Secured Double Layer Data Hiding Using Encryption and Decryption Techniques

H.MaheshKumar

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.

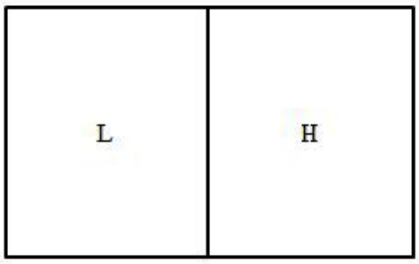
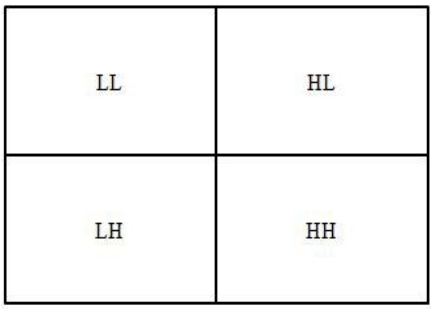


Fig.1. First stage of step 1 wavelet decomposition

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



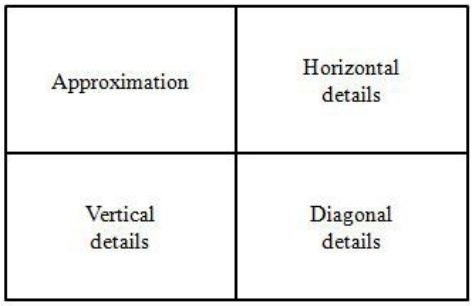


Fig.2. Final stage of step 1 wavelet decomposition

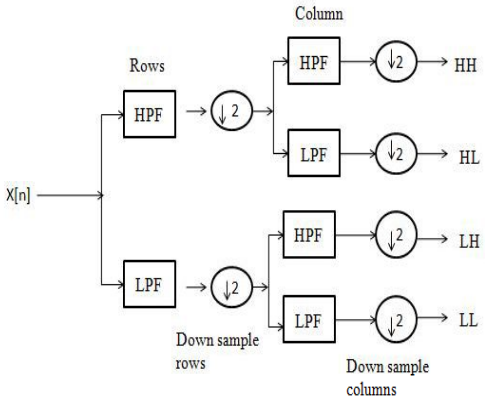


Fig.3. Block diagram of 1 step 2-D DWT

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.

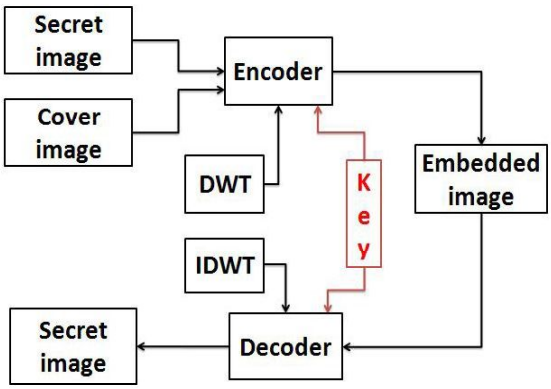


Fig.4. Block diagram of secret message embedding procedure of steganography

ENCODING:

Steps-

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

DECODING:

Input: An m × n carrier image and an m × n stego-image.

Output: A secret message/image.

Steps-

Step 1: Take stego image.
Step 2: stego color image is decomposed into three colors planes.
Step 3: Calculate LSB for each pixels of stego-image.
Step 4: Retrieve bits and convert each bit into secret message/image.
Step 5: Apply IDWT
Step 6: Original hidden data.
Step 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 x 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

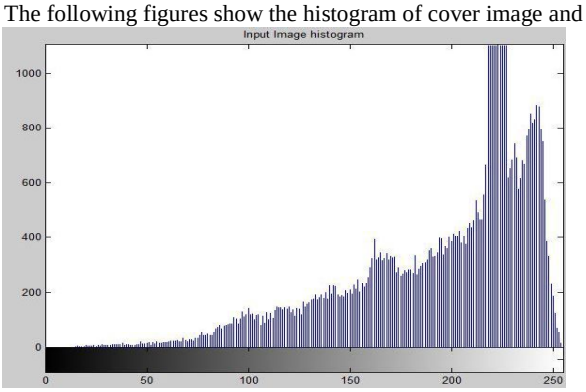


Fig.5.Histogram of Input Image

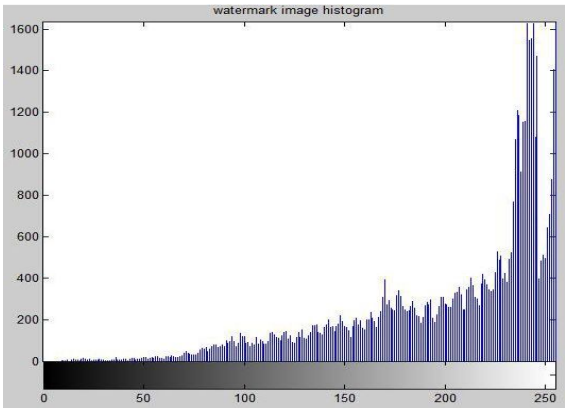


Fig.6.Histogram of watermark Image

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

$$MSE(x, y) = \frac{1}{N}\sum_{i=1}^{N}(xi - yi)$$

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 x N grayscale image,

$$PSNR = 10\log 10 \frac{255 \times 255 \times M \times N}{\sum_{i=1}^{M}\sum_{j=1}^{N}(pi, j - qi' j)^2} db$$

IV. SIMULATION RESULTS

A. ENCODING PHASE AND DECODING PHASE

Fig.7. Cover Image

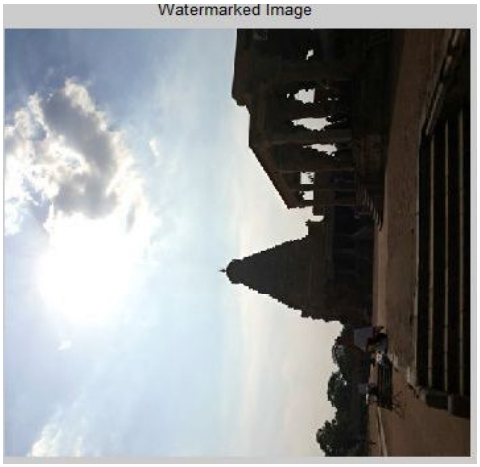


Fig.8. Secret Image

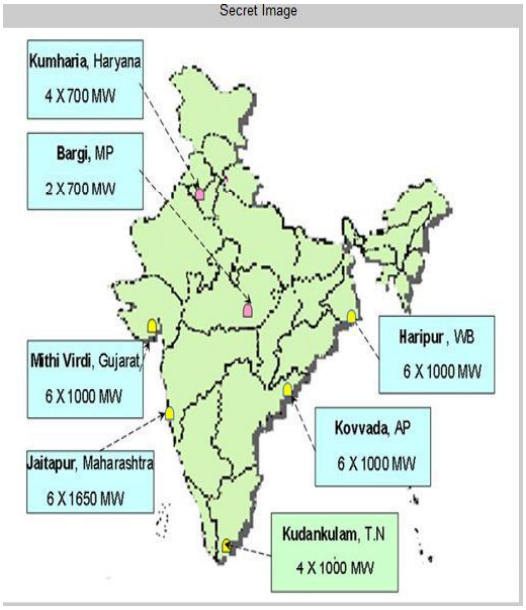


Fig.9. Watermarked Image

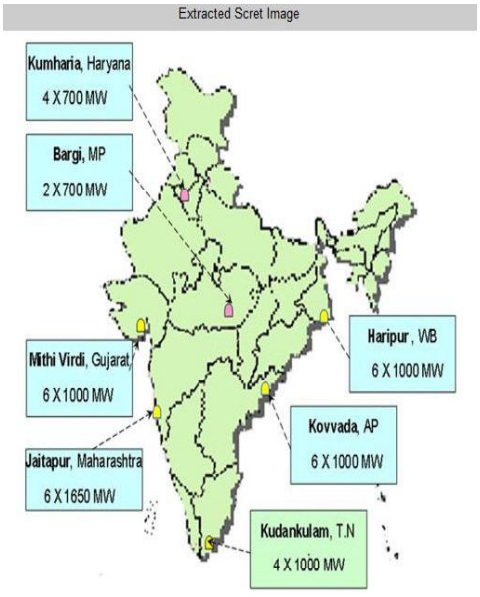


Fig.10. Extracted Secret Image

TABLE I: Psnr Value for Different Images

S.No	Image name	Size in Bytes	PSNR(dB)
1	Cover image	37000	44.800
2	Secret Image	30000	46.380
3	Watermarked image	34800	42.470
4	Extracted image	25000	49.058

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

[1] Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt (2010),' Digital image steganography: Survey and analysis of current methods', Elsevier Signal Processing, pp. 727-752.

[2] Abdul-mahdi N.H, Yahya A, Ahmad R.B and Al-Qershi O.M (2013),' Secured and robust information hiding scheme', Elsevier, pp. 463-471.

[3] Biswas D, Biswas S, Majumder A, Sarkar D, Sinha D, Chowdhury A, Das S.K (2012), 'Digital image steganography using dithering technique', Elsevier, pp. 251-255.

[4] Chin-chen chang, Min-hui lin, Yu-chen hu (2002),' A fast and secure image hiding scheme based on lsb substitution', international journal of pattern recognition and artificial intelligence, Vol. 16, no. 4,pp. 399-416.

[5] Fridrich J, Goljan M, Du R(2001), 'Detecting LSB steganography in color and gray-scale images', IEEE MultiMedia, Vol. 8, no. 4, pp. 22– 28.

[6] Li Fan , Tiegang Gao , Qunting Yang , Yanjun Cao (2011), 'An extended matrix encoding algorithm for steganography of high embedding efficiency', Elsevier, pp. 248-254.

[7] Min Wu, Bede Liu (2004), 'Data hiding in binary image for authentication and annotation', IEEE Trans on multimedia, Vol. 6, no. 4, pp. 528.

[8] Najme Maleki, Mehrdad Jalali (2014).' Adaptive and non-adaptive data hiding methods for gray scale images based on modulus function', Egyptian Informatics Journal, pp. 115-127.

[9] Orhan Bulan, Gaurav Sharma, Vishal Monga(2010),' Orientation modulation for data hiding in clustered-dot halftone prints', IEEE TRANS,Vol. 19,no. 8,pp. 2070.

[10] Qian Mao (2014), 'A fast algorithm for matrix embedding steganography', Elsevier, pp. 855-862.

[11] XiaotianWu, WeiSun (2014), 'High-capacity reversible data hiding in encrypted images by prediction error', Elsevier signal processing.

[12] Yu-Chi Chen, Chih-Wei Shiu, Gwoboa Horng (2014), 'Encrypted signal-based reversible data hiding with public key cryptosystem', Elsevier, pp. 1164-1170.

[13] Zhicheng Ni, Yun Q. Shi (2008),' Robust lossless image data hiding designed for semi-fragile image authentication', IEEE TRANS, Vol. 18, no. 4, pp. 497.