ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

STEGANOGRAPHY IMAGE IN COLOR IMAGE USING WAVELET TRANSFORM

Anita Vyas*, Prof. Chiranjeevi Mondikathi
* Department of Electronics & Communication, Acropolis,
Indore, India,

Abstract

The Discrete Wavelet Transform is a relatively recent and computationally efficient technique in computer. The wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis system. Discrete wavelet transform (DWT) technique has been used for steganography image. Though steganography is a old method of hiding information behind some object, but still this is very effective for secure data transfer and data exchange. A method for image steganography has been discussed, utilising basics of discrete wavelet transform. The cover image is divided into higher and lower frequency sub bands and data is embedded into higher frequency subbands. This is proved by the high Peak Signal to Noise Ratio (PSNR), value for both steganography and extracted secret. The results are compared with the results is similar techniques and it is found that the proposed technique is simple and gives better Peak Signal to Noise Ratio (PSNR) values than others.

KEYWORDS: Wavelet Trabsform, Steganography, PSNR, RMSE, Secret Image, etc.

INTRODUCTION

The main purpose of Steganography, which means 'writing in hiding' is to hide data in a cover media so that others will not be able to notice it. While cryptography is about protecting the content of messages, steganography is about concealing their very existence [1]. The applications of information hiding systems mainly range over a broad area from military area, intelligence agencies, internet banking, online elections, medical-imaging and so on. The cover medium is usually chosen keeping in mind the type and size of the secret message and many different type carrier file formats can be used. These variety of applications make steganography a hot topic for study. In the current situation digital images are the most popular carrier/cover files that can be used to transmit secret information.

Fig. 1 Data Hiding Scheme

Steganography is the art or practice of concealing a text, image, or file within another message, image, audio, video, or file. In word steganography is of Greek origin and means concealed writing or covered writing. In digital steganographic image, electronic communications may include steganographic coding inside of a transport layer, and such as an image file, document file, program or protocol. A media files are ideal for steganographic transmission because of their large size data. For example, in a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, and a change so subtle that someone not specifically looking for it is unlikely to notice it. In the proposed algorithm has two stages of implementation process. In the first stage the secret message is hidden in an image size 640 x 480 using LSB algorithm method, and in the second stage the stego-image resulting is hidden in a cover image size 1024x1024, using the decomposition of multi-resolution discrete wavelet transform (DWT). Thus simultaneous hiding the secret message and secret images in a single cover image.

Steganography equation is 'Stego-medium = Cover medium + Secret message + Stego key'. The general model of the data hiding can be described as follows steps. The embedded data is the message that one wishes to send secretly system. It is usually hidden in an innocuous message referred to as a covertext or cover-image or cover-audio as appropriate, thus producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and /or recovery of the embedded data to parties who know it [3].

BASIC STEGANOGRAPHIC SYSTEM

A classical steganographic system security relies on the encoding systems. Although such a system might work for a time, it is simple enough to expose the entire received media passing by to check for hidden messages ultimately, a steganographic system fails. In modern steganographic system, as shown in Figure 2 attempts to be detectable only if secret information is known namely, a secret key. For in this case, in in cryptography should be involved, which holds that a cryptographic system's security should rely solely on the key material. Steganography to remain undetected and the unmodified cover medium must be kept secret system, because if it is exposed, a comparison between the cover and stego media immediately reveals the changes.

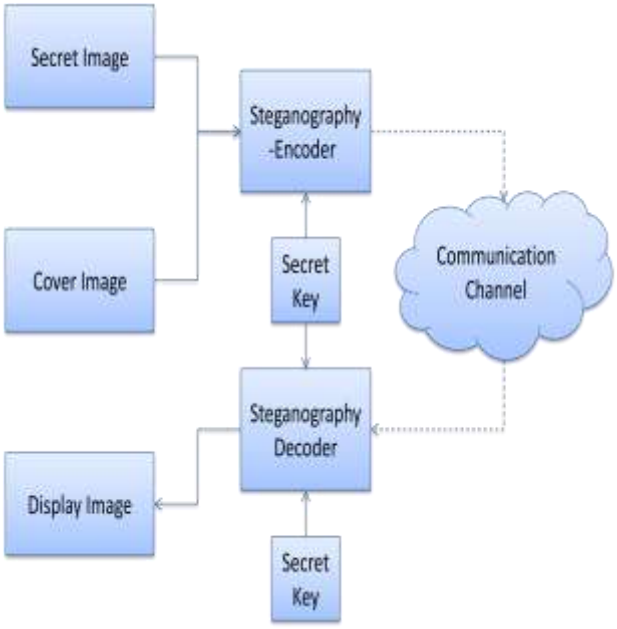

Fig. 2 A modern steganography systems.

STEGANOGRAPHY TECHNIQUES

The different types Classification of Steganographic Categories

- Pure steganography where is no stego key. Based on the assumption that no other party is aware of the communication.
- In secret key steganography where the stego key is exchanged prior to communication system. This is most suspectible to interception.
- The public key steganography where a public key and a private key is used for secure communication.

The Classification of Steganographic Methods

The steganography methods can be classified mainly into six type, although in some cases exact classification is not possible [2].

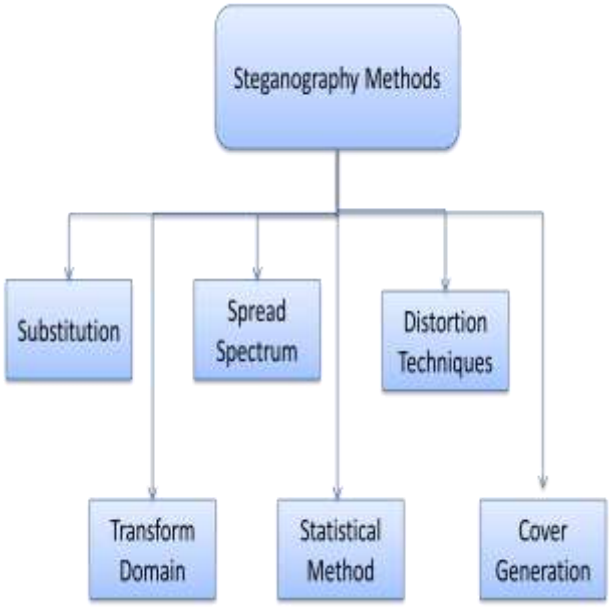

Fig. 3 Steganography Process

- Transform domain techniques embed secret image information in a transform space of the signal.
- In the spread spectrum techniques adopt ideas from spread spectrum communication systems.
- The statistical methods encode information by changing several statistical properties of a0 cover and use hypothesis testing in the extraction process.
- Distortion techniques store information by signal distortion and measure the deviation from the original cover image in the decoding step.
- The cover generation methods encode information in the way a cover for secret communication is created.

WAVELET TRANSFORM

Wavelet transform is used to convert a spatial domain into frequency domain function. The use of wavelet in image stenographic model lies in the fact that the wavelet transform clearly separates the high frequency and low frequency information on a pixel by pixel basis process. The Discrete Wavelet Transform (DWT) is preferred over Discrete Cosine Transforms (DCT) because image in low frequency at various levels can offer corresponding resolution needed. One dimensional Discrete Wavelet Transform is a repeated filter bank algorithm, and the input is convolved with high pass filter and a low pass filter.

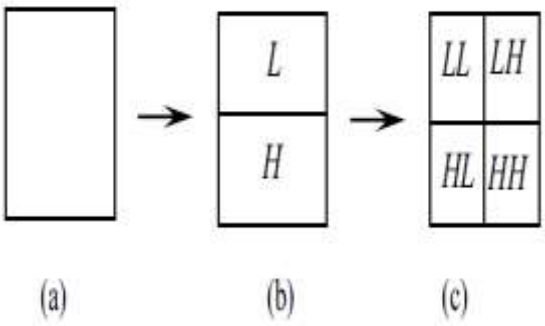

Fig. 4 Wavelet decomposition sequence (a) Original Image (b) Wavelet transform and decimation in column (c) Wavelet transform and decimation in row

The LL wills called as approximation of image and it contrail the low frequency information of image .Due to our limited resolution ability for high frequency image this will contain almost information about the image. In this high frequency contain LH, HL, HH are used to de-noised the image

The wavelet transform (WT) is based on signal processing and developed from the Fourier transform basis. The wavelet transform is expressed as a series of functions which are related with each other by translation and simple scaling. The original WT function is called mother wavelet [5, 6] and is employed for generating all basis functions. A set of functions is constructed by scaling and shifting the mother wavelet $\psi(t)$.

$$\psi_{a,b}(t) = \frac{1}{\sqrt{b}}\psi\left(\frac{t-a}{b}\right) \quad (1)$$

The original signal can be reconstructed by an appropriate integration and this is performed after projecting the given signal on a continuous family of frequency band. The continuous wavelet transform (CWT) of a signal x(t) is given by:

$$CWT(a,b) = \frac{1}{\sqrt{b}}\int_{-\infty}^{\infty} x(t)\,\psi\left(\frac{t-a}{b}\right) dt \quad (2)$$

Where the superscript is the complex conjugate and $\psi*a,b$ represents a translated and scaled complex conjugated mother wavelet. The mother wavelet ψ is invertible when it verifies the condition of admissibility which is stated as:

$$\int_{-\infty}^{\infty} x(t)\,\psi\left(\frac{\hat{\psi}(\omega)}{\omega}\right) d\omega < \infty \quad (3)$$

Many mother wavelets are used for computing the wavelet transform and Morlet is one of them. It is expressed as follow [7]:

$$\psi(t) = \frac{1}{\sqrt{\pi f_b}} e^{2i\pi f_c \cdot t_e} - \frac{t^2}{f_b} \quad (4)$$

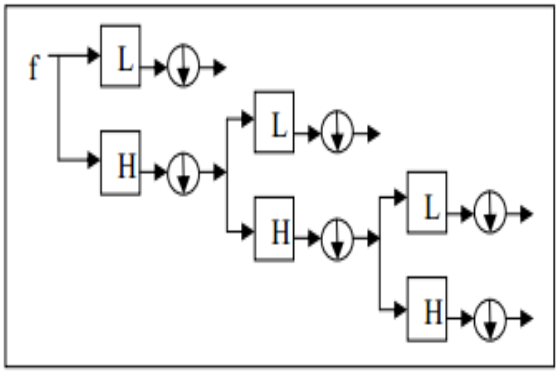

Fig. 5 2DWT

RESULTS AND DISCUSSION

The performance of steganography technique using discrete wavelet transform. Wavelet domain is pretty new and efficient transform domain than previously used Fourier Transform. The results of proposed approach are obtained in the form of PSNR, RMSE, with compare to noise density for the images. Execution time of algorithm also calculated.

Fig. 6 Color images that are used as cover images

Fig. 7 Cover image convert to gray image

Fig. 8 Images which are used as secret images

Fig. 9 Secret image convert to gray image

Fig. 10 Stego Image

Fig. 11 Stego Image

Fig. 12 Steganographic hidden image

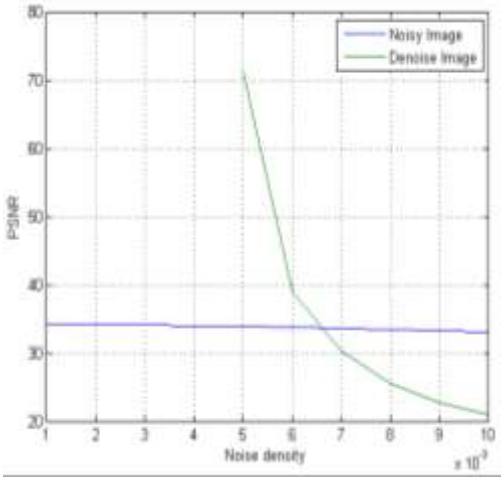

Fig. 13 Performance of wavelet de-noising, PSNR Vs Noise density

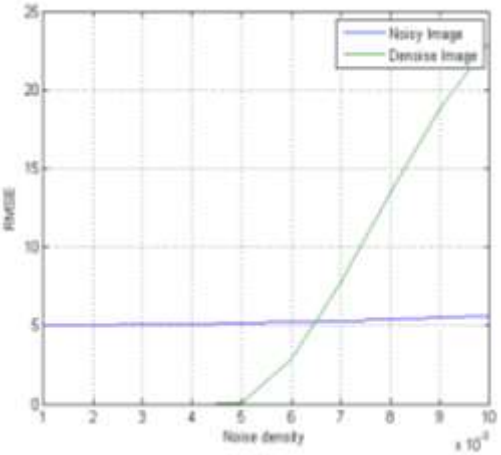

Fig. 14 Performance of wavelet de-noising, RMSE Vs Noise density

CONCLUSION

This work is related with steganography image using discrete wavelet transform. The DWT is applied on color images. Arnold transformation is used to improve security. The results are shown in the form of stego and recovered images. Analysis of the algorithm is accomplished by comparing the proposed approach with similar existing approaches. This method succeeds to keep intact the original image, after the extraction of embedded secret message. In this proposed method can be termed as successful new technique of image steganography.

REFERENCES

[1] *C.P.Sumathi1, T.Santanam, "Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.*

[2] *Barnali Gupta Banik, "A DWT Method for Image Steganography", ijarcsse. Volume 3, Issue 6, June 2013.*

[3] *H S Manjunatha Reddy, "High capacity and security steganography using discrete wavelet transform", International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (6).*

[4] *Parul1, Manju2, Dr. Harish Rohil, "Optimized Image Steganography using Discrete Wavelet Transform (DWT)", ISSN 2347 - 6435 (Online) Volume 2, Issue 2, February 2014.*

[5] *Ali A-Ataby and Fawzi A-Naima, "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", International Arab Journal of Information Technology, Vol. 7, No. 4, October 2010.*

[6] *Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, "A secure color image steganography in transform domain", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, March 2013*

[7] *Bilgin A., Sementilli J., Sheng F., and Marcellin W., "Scalable Image Coding Using Reversible Integer Wavelet Transforms," Computer Journal of Image Processing IEEE Transactions, vol. 9, no. 4, pp. 1972 - 1977, 2000.*