# IMPLEMENTATION OF A NEW TECHNIQUE FOR SECURED IMAGE TRANSMISSION

S.Rathika1
[1]*Research Scholar, Department of Electronics and Communication Engg, Annamalai University, Chidambaram*

**ABSTRACT**

*Since the rise of usage of internet in the world security is becoming the major concern all over, developers are continuously working to make internet a safe environment for all the users. Many algorithm or techniques are proposed and they worked but as the intruders are acting smartly to hack information developers are also supposed to invent new techniques to stop hacker's intentions. As per the basic knowledge more is the PSNR value and lesser is the MSE results are better. So here, we are proposing a new method by combining two major security techniques that is cryptography and steganography that will not only hide the information and analysing different features by applying LSB and Integer Wavelet Transform (IWT) techniques to improvise the results for MSE, PSNR and Embedding capacity still after the noise attack, also with the obtained results the best efficient technique could be identified and enhanced in future.*

**Keyword :** - *Cryptography, Steganography, IWT, LSB, Data hiding, Watermarking, MATLAB*

## 1. INTRODUCTION

The purpose of this paper is to transmit the data securely. For that necessity we are obtaining the best efficient techniques could be combining Cryptography and Steganography (3). According to Cryptography process is original text is converted into watermarked image (1). At the same time in Steganography the image is changed into watermarked image. The result of combining Cryptography and Steganography will give the watermarked image which will contain the encrypted text image as well as cover image (2). Hence we propose a hiding technique using least significant bit Algorithm (LSB) and Integer Wavelet Transform (IWT).

## 2. LITERATURE SURVEY

In any of the image transmission process the privacy and security plays a major role as it can be misused easily in the internet. So to ensure security so many techniques has been implemented. Among them the most commonly used techniques are cryptography and steganography. Combining these techniques will provide higher order of security [1]. Steganography is the process of hiding an image which involves image compression whereas cryptography is the process hiding text. It involves encryption, decryption and key. Combining cryptography and steganography has more features such as robustness, efficiency and capacity [2]. For data transfer digital communication is efficient in all the ways. Security and integrity of data is the major requirement. The comparative study of Steganography, Cryptography and watermarking gives a clear idea on the advantages in the three major techniques [3]. In this study a new encryption method is applied using Least Significant Bit algorithm. By doing this the unauthorized user cannot use stegnalysis to recover the data [4].The Steganography technique is used to conceal the existence of hidden secret data inside a cover object. Images are the most popular cover objects embedding secret information inside images. The spatial domain techniques manipulate the cover-image pixel bit values to embed the secret information. The secret bits are written directly to the cover image pixel bytes. The Least Significant Bit (LSB) is

one of the main techniques in spatial domain image steganography [5]. Steganography attempts to hide the secret information into the image and make communication undetectable. Stenographic method use integer wavelet transform (IWT) for increasing hiding capacity and imperceptibility [6].

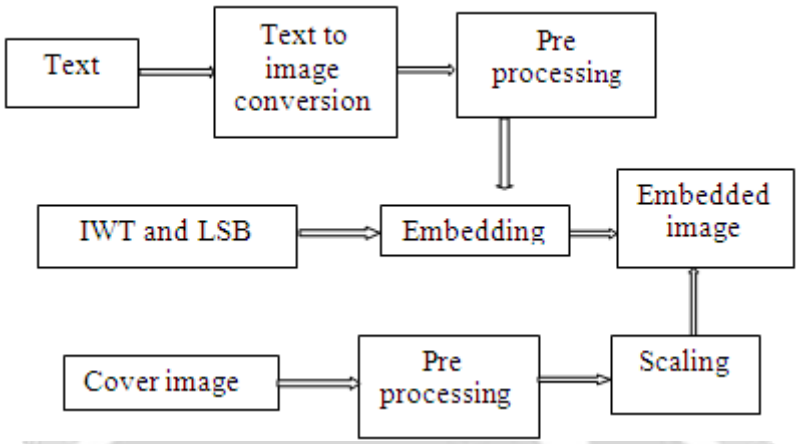


**Fig -1**: **Embedding process**

Initially the text is given as the input then the text is converted to an image. It involves the pre-processing step that means unwanted distortions are removed there. At the same time cover image also involves the pre-processing step, and then the cover image is resized according to the text size. Because then only the text will be hide into the image. Finally the embedding is done by both IWT and LSB algorithms, in LSB colour planes are separated then the secrete text is hide into the last bit of the image then only the hacker will not identify the original text, it's looks like the same image. In IWT split, compression, update steps are involved at last the embedding image is involved the extraction process.

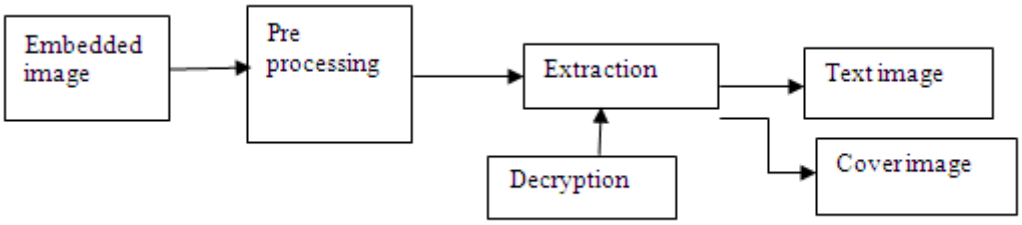


**Fig2. Extraction process**

The extraction process is exactly reverse of the embedding, initially the unwanted signals again added to the original image, cover image and the original text will be separated by Inverse Integer Wavelet Transform (IIWT), and LSB algorithms. Here the LSB remove the secrete text from the image and is used to add the colour planes to the original image, finally the text and image are separated. In IIWT update, compression, split steps are involved in order to perform the extraction process to get the original image as well as user data.

## 3. EMBEDDING PROCESS

Firstly the text is hiding into the image. Then the image is converted into the invisible watermarking. Before converted into the invisible watermarking each color planes separate by IWT. The embedding process is used to

stores (N) message bits in the least significant bits. So LSB also take place in embedding side. Embedding side the secret message is converted into a bit stream sequence. When IWT is applied to the cover image, it will split the each color plane separately. The embedding process is used to stores (N) message bits in the least significant bits of the IWT coefficients of the cover image. Then the pseudorandom permutation is applied to arrange the coefficients in an order.

## 4. EXTRACTING PROCESS

Extraction is reverse process of the embedding process. In this process Inverse IWT algorithm is applied on each color plane of the embedded image. The bit sequence is extracted by applying permutation scheme. The embedded coefficients are selecting, till extracting the embedded message bits from the LSB's of the integer coefficients. Further the extracted bits are converted into the original message. That is shown in fig2.

## 5. ALGORITHMS

Basically this paper contains two algorithms.

1. LSB (Least Significant Bit)
2. IWT (Integer Wavelet Transform)

In both embedding as well as extracting process contains IWT and LSB algorithms for increase the capacity and robustness of the data.

## 5.1 LSB ALGORITHM

The LSB algorithm is taken place embedding process as well as the extracting process. When the LSB algorithm is apply to the right most position of the image bit sequence, it will not affect the quality of the original image. That means the embedded image is looks like the cover image (5).The LSB is used to increase the capacity of the image. The position of the LSB is not dependent upon the transmitted bit position. To hide the data into an image all of the bytes inside an image is changed into bit of the message by applying the LSB algorithm. Basically the image is separated under two types of bits one is 24 bit the other one is 8 bit.
For 24 bit image three bits of information in each pixel is hidden, for 8 bit image only one bit of information in each pixel is hidden(4).

### 1. PIXEL PROCESSING

The information which we want to hide is converted into a secret code and then encryption is done. After this step we have to embed the data in the image. For this process we are using the least significant bit algorithm. The LSB is used for data embedding because,
1. The intensity of the image after which data hiding is done will not change that much when compared to the original image.
2. For example
1111100**0** **1**11111001
The change is only one bit so that the intensity of image is not affected too much and we can easily transfer the data.

**Steps To Insert Data In Image:-**

1.) The pixel values of the input image are calculated. Find out the pixel values.
2.) Selecting a particular pixel in which the data is inserted.
The user can choose the pixels in which he wants to insert data. It can be continuous or alternate. The distance can be kept fixed or it may vary according to user's convenience.
For example, consider a grid for 3 pixels of a 24-bit image.
00111101001111100111111**0**
10110110110011000010110**0**

1100001**0**1011110**1**01100001**1**

1.) At first the number is converted into a binary representation.

2.) Then the secret message is embedded in the least significant bit of the image so that the output image resembles the original image and it will be less sensitive to the visual system.

### 5.2 INTEGER WAVELET TRANSFORM

In Integer wavelet transform the data will be hidden in these regions HL, LH, HH. These regions are known as high resolution detail bands (5). When the data is embedded in these regions the original message will have less distortion and also we can increase the robustness. Consider, we are transforming a signal SI, and then the wavelet transform will separate the low frequency component SI-1 and the high frequency coefficients DI-1 as odd and even signals. The integer wavelet transform performs three steps. They are as follows, 1. Split 2. Compression and 3. Update (6).

**1) Split step**

It is also known as "Lazy Wavelet" transform. It splits the signal SI into two new signals which is even SI-1 and odd SI-1 subsets.

**2) Compression Step**

This step computes a prediction for odd samples based on even samples or vice versa. By doing this, the subset DI-1 can be predicted efficiently from subset SI-1. This prediction is subtracted from the odd samples creating an error signal which is known as prediction error. Once the prediction is made, the signal SI can be replaced by subset SI-1 and prediction error between the predicted di-1 and the real values of DI-1 obtained from the split.

**3) Update Step**

With the prediction values now we are enhancing the subset SI-1 in this step. This process is necessary because some of the properties of the subset SI-1 do not match with the properties of the original signal transmitted as some of the energy will be lost during sub sampling. This step will rectify the low frequency components which are missing at the receiver end.

On doing this steps the result obtained will be low pass coefficients SI-1 and high pass coefficients DI-1. The wavelet transform used is HAAR wavelet transform. HAAR wavelet transform is also known as the S integer wavelet transform. At the receiver side inverse lazy wavelet transform is performed for extracting the secret message from the cover image. At the user end it will compile the update step at the first place and then the results are added to the even samples. By doing this it is possible to generate the prediction values exactly and then the prediction values are added to the odd samples. We are inverting the lazy wavelet transform so that we can recover the original signal transmitted (6)

## 6.CONCLUSION

This paper provides an overview of cryptography and steganography techniques using Least Significant Bits (LSB) and Integer Wavelet Transform (IWT) algorithms. Even though both these methods provide security we are combining cryptography and steganography together to achieve higher levels of security (3). LSB is a simple technique which helps to embed the secret message in to an image. The last bit in a pixel is used to conceal the message. For data hiding not only image is used, it includes letters, symbols and numbers. Similarly in Integer wavelet transform we are hiding the data in high resolution detail bands. Though the transform does not make use of dilation and translation like the regular wavelet transform it is able to keep the multi resolution properties of the wavelet transform. The proposed system will provide more security when compared to any other existing systems. The hidden information will be protected along with high embedding capacity. The distortion of the original image will be less due to the lossless compression. It allows us to increase the robustness and efficiency. In future for data hiding not only image is used, it includes letters, symbols and numbers also for increase the security and robustness.

## 7. REFERENCES

[1] Pooja Rani, Apoorva Arora, (2015), Image Security System using Encryption and Steganography: International Journal of Innovative Research in Science,Engineering and Technology, vol. 4, no. 6.

[2] Md. Khalid Imam Rahmani, Kamiya Arora , Naina Pal, (2014), A Crypto-Steganography: A Survey: International Journal of Advanced Computer Science and Applications, vol. 5, no. 7.

[3] Hardikkumar, V. Desai, (2012), Steganography, Cryptography, Watermarking: A Comparative Study: Journal of Global Research in Computer Science, vol. 3, no. 12.

[4] Mr . Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar (2012), Image Security System using Encryption and Steganography: of Global Research in Computer Science, vol. 3, no. 3.

[5] Champakamala .B.S, Padmini. K, Radhika .D. K, Least Significant Bit algorithm for image steganography: International Journal of Advanced Computer Technology (IJACT), vol. 3, no. 4.

[6] Jayasudha, (2013), Integer Wavelet Transform Based Steganographic Method Using OPA Algorithm: International Journal Of Engineering And Science, vol. 2, no. 4, Pp.31-35.

[7] Pooja Rani, Apoorva Arora, (2015), Image Security System using Encryption and Steganography: International Journal of Innovative Research in Science,Engineering and Technology, vol. 4, no. 6.

[8] Mohamed M. Fouad, (2015), A Lossless Image Compression Using Integer Wavelet Transform with a Simplified Median-edge Detector Algorithm: International Journal of Engineering & Technology IJET-IJENS, vol. 15, no. 4.