Image Steganography Based on Discrete Wavelet Transform and Chaotic Map

Iman I. Hamid

University of Baghdad, Collage of Education for Women, Computer Science Department, Iraq-Baghdad

Abstract: ***Steganography is the science of hiding information in the cover media, a force in the context of information security. In this work, a gray image was hidden into another gray scale image using an algorithm was proposed. Firstly, the secret image was encrypted using 'logistic chaotic map' to achieve 'high security'. Then the encrypted secret image embedded into the HH sub band of the wavelet transformed cover image. Favorable results obtained using peak signal to noise ratio (PSNR) and correlation criteria. The implementation of our proposed method done using MATLAB version 2010a.***

Keywords: Steganography, Discrete wavelet transform (DWT), logistic Chaotic map.

1. Introduction

The way for encryption special communications called Cryptography with a diverse method of securing established for encrypt or decrypt the data to maintain the mystery of the message. Keeping the subject of the secret message gives unsecure method, but it could be obligatory to maintain a presence of the secret message. The technology used to implement this, concealing information called steganography. The way could be the messages hidden in the average so-called cover the object in a technique that there is a message unnoticeable, noiselessness is the most significant obligation. In 'Steganographic' schemes cover object' can be a 'digital image' of the cover object, audio, or video file. 'In a confidential, letter called the payload can be audio, video, plain text or image files'. Frequency and spatial domain are the main components of 'Steganographic' procedures. In this paper, we proposed an image steganography method in DWT domain using logistic chaotic map. Moreover, the algorithm has a high capacity and a good Invisibility [1].

2. Related work

A.Nag, S. Biswas et al. [2], they used Haar-DWT spatial domain of original image was transformed to frequency domain. The two dimension 'Discrete Wavelet Transform' (2D-DWT) was implemented on cover image with a gray level and Huffman encoding is implemented on the secret image previously inserting. The quality of an image can be improved using preserving the coefficients of wavelet in the low frequency sub band.

3. Discrete Wavelet Transform

Converting the spatial field in the frequency domain usually done using Wavelet transform. The use of wavelets in the form of shorthand model lies in a statement that the wavelet transform is obviously splits the high from the low-frequency information based on pixels.

The simplest method of wavelet transforms is the Haar wavelet. In Hara, transform the coefficient in the low frequency wavelet was created by take the averaging of the values of two pixel, and it can created the high frequency

Coefficients by taking half difference of the similar two pixels. Figure (1) shows four bands approximate, Vertical, Horizontal, and diagonal Bands that represented as LL, LH, HL and HH restively. The spatial domain image is an important part of the low frequency wavelet coefficients, which lies in approximation band. Also, the spatial domain image have the edge details of the high frequency coefficients which lies in other bands called detail bands. [3, 4].

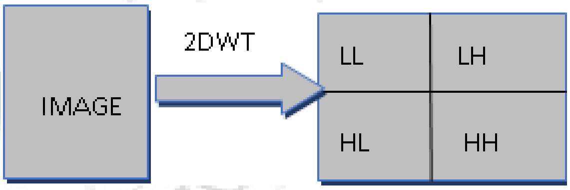
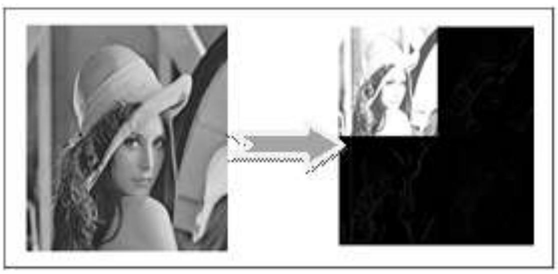


Figure 1: Components of 1-level 2DWT

In figure (2), we can show the 2D Haar- DWT on image "Lena". The eyes of a human cannot recognize the small changing on the edges and textures of an image but it is very sensitive to any changes in the smooth parts. By knowing this fact, this can lead to hide the secret image inside high-frequency sub-bands and will not be recognized by the human eyes, [2].



(a) (b)

Figure 2: ('a') image of LENA before 2-D Haar-DWT, ('b') after the 2-D Haar-DWT

International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2015): 6.391

4. Logistic Chaotic map

To increase the security the chaotic maps have been useful in steganography and watermark. The interesting part of the chaos in embedding information features are very compassion to preliminary conditions and the spread of the orbits of the total space. The chaotic maps it is a perfect candidates of encryption and watermarking because it have special characteristics. Signals chaos, which is complex and it is impossible to predict over the long time, which generated by a simple dynamical systems such as logistics map. You can create a large number of confusing signals uncorrelated, such as random, but inevitable with a minor perturbation of factors. Save the information chaos and primary condition as a secret key, signal chaos could be easily regenerated. [5, 6].

The 2-D logistic map is analyses for its complex reactions in attraction evolution. It has further complexity in chaotic processes than 1-D logistic map [7].

4.1 Mathematical Definitions

The 2D logistic map can be defined as the equation (1), where "r" is the variable of the system and (x_i, y_i) is the point of the pair-wise at the i^{th} loop' [7].

$$\left.\begin{aligned} x_{i+1} &= r(3y_i + 1)x_i\,(1 - x_i) \\ y_{i+1} &= r(3x_{i+1} + 1)y_i\,(1 - y_i) \end{aligned}\right\} \qquad (1)$$

In this paper, 2D logistic chaotic map was used to implement the permutation process to encrypt the secret image and generate the random key as shown in figure (3) and decryption method shown in figure (4).

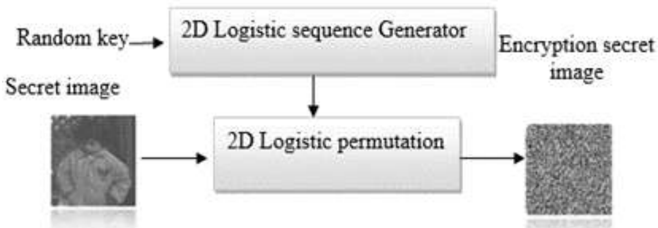


Figure 3: Encryption method

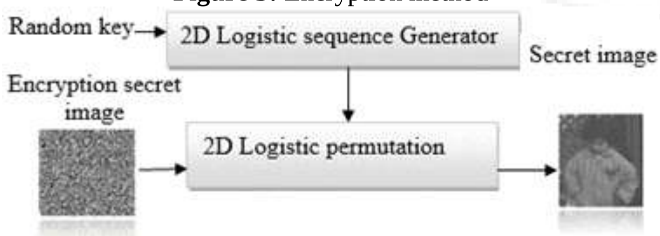


Figure 4: Decryption method

5. The Proposed Method

In this section, the main steps of the 'proposed work' will be explained. Where the idea of the work based on hide secret gray scale image into a cover gray scale one, and the secret image permutation by using logistic chaotic map method (as explain in section 4) to increase security before hiding process, the cover image decomposed by 'wavelet Transform (DWT)' and then embedded the encryption "secret image" in HH band. The block diagram of the embedding system shown in figure (5) the encryption of the 'secret image' explained in section (4).

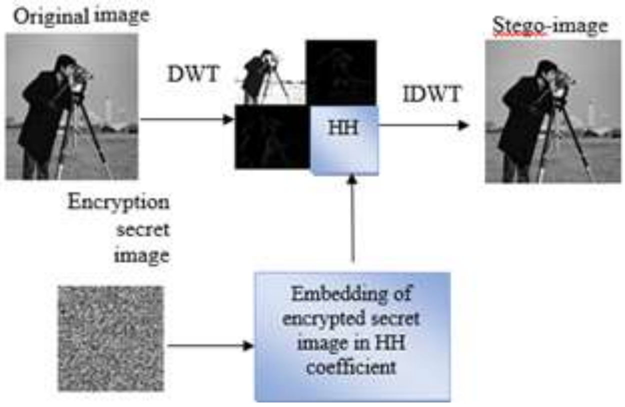


Figure 5: Block diagram of the Embedding Process

5.1 The Embedding Process

In the following a brief description for embedding algorithm:
Input: "Cover image" of size n x n and "secret image" of size n/2 x n/2.
Output: Stego Image n x n.

1) Read the Cover image of size n x n.
2) Read the 'Secret image' that have a size 'n/2' x 'n/2'.
3) Decompose the Cover image by using "db1" wavelet transforms. The cover image was decomposed into (LL, LH, HL and HH) sub bands.
4) Permute the secret image by logistic chaotic map method.
5) Embed the encrypted secret image (obtained from steps) in the HH sub band of 'cover image' by applying the equation (2):

$$Co(i_{hh}, j_{hh}) = \alpha * Se(i,j) \qquad (2)$$

Where $Co(i_{hh}, j_{hh})$ is a coefficient values of HH band, α is an imperceptibility scaling factor (by experimental test its found to be equal to 0.005), Se (i,j) is a secret encryption image and ((i,j)=1,2,3,…,n/2).

6) Apply Inverse Discrete Wavelet transformation to obtain the stego image.

5.2 Extraction process

In figure (6) block diagram for extracting the encryption secret image shown:

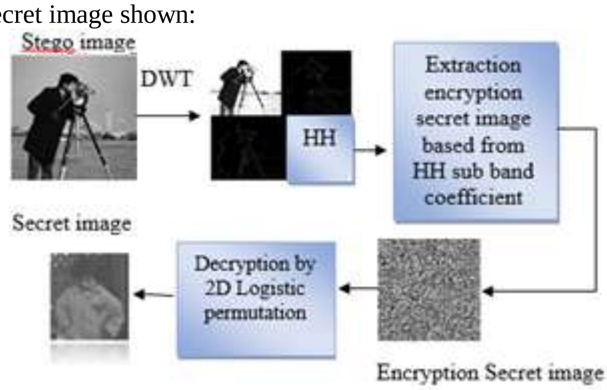


Figure 6: Block Diagram of the Extraction Process

Extracting process steps:
Input: 'stego image'.
Output: 'secret image'.

1) Load the stego image.
2) Decompose 'the 'stego image" using Discrete Wavelet transform to get [LL, LH, HL, HH] sub bands.
3) Extract secret encrypted image from the coefficient values of HH sub band, by using the equation (3):

$$Se\ (i,j) = Co(i_{hh,}j_{hh}\ )/\alpha \quad (3)$$

Where α is the scaling Embedding factor (equal to 0.005) and Co ($i_{hh,}j_{hh}$) is the coefficient of HH sub band.

4) Apply the inverse of chaotic map to decrypt the extracted secret image.

6. Evaluation of the Proposed Algorithm

In this part, we want to discuss the results that have been obtained through the proposed work. In this proposed work, two cover gray scale images (cameraman and Lena) of size 265x265 and two secret images (pout and boat) of size 128 x 128 are used, Figure (7) below shows the test images used in this work.

Figure 7: ('a'-'b') the set of "cover images" ('c'-'d') the set of "secret images"

The "Peaks Signal to Noise Ratio (PSNR)" factor used to evaluate the performance of the "proposed steganography algorithm". ‘‘PSNR’’ computed by using equation (4), [8]:

$$\textbf{PSNR = 10 log10 (255}^2\textbf{/ MSE)} \quad (4)$$

$$MSE = (1/N)^2\ \Sigma\Sigma\left(x_{ij} - x_{ij}\right)^2 \quad (5)$$

Where: x_{ij} = the "original pixel values", $x_{ij}{'}$ = the "modified pixel values", and 'N ' is the dimension of image.
and the correlation factor (CF) is used to measure the matches between the recovered data and the original secret data. Equation (6) represent CF, [8].

$$\text{CF} = \frac{\sum_m \sum_n (C_{mn} - \bar{C})\ (S_{mn} - \bar{S})}{\sqrt{(\sum_m \sum_n (C_{mn} - \bar{C})^2)(\sum_m \sum_n (S_{mn} - \bar{S})^2)}} \quad (6)$$

Where "C" is a 'cover image', "S" is a 'Stego image'. And " $\bar{C}$" = mean (C) and "$\bar{S}$"= mean (S).

Table (1), shows the CF and the PSNR results of the stego images obtained by the hiding process. The extracting secret images are also included.

Table 1: The results of the proposed work

Cover image 512 x512	Secret image 128 x128	Stego image	PSNR (db)	Extracted Image 128 x128	CF
			35.192		1.00
			35.191		1.00
			39.239		1.00
			39.240		1.00

As a result, for the proposed work, the PSNR value shows an acceptable result more than 30dB and the CF value show a good value equal 1 that means the secret image return as it was.

7. Conclusion

Through the proposed, algorithms were concluded the following:

1) High capacity of secret data can be gotten; the system can hide the secret images of (1/4) size of cover image.
2) A security is achieved by using logical chaotic map, which it is useful with steganography technique.
3) Depending on the value of PSNR the system gives us good invisibility (PSNR value above 30dB).

References

[1] Bandyopadhyay. Debiprasad, Dasgupta. Kousik. Mandal3. , J. K., Dutta. Paramartha," A Novel Secure Image Steganography Method Based On Chaos Theory In Spatial Domain ", International Journal of Security, Privacy and Trust Management (IJSPTM) Vol 3, No 1, February 2014.
[2] A.Nag, S. Biswas, D. Sarkar, P.P. Sarkar. "A Novel Technique for Image Steganography Based on DWT and Huffman Encoding", International Journal of Computer Science and Security, Volume (4).
[3] Abdul Latef. A. A," Color Image Steganography Based on Discrete Wavelet and Discrete Cosine Transforms", Ibn Al- Haitham J. For Pure & Appl. Sci. Vol.24 (3) 2011.
[4] Alwan, Iman M.G. "Comparative Study of Image Denoising Using Wavelet Transforms and Optimal
[5] Threshold and Neighbouring Window",J. Of College Of Education for Women vol. 25 (4) 2014.

[6] Wu, Xianyong, Guan. Zhi-Hong," A novel digital watermark algorithm based on chaotic maps", Physics Letters A 365 (2007) 403–406.

[7] Babazade Gorji. Rezvaneh, Hosseini Shirvani. Mirsaeid, Mooziraji. Farhad Ramezani," A new image encryption method using chaotic map", Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 3159-0040 Vol. 2 Issue 2, February - 2015

[8] 7-Wua. Yue, Yangb. Gelan, Jinb. Huixia, Noonana. Joseph P," Image Encryption using the Two-dimensional Logistic Chaotic Map" Journal of Electronic Imaging, January 2012.

[9] 8-Al-Ataby, Ali and Al-Naima, Fawzi."A Modified High Capacity Image Steganography Technique Based on Wavelet Transform", The International Arab Journal Technology, Vol.7, No.4, October 2010.

Author Profile

Iman I. Hamid received M.S. degrees in computer science from Iraqi commission for computers and informatics, Informatics Institute for postgraduate studies, she now **Instructor** in Computer Science Department at Collage of Education for Women, University of Baghdad Iraq-Baghdad.