ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

Image Steganography in DWT Domain

Ch.Kavya[#1], B.Anusha[*2], T.Lakshmi Prasanna[#3]

Academic Consultant, Dept. of ECE, SPMVV, Tirupati, Andhra Pradesh, India[#1]

Student, Dept. of ECE, SPMVV, Tirupati, Andhra Pradesh, India[#2]

Student, Dept. of ECE, SPMVV, Tirupati, Andhra Pradesh, India[# 3]

ABSTRACT: In this paper, we present a novel Steganography method for embedding of secret data in still grayscale image. In order to provide large capacity of the secret data while maintaining good visual quality of stego-image, the embedding process is performed in transform domain of Discrete Wavelet transform (DWT) by modifying of transform coefficients in an appropriate manner. In addition, the proposed method do not require original image for successful extraction of the secret information. The experimental results show that the proposed method provides good capacity and excellent image quality.

KEYWORDS : Steganography, Haar-DWT transforms.

I. INTRODUCTION

Steganography is a method of embedding the secret message into a camouflage media to ensure that unintended recipients will not be aware of the existence of the embedded secret data in cover media.Steganography is different from cryptography. Steganalysis is the science of detecting hidden information. The main objective of steganalysis is to check whether the condition is met or not. There are two types of steganalysis. They are visual attacks, Statistical attacks. These are of three types-passive attacks and active attacks and structural attacks.

II. LITERATURE SURVEY

The security of Transmission of data becomes a huge issue in information and communication Technology. So ,to ensure the security of data during transmission, Two major techniques are adopted. They are Cryptography and Steganography. In these, the input data is encrypted using encryption algorithms and embedded into carrier image then transmitted through a communication channel, at the receiver side, data decrypted using data decryption algorithms is restored with error free. A most interesting application of data embedding is providing different access levels to the data. For example, the amount of detail that can be seen in a given image can be controlled. A person with a high access level can see details that another person with a lower access level would not see.

Most data-embedding algorithms can extract the hidden data from the host signal with no reference to the original signal. In some scenarios, an original is available to the detection algorithm. Typically, data-embedding algorithms that use the original signal during detection are robust to a larger assortment of distortions. The detection algorithm may “subtract off” the original signal from the received signal prior to data detection

III. PROPOSED ALGORITHM

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 advantageous as it performs local analysis and multi-resolution analysis. To analyse a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). Wavelet analysis can be of two types: continuous and discrete. In

DOI: 10.15680/IJIRCCE.2017. 0504232

this paper, discrete wavelet transform technique has been used for image steganography. This method transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object.

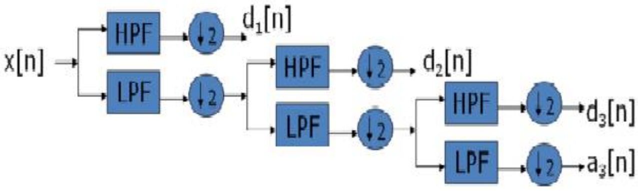


Figure1: 3-level wavelet decomposition

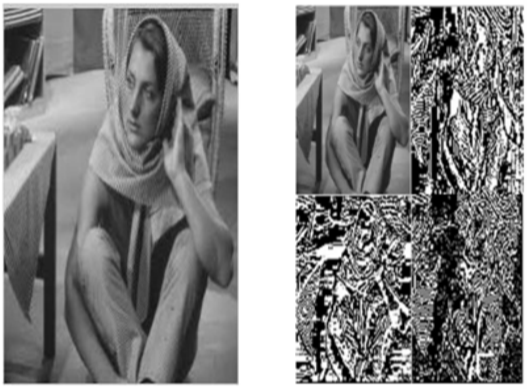
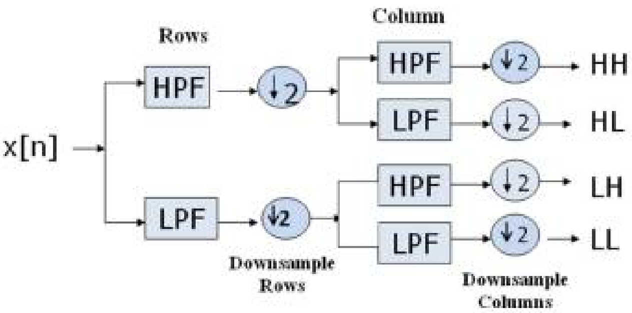


Figure2: original image & step decomposition

Next we apply one step to all columns .This results in four types of coefficients: LL, LH,HL,HH as follows:

LL	HL
LH	HH

Approximation	Horizontal Details
Vertical Details	Diagonal Details



If we apply DWT on an image, it divides the image in frequency components. The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image. These detailed coefficients can be used to embed secret image.

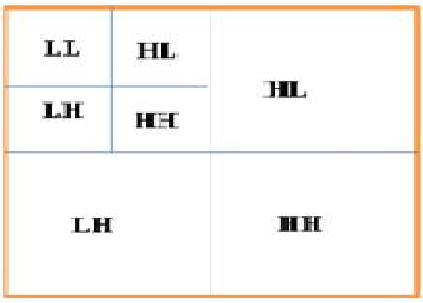


Figure3: step decomposition

Here we have taken an image as cover object and another small image as secret message. In embedding process, first we convert cover image in wavelet domain. After the conversion we manipulate high frequency component to keep secret image data. These secret image data further retrieved in extraction procedure to serve the purpose of steganography.

III. EMBEDDING PROCEDURE

In this step, insertion of secret message onto cover object is carried out. Additional components rather than usual steganographic object 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
Input: An m × n carrier image and a secret message/image.
Output: An m × n stego-image.
Algorithm: Steps-

1. Read the cover image (Ic)
2. Calculate the size of Ic
3. Read the secret image (Im)
4. Prepare Im as message vector
5. Decompose the Ic by using Haar wavelet transform
6. Generate pseudo-random number (Pn)
7. Modify detailed coefficients like horizontal and vertical coefficients of wavelet decomposition by adding Pn when message bit = 0.
8. apply inverse DWT
9. Prepare stego image to display

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

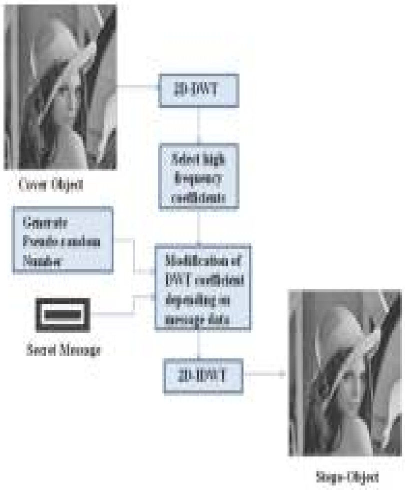

Cover Object
2D-DWT
Select high frequency coefficients
Generate Pseudo random Number
Modification of DWT coefficient depending on message data
Secret Message
2D-IDWT
Stego-Object

Figure5: Block diagram of secret image embedding procedure of steganography

IV. EXTRACTION PROCEDURE

In this step extraction of secret message is carried out. Additionally correlation theory is being used. Correlation is the degree to which two or more quantities are linearly associated [6]. The correlation between two same size matrices can be

$$r = \frac{\sum_{m}\sum_{n}(A_{mn}-\overline{A})(B_{mn}-\overline{B})}{\sqrt{\left(\sum_{m}\sum_{n}(A_{mn}-\overline{A})^{2}\right)\left(\sum_{m}\sum_{n}(B_{mn}-\overline{B})^{2}\right)}}$$

where $\overline{A}$ = mean2 (A), and $\overline{B}$ = mean2 (B).

Input: An m × n carrier image and an m × n stego-image.
Output: a secret message/image.
Algorithm: Steps-
1. Read the cover image (Ic)
2. Read the stego image (Is)
3. Decompose the Ic and Is by using Haar wavelet transform
4. Generate message vector of all ones
5. Find the correlation between the original and modified coefficients
6. Turn the message vector bit to 0 if the correlation value is greater than mean correlation value
7. Prepare message vector to display secret image

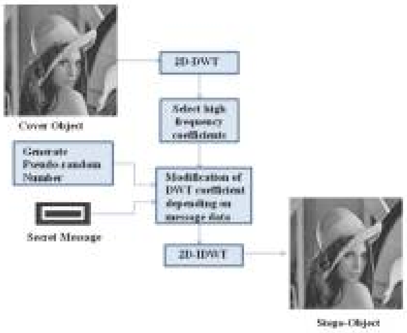

Cover Object
2D-DWT
Select high frequency coefficients
Generate Pseudo random Number
Modification of DWT coefficient depending on message data
Secret Message
2D-IDWT
Stego-Object

Figure6: block diagram of extraction of secret message from stego image

V. CONCLUSION

A combination of Steganography and Cryptography is a powerful technique for security of Data transmission. It provides additional security to the data. All these existing systems contains some problems, so we need to improve the secure data transmission by using powerful and efficient algorithms and combination of cryptographic and steganographic techniques. Hence data encryption and data decryption become error free.

REFERENCES

[1] BÁNOCI, V., BUGÁR, G., LEVI using by CDMA techniques, Radio 183 – 186 .
[2] COX, I. J., MILLER, M. L., BKALKER, T. Digital water marker Burlington: Morgan Kaufmann, 2000
[3] LEE, Y.K., CHEN, L. H. High cap Vision, Image Signal Process., 2000
[4] TSAI, P. ., LIN, J. substitution and genetic algorithm.3, p. 671 – 683 .
[5] CHUNG, K. L., SHEN, C. H., CHA Based Image Hiding Scheme., HU, Y. C., CHANG, C using block truncation coding. Pro Digital Steganogarphy. Kitakyaushu.
[6] WANG, R. Z., LIN, C. F steganogron Digital Watermarking, 2003, p.1.
[7] MIYAKE, K., IWATA, M., SHIO utilizing features of JPEG images. I Electronics, Communications and C 4, p. 929 – 936.
[8] XIANG-YANG, L., DAO-SHUN, review on blind detection for image 2008, Vol. 88, no. 9, p. 2138 – 2157.

BIOGRAPHY

CH.Kavya is an Academic consultant in Electronics and Communication Engineering Department, Sri Padmavathi Mahila Visvavidyalayam, Tirupati. Completed her M.Tech in sree vidyanikethan engineering college, tirupati her research interests are Digital Image Processing (DIP), Digital Signal Processing (DSP) and VLSI design.