INTERNATIONAL JOURNAL OF

INVENTIONS IN APPLIED SCIENCE

AND ENGINEERING

e-ISSN: 2454-9258; p-ISSN: 2454-809X

Hiding Secret image in image based Discrete Wavelet Transform

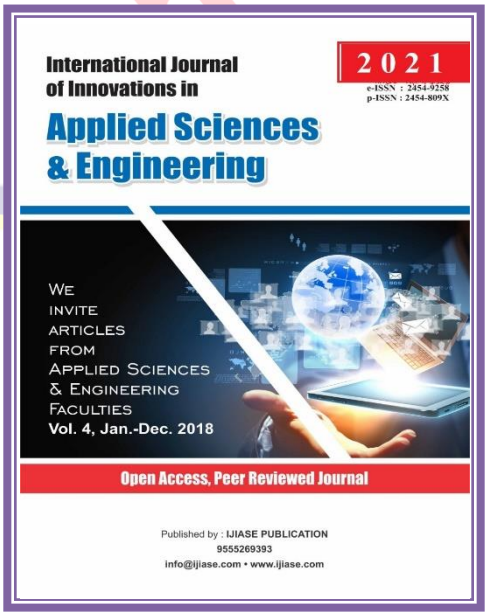
Doaa Mahmood Abass, Ali Hussien Mary
Informatic Institute for postgraduate studies, University of technology

Paper Received: 14th February, 2021; **Paper Accepted:** 16th March, 2021;

Paper Published: 18th March, 2021

How to cite the article:

Doaa Mahmood Abass, Ali Hussien Mary, Hiding Secret image in image based Discrete Wavelet Transform, IJIASE, January-December 2021, Vol 6; 12-18



ABSTRACT

Sending encrypted messages would always attract third parties' attention, i.e. crackers and hackers, likely triggering attempts to break and expose the original messages. Steganography is applied in a digital environment to mask the presence of contact by concealing a hidden message within another. The goal of this paper is to develop a suggested method for providing a high-level safety system by implementing and developing a steganography system to hide data in an image cover. This is a more complicated system. It implemented the system at two embedding levels, and this is a high level of security problem since two extraction levels were needed to extract the hidden data. In the frequency domain, the framework is implemented using wavelet domain transformation. The principle of using transformation in the proposed method is due to the results of previous published works that showed that hiding in the frequency domain is more efficient than hiding in the time domain, due to the compactness and robustness of such transformations. In this proposed method, a Haar Wavelets Transformation (WT)

Keywords: Steganography, Watermarking, Wavelet Transform (WT), DWT.

INTRODUCTION

It has become possible to exploit a large amount of multimedia sent over the Internet or any other network because of the increased creation of multimedia processing techniques and applications. Internet connection makes it easy to insertIt is easier and cheaper to change, remove and/or distribute digital content. The method of transmitting data over the internet could also be unsafe. Many data protection strategies have been proposed to deal with this issue. Cryptography and steganography, which are used essentially to protect data against malicious activities or unwanted parties, are the two most common and related among them [1]. Preserving the presence of a message secret is the main distinction between cryptography and steganography. In the case of cryptography, the message is altered in some way so that it is visible, but the unintended individual does not comprehend it. Whereas, steganography masks the fact that by concealing it within another media, the message remains. In other words, as a method of concealing secret information within a data carrier, digital steganography can be described in such a way that the existence of secret information is imperceptible. Therefore, compared to cryptography [2], steganography provides an additional layer of security for confidential

information. In general, by applying the embedding algorithm inversely to the intended receiver, it is possible to extract secret information. Three difficult factors are mainly defined by steganography systems: imperceptibility, robustness, and ability the imperceptibility of steganography refers to the ability to hide data without human detection being detected. Although robustness tests the resistance of steganography to signal manipulation or even external attacks without affecting secret information extraction processes. The most significant factors in assessing the consistency of steganography techniques are robustness and imperceptibility since they interfere with each other.

LITERATURE REVIEW

Below are some of the related works listed:

Manjula1 G.R., et al.in 2015[3], implements a method for integrating a hidden (color image) into a cover (color image). For image steganography, a 2-3-3 LSB insertion method has been implemented.

Gupta H! Gupta H. Two techniques in picture steganography were offered by et al. in 2013[4] (image domain, transform domain). This leads to minimizing the MSE values for image demain when using the LSB algorithm and making the PSNR values greater when the amount of bits substituted is high.

In 2013, in this paper, Arora S.et al.[5] applied a new approach to color image steanography using edge detection. In this proposed work, after detecting the edge of a color image, the hidden message (text) hides in the edge of the color image by making the scanning work in a window size 3*3.

From Ghasemi E. The implementation of the frequency domain (discrete Wavelet Transform) and artificial intelligent algorithm (Genetic Algorithm) was offered in 2011[6]. The cover image segmentation in 4*4 blocks using (DWT) and the mapping function-based genetic algorithm is applied to conceal hidden messages in DWT coefficients. The Best Pixel after Covering the Hidden Message It uses adaptation. The Genetic Algorithm and the best Pixel Adjustment were used for the best mapping function to reduce the MSE between the cover-image and the stego-image for high robustness frequency domain.

HAAR WAVELET TRANSFORM

The transformation of the wavelet is a mathematical tool that can translate images from the spatial domain into the frequency domain. The low and high frequencies are obtained by passing the image through filters

for high and low passes, respectively. Wavelet translates signal analysis treaties and splits the category and the category of approximations into specifics. The signal is analyzed on various scales and frequency bands. Two feature classes are added to DWT: scaling and wavelet, which apply to high and low pass filters. The decomposition works by splitting the division of time. In other words, just half of the samples in a signal are adequate for the entire signal to double the frequency separation [7]. The low frequency wavelet coefficient is generated by measuring the average of the two pixel values in the Haar Wavelet Transform and high frequency coefficients are generated by taking half of the difference for the same two pixels. For two pictures of damnation, In addition to horizontal high-low (HL), vertical low-high (LH) and diagonal high-high (HH), WT decomposes the image into various sub-bands as the resolution approximation band or low-low (LL), detailed components as shown in Figure 1 In the low-frequency wavelet coefficients (approximation band), the essential information of the spatial domain image (smooth parts) exists and the edge and texture details usually exist in the high-frequency sub-bands, such as LH, HL, and HH[11]. The transformation of the Haar wavelet is similar to its opposite, which is considered to be a significant feature of it [7].

Figure (1) Haar Wavelet Transform

PROPOSED METHOD

Double Wavelet transforms were described in this review. The hidden image is translated into its own. Corresponding coefficients of wavelets for the cover image. The suggested steps in the technique are the as follows:

- Read the host image.

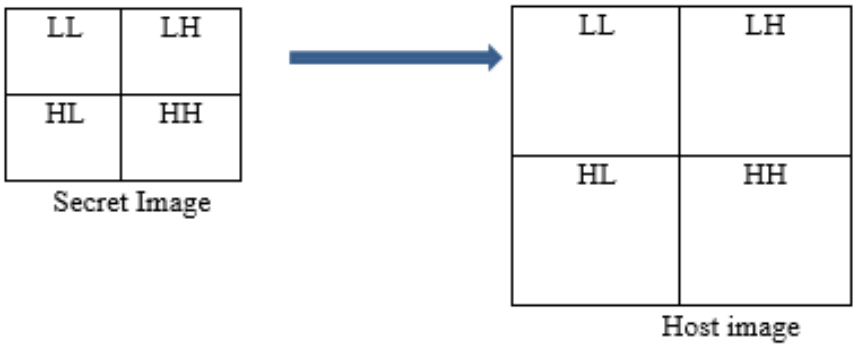
- Read the Secret image

1- Apply 2DWT for the secret image

2- Apply 2DWT for the host image

3- Propose the following equation for inserting the secrete data into host image

4- water_marked_LL = host_LL + (k*_DWT_secrete_image);



Receiver

1- Apply 2DWT for the watermarked image

2- Apply 2DWT for the host image

3- Extract the secret image

4- DWT_secrete_image= (water_marked_LL - host_LL)/k

SIMULATION AND RESULTS

The proposed system is designed using Matlab 2018 for programming. Three different images are used as secret image , Lena is employed as the cover-images of size 512x512, 8-bit gray-level images as shown in Figure 2. In this section, demonstrates the results and evaluate the efficiency of the hiding algorithm, PSNR and image fidelity are used to test images. PSNR is measured as:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

Table 1. Show the capacity, PSNR from Lena stego-image.

K	PSNR	IF
0.01	90.0309	-3.1558e-09
0.02	84.0103	84.0103
0.03	80.4885	-3.0129e-08

Figure (2) results image gray-level images

CONCLUSIONS

In this job, some of the conclusions are reached; these are as follows;

1. MSE and PSNR are the most important steganography consistency factors

2. DWT-based hiding techniques have concluded that all sub-bands offer similar results with some little varying outcome.

3. The results of the MSE and PSNR in traditional LSB are higher than DWT by comparing steganography with DWT and steganography using the traditional LSB process, but the protection in DWT is much higher than LSB.

REFERENCES

[1] X. Duan, D. Guo, N. Liu, B. Li, M. Gou and C. Qin, A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network, in IEEE Access, vol. 8, 2020, pp. 25777-25788.

[2] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan and B. Balusamy, Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques, in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, Jan. 2020, pp. 73-80.

[3] - Manjula G.R, and AjitDanti, " A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain", International Journal of Security, Privacy and TrustManagement (IJSPTM) Vol 4, No 1, February 2015.

[4] Gupta H, Kumar R, Changlani S,"Steganography using LSB bit Substitution for data Hiding", International Journal of Advanced Research in Computer Science and ElectronicsEngineering (IJARCSEE) Volume 2, Issue 10, October 2013.

[5] . Arora S, Anand S," A New Approach for Image Steganography using Edge Detection Method", International Journal of Innovative Research in Computer and CommunicationEngineering Vol. 1, Issue 3, May 2013.

[6] Ghasemi E, Shanbehzadeh J, and Fassihi N: "High Capacity Image Steganography using Wavelet Transform and Genetic Algorithm", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2011, Vol. I, IMECS March 2011.

[7] Houssein , E.H.; Ali, M.A.S.; Hassanien, A.E. An Image Steganography Algorithm using Haar Discrete Wavelet Transform with Advanced Encryption System. IEEE Proceedings of the Federated Conference on Computer Science and Information Systems.2016, 8, 641– 644, doi: 10.15439/2016F521.