



COMPARISON OF LSB AND DWT STEGANOGRAPHY TECHNIQUES

Syed Mujtiba Hussain¹, Salihah Yousu¹, Syed Bisma¹, Mehvish Siddiqi¹, ZahidGulzar Khaki²

¹Department of Computer Science and Engineering, Islamic University of Science and Technology.

²Department of Electronics and Communication Engineering, Islamic University of Science and Technology

ABSTRACT: *Steganography is the art and science of hiding communication; in steganography we embed data in a cover medium such that this information is not vulnerable to suspicion. In this paper we attempt to compare the two techniques of steganography LSB and DWT and make comparisons on the basis of two parameters Statistical Parameters and Image Quality Parameters. We found that DWT provides low embedding capacity with respect to LSB, which provides more embedding capacity. And the quality of the image is maintained in LSB than DWT.*

Keywords: *Steganography, LSB, DWT, stego-image, PSNR, discrete wavelet transform, Least significant bit.*

I. INTRODUCTION

We live in times of secrecy and espionage, where the security of communication is of prime importance. This is the major reason why steganography has gained significance. Steganography is derived from two Greek words stegos meaning secret and graphic meaning writing. Steganography is the art of hiding information in a cover such that this message is impercievable [1, 2, 3] Steganography has started its journey from a humble 'shaved head method' to highly efficient techniques. It derives its roots from data hiding .steganography is implemented both in spatial domain as well as in frequency domain. In this paper we are choosing one technique from both the domains, namely LSB and DWT respectively. Least Significant bit insertion is the most commonly used approach .In LSB we embed data in a cover by altering the least significant bits in the pixel.this technique is easy to implement but is vulnerable to even small cover modifications. In DWT technique we embed information by changing the cover to frequency domain and then altering certain frequency coefficients.This technique provides more security.

II. LSB TECHNIQUE

Least significant bit (LSB) [6] insertion is a common, simple approach to embedding information in a cover image. For instance, a simple scheme proposed, is to place the embedding data at the least significant bit (LSB) of each pixel in the cover image . The altered image is called stego-image. Altering LSB doesn't change the quality of image to human perception but this scheme is sensitive a variety of image processing attacks like compression, cropping etc [4].

➤ PROPOSED ALGORITHM

Embedding Algorithm:

Input: cover image, key, secret message

Procedure:

Step1: Take a gray scale image(8-bit).

Step2: Convert the secret message into bit stream.

Step3: Now generate the sequence of indices for bit insertion. Here odd bits of the stream is embedded in IJth location and the even bit is embedded in JIth location. We increase IJ by some stepsize and proceed respectively

Step4: While complete bit stream not embedded

{ Reduce the value of stepsize by some constant value and replace least significant bit of pixel at IJth location. }End.

Output: Stego-Image.

On the receiver side extraction of this secret message is performed. The receiver has the knowledge about the key and the length of the secret message.

Extraction Algorithm:

Input: stego-image, key

Procedure:

Step1: Take the stego-image

Step2: Calculate the pixel positions in the same way as in the embedding algorithm by using the same key.

Step3: Form the secret bit stream by the LSB's of these pixels.

Step4: Convert this bit stream into the corresponding ASCII value by using 8-bit conversion.

End

Output: Secret-Message