Scientific Journal of Impact Factor (SJIF): 4.72

e-ISSN (O): 2348-4470
p-ISSN (P): 2348-6406

International Journal of Advance Engineering and Research Development

Emerging Trends and Innovations in Electronics and Communication Engineering - ETIECE-2017

Volume 5, Special Issue 01, Jan.-2018 (UGC Approved)

Analysis of LSB and DWT Steganography Techniques over Various Attacks

Syed Mujtiba Hussain[1], Salihah Yousu[1], Syed Bisma[1], Mehvish Siddiqi[1], ZahidGulzar Khaki[2]

[1]*Department of Computer Science and Engineering, Islamic University of Science and Technology.*
[2]*Department of Electronics and Communication Engineering, Islamic University of Science and Technology.*

ABSTRACT: *Due to phenomenal increase in the concern about security and confidentiality of information over the internet, various techniques have been proposed. Steganography is one such technique. It's a form of security from obscurity. a Steganography is a technique of hiding one piece of information into another. In this paper we make comparisons between two steganography techniques one from spatial domain (LSB) and other from frequency domain (DWT) on the basis of various attacks. No doubt LSB provides high PSNR and good image quality but it's not so robust to attacks. Full retrieval of data is not possible after attacks. On the other hand DWT is more robust to attacks.*

Keywords*: steganography, LSB, DWT, stego-image, discrete wavelet transform, least significant bit*

I. INTRODUCTION

The 21st century has brought with it the dawn of assailability. Whenever we communicate via a medium the security of our message becomes an inevitable concern. Steganography provides us with data hiding capabilities. Steganography can be viewed as kin of cryptography .No one apart from sender and recipient suspects the existence of the message in steganographic techniques. In this paper we are analysing LSB and DWT technique for data security applications [1]. LSB technique is the most basic spatial domain method in image steganography, where a message is embedded in the insignificant bits of a cover. On the contrary DWT is a frequency domain method where data is embedded by altering the frequency coefficients. Transform domain methods embed messages in significant area of cover image which makes them robust against various operations and attacks like cropping, rotation and image compression. Thus DWT provides a very secure way of communicating confidential data through an unsecure medium. Though LSB provides better embedding capacity but it is prone to even small cover modifications.

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 IJthlocation 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.

