Secured Double Layer Data Hiding Using Encryption and Decryption Techniques

H. Mahesh Kumar
M. Vignesh

Abstract—In this period of Internet every digitized object is transferable and exchangeable over internet for various purposes. As every computer user knows that there are numerous security threats for digitized objects hence methods like steganography are getting more importance every day. On the other hand steganography is a very old method of hiding information behind some object, but quite this is very effective for shield data transfer and data exchange. Today this method is used for digital objects like script, audiovisual and pictures. In this paper a method for image steganography has been discussed, utilizing basics of discrete wavelet transform.

Index Terms—DWT, MSE, PSNR, Fourier Transform

I. INTRODUCTION

A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is right as it host local analysis and multi-resolution analysis. To analyze a signal at distinct frequencies with different resolutions is called multi-resolution analysis (MRA).

Wavelet analysis can be of two types: continuous and discrete. Here, discrete wavelet transform technique has been used for image steganography. This technique transforms the object in wavelet domain, steps the coefficients and then performs inverse wavelet transform to represent the original format of the stego object.

II. PROPOSED METHOD

Wavelet transforms converts spatial domain information to frequency domain information. The Fourier transformed signal \( X_{FT}(f) \) gives the global frequency distribution of the time signal \( x(t) \). The original signal can be reconstructed using the inverse fourier transform.

\[
X_{FT}(F) = \int_{-\infty}^{\infty} x(t) e^{-j2\pi ft} dt
\]

\[
x(t) = \int_{-\infty}^{\infty} X_{FT}(f) e^{-j2\pi ft} dt
\]

Before wavelet transform, most well known method for this purpose was Fourier transform (FT). Limitations of FT have been overcome in Short Time Fourier Transform (STFT) which is able to retrieve both frequency and time information from a signal. In STFT along with FT concept, a windowing concept is exhausted. Here FT is applied over a windowed part of the signal and then moves the window over the signal.

\[
X_{STFT}(\tau, f) = \int_{-\infty}^{\infty} x(t) g^*(t - \tau) e^{-j2\pi ft} dt
\]

The advantage of wavelet transform over Fourier is narrow analysis. That means wavelet analysis can leak signal aspects like discontinuities, disintegrate points etc.

Human eyes are less sensitive to high frequency details. Here the Haar DWT - simplest type of DWT has been used. In 1D-DWT average of fine details in small area is recorded. In case of 2D-DWT first perform one step of the
transform on all rows. The left sides of the matrix covered down sampled low pass coefficients of each row; the right side contains the high pass coefficients as shown in the fig.1.

Fig.1. First stage of step 1 wavelet decomposition

Next, apply one step to completely all columns. This result in four types of factors: LL, HL, LH, HH as follows (fig.2.):

Fig.2. Final stage of step 1 wavelet decomposition

Fig.3. Block diagram of 1 step 2-D DWT
III. EMBEDDING PROCEDURE

In this step, insertion of secret message onto cover object is carried out. Additional components rather than usual steganographic objects used here is pseudo-random number. Pseudo-random sequences typically exhibit statistical randomness while being generated by an entirely deterministic causal process generator. A pseudo-random number generator is a program that on input a seed generates a seemingly random sequence of numbers.

![Block diagram of secret message embedding procedure of steganography](image)

ENCODING:
Steps-
1. Read the cover image.
2. Read secret image and convert it in binary.
3. Calculate LSB of each pixels of cover image.
4. Apply LSB replacement method to replace LSB of cover image with each bit of secret image.
5. Apply DWT
6. Write stego image.

DECODING:
Input: An m × n carrier image and an m × n stego-image.
Output: A secret message/image.
Steps-
1. Take stego image.
2. stego color image is decomposed into three colors planes.
3. Calculate LSB for each pixels of stego-image.
4. Retrieve bits and convert each bit into secret message/image.
5. Apply IDWT
6. Original hidden data.
7. Compute PSNR.

In this section some experiments have been carried out to prove the relationship between expected results and actual results of proposed methods. The proposed two algorithms have been simulated with MATLAB. Images of size 512 × 512 have been used as the carrier or cover object and another image of size 100 × 100 have been used as message object. After the embedding procedure, the resultant object i.e. the stego object is quiet good in quality with respect to visibility. In extraction procedure it has been aimed to extract the original message intact which has been executed successfully by the above mentioned extraction algorithm.

After implementations of this technique just have a look on the histogram of both the images cover image and...
stego image respectively and find both are very different from each other.

The following figures show the histogram of cover image and stego image.

![Fig.5.Histogram of Input Image](image1)

![Fig.6.Histogram of watermark Image](image2)

The above figure shows the histogram of cover image and the histogram of Stego Image. Both the images are different from each other.

A. Mean Squared Error (MSE)

The described as a signal fidelity measure, the goal of a signal fidelity measure is to compare two signals by providing a quantitative score that describes the degree of similarity / fidelity or, conversely, the level of error/distortion between them suppose that \( x = \{x_i | i = 1, 2, \ldots, N \} \) and \( y = \{y_i | i = 1, 2, \ldots, N \} \) are two finite-length, discrete signals like images, where \( N \) is the number of signal samples (pixels, if the signals are images) and \( x_i \) and \( y_i \) are the values of the \( i^{th} \) samples in \( x \) and \( y \), respectively. The MSE between the signals is given as

\[
MSE(x, y) = \frac{1}{N} \sum_{i=1}^{N} (x_i - y_i)
\]

For the steganographic purpose, \( x \) is cover image and \( y \) is message to be hidden. Hence it will be referred to as error signal, a difference between original image and its watermarked version.

B. Peak Signal to Noise Ratio (PSNR)

For image processing specifically, MSE is converted into PSNR as follows:

\[
PSNR = 10 \log_{10} \frac{L^2}{MSE}
\]

Where \( L \) is the dynamic range of allowable image pixel intensities, calculated as follows:
$L = 2^n - 1$

Where $n$ is number of allocated bits/pixel. The PSNR is used to evaluate the quality of stego image. For an $M \times N$ grayscale image,

$$PSNR = 10 \log_{10} \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M} \sum_{j=1}^{N} (p_{i,j} - q_{i,j})^2}$$

IV. SIMULATION RESULTS

A. ENCODING PHASE AND DECODING PHASE

![Cover Image](image1)

Fig. 7. Cover Image

![Watermarked Image](image2)

Fig. 8. Secret Image
Fig. 9. Watermarked Image

Fig. 10. Extracted Secret Image
V. CONCLUSION

The Steganography is the art and science of inditing obnubilated messages in such a way that no one, apart from sender and intended recipient, suspects the esse of message, form of security. In this paper analysis of LSB method has been prosperously implemented & results are delivered. From the result it is clearly shows that PSNR value of the image is high.

REFERENCES


TABLE I: PSNR Value for Different Images

<table>
<thead>
<tr>
<th>S.No</th>
<th>Image name</th>
<th>Size in Bytes</th>
<th>PSNR(dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cover image</td>
<td>37000</td>
<td>44.800</td>
</tr>
<tr>
<td>2</td>
<td>Secret Image</td>
<td>30000</td>
<td>46.380</td>
</tr>
<tr>
<td>3</td>
<td>Watermarked image</td>
<td>34800</td>
<td>42.470</td>
</tr>
<tr>
<td>4</td>
<td>Extracted image</td>
<td>25000</td>
<td>49.058</td>
</tr>
</tbody>
</table>

S.No  Image name          Size in Bytes  PSNR(dB)
01 C 0ver image          37000         44.800
02 S ecret Image         30000         46.380
03 W atermarked image    34800         42.470
04 E xtracted image       25000         49.058