety. But security isn't a goal or an absolute thing to reach it because in spite of using many of the security procedures to protect something there is no 100 percent security [64]. Human beings have been developing, creating and using many safety procedures since ancient times to protect their lives. In the past, only things with physical presence needed protection and security; for example: a house was used to get protection against the harshness of nature, guards were used to protect places, and weapons were used to protect human beings, watchtowers, gates, moats, locks and other forms of protections. Security has three main parts: requirements, policy and mechanisms. Requirements define security procedures. They answer the question, "What do you expect security to do for you?" Policy defines the meaning of security. It answers the question, "What steps do you take to reach the goal set out above?" Mechanisms enforce policy. They answer the question, "What tools, procedures, and other ways do you use to ensure the security?" These components exist in all manifestations of security [1].

The use of the Internet is clearly growing daily, the number of the internet users is also increasing day by day, the total population of the world in January 2018 was 7.593 billion the internet users of the world was 4.021 billion; about 53 percent of the world have an access to the internet [2, 3]. Basically, Internet has become the primary medium to transfer data throughout the world, a lot of data and information are sensitive and need a security procedure to protect it whether during the transmission or in its place. Two primary methods are available to protect the data and information in transmission state or in place of permanent storage: Cryptography and Steganography, Cryptography is a technique used to change the characters form from the readable form to unreadable form, in this technique the intruder can know if there is cipher text or not because the characters are altered [4]. Steganography is a technique used to hide the characters or any media in other media, in this method the intruder cannot know if there is a cipher text or not because the characters are hidden in other media, so unauthorized user cannot see the characters because the characters are embedded in another media. Steganography is known as "invisible" communication [5], because it conceals a media in other media.

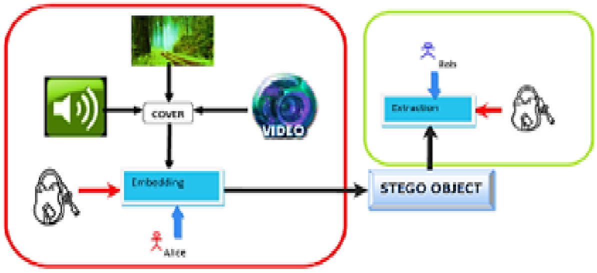


Figure 1: General schematic description

Steganography is a hiding media process over covered media and main objective is to communicate and transfer important information from one place to another in a safe secure and undetectable way. Literally meaning writing in a cover is the practice of hiding messages within other messages in order to conceal the existence of the original. Steganography indicates to the secret message or any digital media file which has been hidden inside another digital media file like image, text, video or audio file [6] [7]. Steganography is the process of hiding something inside something else without any doubt about the existence of the first thing. Steganography word is not new, it comes from the Greek word, "Stegos" that means covered or roof and "Graphia" that means writing. So, Steganography means "Covered Writing", The embedding process of the Steganography creates a stego media by changing the Least Significant Bits with data of the secret message bits [8].

II. PROPOSED METHODOLOGY

Cover-Image: An image in which the secret information is going to be hidden. The term "cover" is used to describe the original, innocent message, data, audio, still, video etc. The cover image is sometimes called as the "host".

Stego-Image: The medium in which the information is hidden. The "stego" data is the data containing both the cover image and the "embedded" information. Logically, the processing of hiding the secret information in the cover image is known as embedding.

Payload: The information which is to be concealed. The information to be hidden in the cover data is known as the "embedded" data.

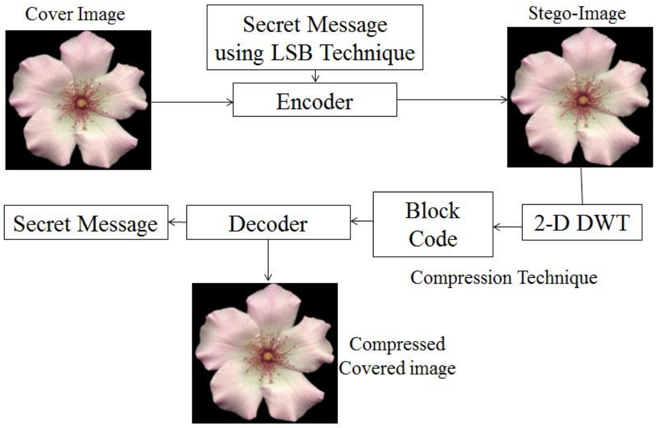


Figure 2: Flow Chart of Proposed Methodology

2.1 MLSB Technique

This technique works best when the file is longer than the message file and if image is grayscale.

When applying LSB technique to each byte of a 24 bit image, three bits can be encoded into each pixel.

If the LSB of the pixel value of cover image C(i, j) is equal to the message bit SM of secret message to be embedded C(i, j) remain unchanged; if not, set the LSB of C(i, j) to SM.

Message embedding procedure is given below:

S(i, j) = C(i, j)-1, if LSB (C(i, j)) = 1 and SM = 0
S(i, j) = C(i, j)+1, if LSB (C(i, j)) = 0 and SM = 1
S(i, j) = C(i, j), if LSB (C(i, j)) = SM

Where LSB (C(i, j)) stand for LSB of cover image C(i, j) and "SM" id the next message bit to be embedded. S(i, j) is the Stego image.

The proposed method follows a directional embedding technique for achieving maximum image quality in the stego image. The proposed method performs a selection of suitable direction for secret byte embedding so as to minimize the bit changes in the cover image when a secret data is embedded.

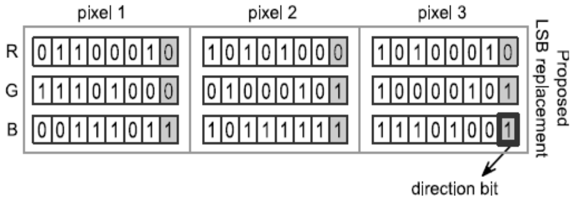

pixel 1
pixel 2
pixel 3
R 0 1 1 0 0 0 1 0 | 1 0 1 0 1 0 0 0 | 1 0 1 0 0 0 1 0
G 1 1 1 0 1 0 0 0 | 0 1 0 0 0 1 0 1 | 1 0 0 0 0 1 0 1
B 0 0 1 1 1 0 1 1 | 1 0 1 1 1 1 1 1 | 1 1 1 0 1 0 0 1
Proposed LSB replacement
direction bit

Figure 3: LSB embedding of the byte 11110000 in the cover image using the proposed method.

As you can see in Fig. 3, the byte 11110000 is embedded in a reverse order (00001111) in the original cover image for minimizing the number of alterations. Here also, we take three consecutive pixels (say $p1$, $p2$ and $p3$) for embedding a byte of information. Firstly, the red channels of $p1$, $p2$ and $p3$ are replaced with secret bits, followed by their green and blue channels. A direction bit is added at the 9-th bit which indicates that the preceding data is in stored in a reverse order. A value for the direction bit indicates a normal forward direction of storing data while a value 1 for the direction bit indicates that the data is stored in reverse direction. It can be noted that the number of bit changes required is 8 whereas in the proposed method shown in Fig. 3 requires no bit alterations. Instead of using only one directional bit per byte of secret data, we can also integrate more directional bits to indicate more directions of storing secret data within the cover image. However, this would decrease the embedding capacity of the cover image.

2.2 Discrete Wavelet Transform

The model used in [8] to implement the tree structure of Direct Wavelet Transform (DWT) is based on the filtering process. Figure 1 depicted a complete 2-level Direct WT. In this figure G and H is the high pass and low pass filter respectively.

Computation period is the number of the input cycles for one time produces output samples. In general, the computation period is M= for a j-level DWT. The period of the 2-level computation is 8. Figure 1, The Sub band Coding Algorithm As an example, suppose that the original signal X[n] has N- sample points, spanning a frequency band of zero to π rad/s. At the first decomposition level, the signal passed through the high pass and low pass filters, followed by subsampling by 2. The output of the high pass filter has N/2- sample points (hence half the time resolution) but it only spans the frequencies $\pi/2$ to π rad/s (hence double the frequency resolution) [9].

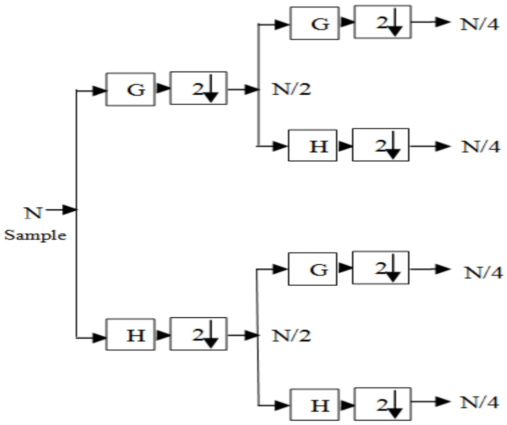


Figure 4: 2- Levels for DWT. Where G, H are the high-pass and low-pass filter coefficient

The output of the low-pass filer also has N/2- sample points, but it spans the other half of the frequency band, frequencies from 0 to $\pi/2$ rad/s. Again low and high-pass filter output passed through the same low pass and high pass filters for further decomposition. The output of the second low pass filter followed by sub sampling has N/4 samples spanning a frequency band of 0 to $\pi/4$ rad/s, and the output of the second high pass filter followed by sub sampling has N/4 samples spanning a frequency band of $\pi/4$ to $\pi/2$ rad/s. The second high pass filtered signal constitutes the second level of DWT coefficients. This signal has half the time resolution, but twice the frequency resolution of the first level signal. This process continues until two samples are left. For this specific example there would be 2 levels of decomposition, each having half the number of samples of the previous level.

The DWT of the original signal is then obtained by concatenating all coefficients starting from the last level of decomposition (remaining two samples, in this case). The DWT will then have the same number of coefficients as the original signal.

4.3 Block Code

Encoder part of the proposed technique shows that the original image is divided into three parts i.e. R component, G component and B component. Each R, G, B component of the image is divided into non overlapping block of equal size and threshold value for each block size is being calculated.

Threshold value means the average of the maximum value (max) of 'k × k' pixels block, minimum value (min) of 'k × k' pixels block and m_1 is the mean value of 'k × k' pixels block. Where k represents block size of the color image. So threshold value is:

$$T = \frac{\max + \min + m_1}{3} \tag{1}$$

Each threshold value is passing through the quantization block. Quantization is the process of mapping a set of input fractional values to a whole number. Suppose the fractional value is less than 0.5, then the quantization is replaced by previous whole number and if the fractional value is greater than 0.5, then the quantization is replaced by next whole number. Each quantization value is passing through the bit map block. Bit map means each block is represented by '0' and '1' bit map. If the Threshold value is less than or equal to the input image value then the pixel value of the image is represent by '0' and if the threshold value is greater than the input image value then the pixel value of the image is represented by '1'.

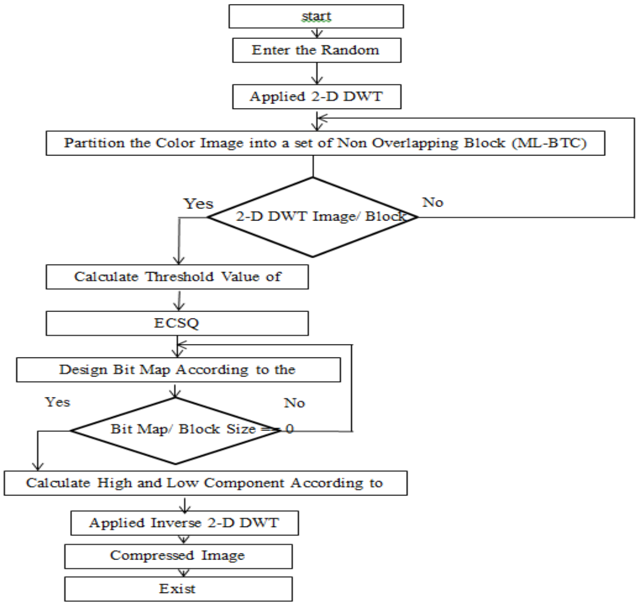

start
Enter the Random
Applied 2-D DWT
Partition the Color Image into a set of Non Overlapping Block (ML-BTC)
Yes
2-D DWT Image/ Block
No
Calculate Threshold Value of
ECSQ
Design Bit Map According to the
Yes
No
Bit Map/ Block Size == 0
Calculate High and Low Component According to
Applied Inverse 2-D DWT
Compressed Image
Exist

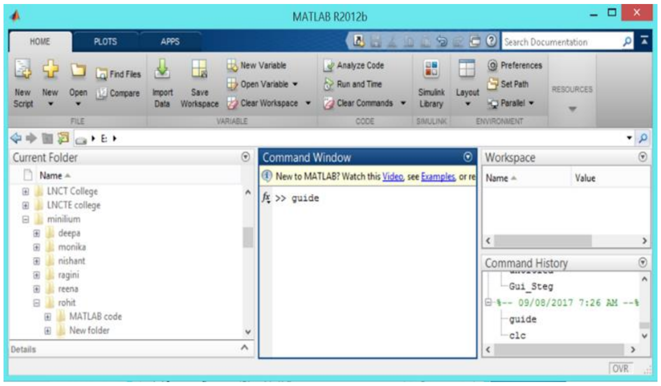
Figure 5: Flow Chart of Proposed Algorithm

III. SIMULATION RESULT

MATLAB (matrix laboratory) is a multi-paradigm numerical computing environment and fourth-generation programming language. A proprietary programming language developed by Math Works, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages.

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}[y(i,j) - x(i,j)]^2 \tag{2}$$

$$PSNR = 10\log_{10}(L*L/MSE) \tag{3}$$



New to MATLAB? Watch this Video, see Examples, or re

```
>> guide
```

```
Gui_Steg
%-- 09/08/2017 7:26 AM --%
guide
clc
```

Figure 6: Open the Graphical User Interface (GUI) Window

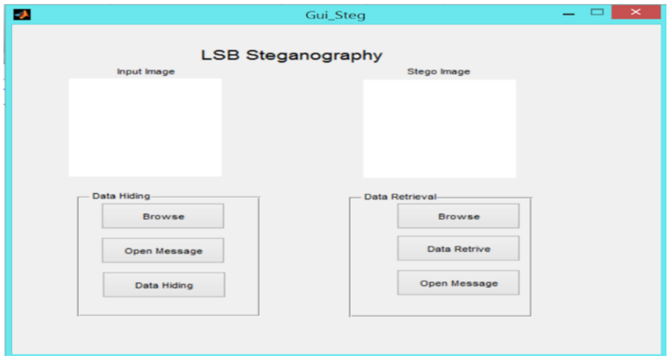
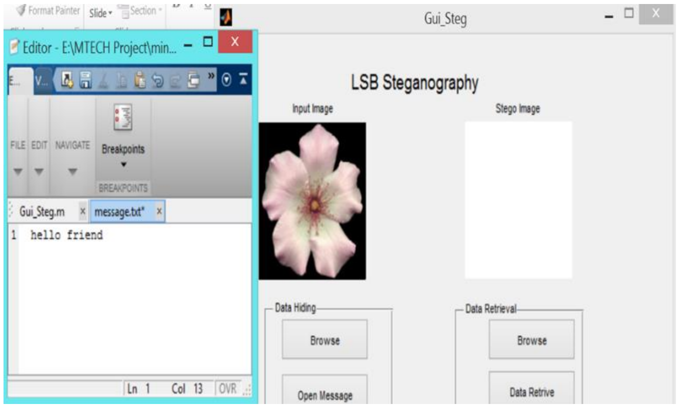
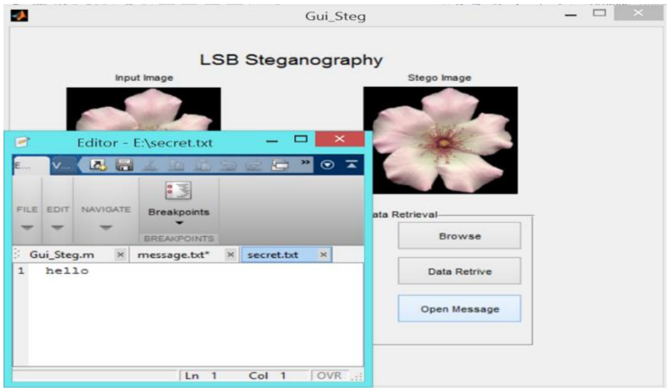


Figure 7: Window for LSB Steganography



```
1  hello friend
```

Figure 8: Window for Inter the Message



```
1  hello
```

Figure 9: Window for Output Message

Table 1: Result for Different Image with 50 Characters

Image	Image Type	Characters	Parameter	
			MSE	PSNR
Flower Image	.jpg	50	0.0017	52.34 dB
Lena Image	.jpg	50	0.0014	53.54 dB
Building Image	.jpg	50	0.0012	53.98 dB
Tiger Image	.jpg	50	0.0014	52.89 dB

Table 2: Result for Different Image with 200 Characters

Image	Image Type	Characters	Parameter	
			MSE	PSNR
Flower Image	.bmp	200	0.0081	46.55 dB
Lena Image	.bmp	200	0.0084	46.01 dB
Building Image	.bmp	200	0.0092	46.21 dB
Tiger Image	.bmp	200	0.0090	45.88 dB

IV. CONCLUSION

As compared with the traditional Least Significant Bit algorithm, the data hiding steganography method presented in this paper was found to be of increased imperceptibility to stego analysis attacks on the cover image. Therefore, this method is best suited for the purposes of communication applications. The recommended mode of transmission of stego images is through email attachments or web postings.

The results indicate that the proposed method performs well especially when embedding secret data at higher LSB bit positions. There are few methods that try to improve the quality of stego image by embedding secret data only in the channels of least importance. The proposed method can also be combined with those methods but it would naturally result in a reduction in the embedding capacity.

REFRENCES

[1] He Huang;Yinghui Xue;Linna Fan;Mo Li, "The Development and New Direction of Digital Image Stenography", International Conference on Robots & Intelligent System (ICRIS), IEEE 2020.

[2] Yıldıray Yiğit;Murat Karabatak, "A Stenography Application for Hiding Student Information into an Image", 7th International Symposium on Digital Forensics and Security (ISDFS), IEEE 2019.

[3] Nazir A. Loan, Nasir N. Hurrah, Shabir A. Parah, Jong Weon Lee, Javaid A. Sheikh, and G. Mohiuddin Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption", Received January 4,

2018, accepted February 7, 2018, date of publication March 16, 2018, date of current version April 25, 2018.

[4] Tomas Denemark, and Jessica Fridrich, "Steganography with Multiple JPEG Images of the Same Scene", IEEE Transactions on Information Forensics and Security, Volume: 12, Issue 10, 2017.

[5] Morteza Heidari, Nader Karimi, and Shadrokh Samavi, "A Hybrid DCT-SVD Based Image Watermarking Algorithm", Iranian Conference on Electrical Engineering (ICEE), IEEE 2016.

[6] N. Senthil Kumaran, and S. Abinaya, "Comparison Analysis of Digital Image Watermarking using DWT and LSB Technique", International Conference on Communication and Signal Processing, April 6-8, 2016, India

[7] Bidyut Jyoti Saha, Kunal Kumar Kabi and Arun, "Non Blind Watermarking Technique using Enhanced One Time Pad in DWT Domain", International Conference of Digital Signal and Processing, ICCCNT, IEEE 2014.

[8] Jiann-Shu Lee and Fei-Hsiang Huang, "A New Image Watermarking Scheme Using Non-dominated Sorting Genetic Algorithm II", International Symposium on Biometrics and Security Technologies, IEEE 2013.

[9] Teruya Minamoto and Ryuji Ohura, "A non-blind digital image watermarking method based on the dual-tree complex discrete wavelet transform and interval arithmetic", Ninth International Conference on Information Technology- New Generations, IEEE 2012.

[10] Baloshi Mathews and Madhu S. Nair, "Modified BTC Algorithm for Gray Scale Images using max-min Quantizer", Automation, Computing, Communication, Control and Compressed Sensing, PP. 01-05, 2013 IEEE.

[11] Wang Santosh, U. V. S. Sitarama Varma, K. S. K Chaitanya Varma, Meena Jami, V. V. N. S Dileep, "Absolute Moment Block Truncation Coding For Color Image Compression," International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-2, Issue-6, PP. 53-59, May 2013.

[12] Chen and K. V. Karthik, "A Modified Three Level Block Truncation Coding _or Image Compression", International Conference on Pattern Analysis and Intelligent Robotics, PP.31-35, June 2011 IEEE.

[13] Fan, Arpana Parakale, Bharamgonda Madhuri Mahavir, Bharamu Ullagaddi, "Image Compression using Absolute Moment Block Truncation Coding", International Conference on Pattern Analysis and Intelligent Robotics, PP.97-102, June 2011, Putrajaya, Malaysia.

[14] Bin and Hon-Hang Chang, "A Data Hiding Scheme for Color Image Using BTC Compression Technique," Proc. 9th IEEE International Conference on Cognitive Informatics, PP.845-850, 2010 IEEE.