Gray Scale Image Hiding Using Wavelet Packet Transform

Abbas A. Jasim

University of Basrah
College of Engineering
Computers Engineering Department

Abstract

This work implying the design of hiding system that hides a gray scale image into another gray scale image using two-dimensional wavelet packet transform.

The proposed hiding scheme uses Wavelet Packet Transform (WPT) to embed data elements of the secret image in different frequency bands of the cover image. The data elements of the secrete image are placed within DWT subspaces after simple treatment in order to reduce its significance on the resulting image and to increase security. The resulting image (the cover image within which the secret image is hidden) is called stego_image. Stego_image is closely related to the cover image and does not show any details of the secret image.

The proposed system achieves perfect reconstruction of the secret image. All programs in this work is written by MATLAB 7.

إخفاء الصور ذات التدرج الرمادي باستخدام تحويلة الموجة

عباس عبد الأمير جاسم
جامعة البصرة- كلية الهندسة- قسم هندسة الحاسبات

الخلاصة

يتضمن العمل تصميم نظام إخفاء يقوم بإخفاء صورة ذات تدرج رمادي بصورة أخرى ذات تدرج رمادي أيضا باستخدام تحويلة الموجة ثنائية البعد.

تستخدم الطريقة المقترحة تحويلة الموجة لتضمين بيانات الصورة السرية ضمن حزم ترددية مختلفة في الصورة الغطاء. تخضع بيانات الصورة السرية إلى معالجة أولية قبل تضمينها داخل بيانات الصورة الغطاء. تدف هذه المعالجة الى تقليل تأثيرها في الصورة الناتجة وكذلك لزيـادة درجـة السرية. تسمى الصورة الناتجة بـ(stego_image) و هي عبارة عن الصورة الغطاء مطمور بداخلها الصورة السرية . تتميز هذه الصورة بأنا قريبة جدا من الصورة الغطاء ولا تبين أي تفاصيل تدل على إخفاء صورة أخرى ضمنها (أي الصورة السرية). يحقق النظام المقترح استرجاع تـام للصورة السرية..

جميع البرامج الموجودة ضمن هذا العمل قد كتبت بواسطة برنامج ألـ (MATLAB 7).

1.Introduction

Computer networks development provides inexpensive communication of information between people or computers on opposite sides of world. Special and reliable security in storage and transmission of digital images are needed in many applications such as military image databases, military images communication and medical image system. Image hiding can fulfill such security tasks to protect the content of digital images [1,2] .

In general, information hiding is used to embed data into various forms of media, such as images, audio or text with minimum amount of degradation [2,3]. The practice of hiding (encoding) secret information in a manner such that the existence of secret information is concealed is called steganoraphy [4]. It prevents outside observer from recognizing that hidden information is present. Hence, hiding message with steganography reduce the chance of secret message being detected [5,6].

The content of information (such as image) is not altered by steganography, but it is hidden inside a cover (such as another image)[7]. The resulting stego_image can be transmitted without revealing that secret information is being exchanged [8,9].

2.Gray Scale Images Structure

In gray scale image (so called intensity image), each image is represented as a data matrix of (M×N) elements. Each element of the matrix corresponding to one image pixel. The elements in the intensity matrix represent various intensities ,or gray levels. Where intensity 0 represent black, while intensity level 255 usually represent full intensity, or white.

3.Discrete Wavelet Transform

The wavelet transform is a technique for analyzing signals. It divides a signal into difference frequency components each with different resolution.

The Discrete Wavelet Transform (DWT) is used when a signal being sampled such as with digital image processing [10]. An efficient way to implement DWT uses filters. The signal is filtered by Low Pass Filter LPF and High Pass Filter HPF then the signal is down sampled. The resulting low pass signal is called approximation and it is much similar to the original signal. The high pass signal is called details signal. The filters used as LPF and HPF to compute DWT are commonly referred as h(n) and g(n) respectively. Filters h(n) and g(n) are Quadrature Mirror Filters(QMF) [11]. There are several types of wavelet (such as Haar , Daubechies, Coifman, symlets, and Morlet). Each wavelet has its own filters h(n) and g(n) .

For images Two Dimensional Discrete Wavelet Transform 2D_DWT decomposes image into multi levels of independent information .Images will be transformed in each level of decomposition to four bands, one low information image and three details images. One level DWT for an image can be computed as:

Each row of the image X is passed through LPF h(n) and HPF g(n) and decimated by two to produce signals 'y1' and 'y2' .Then each column of 'y1' is passed through LPF, h(n) and HPF, g(n) and decimated by two to produce 'a'(the approximation) and 'h'. The same thing is done with ‘y2’ to produce 'v' and 'd'.

When the DWT is used to decompose the resulting subspaces (a ,h ,v and d) then the resulting transform is called Discrete Wavelet Packet Transform DWPT.

A 2D_DWT decomposition and reconstruction is shown in Figure1.The four subspaces low-low (approximation), low-high (horizontal), high-low (vertical) and high-high (diagonal) are depicted in Figure2. While Figure3 shows an image with its level_1 DWT. Viewing Figure3 gives two indications, the first is that the most information of an image is contained

in the approximation subspace 'a' of DWT and little information is contained in each of details subspaces 'h' ,'v', and 'd' . So that the secret image data should be placed in details subspaces of DWT of the cover image and not in the approximation in order not to deteriorate the cover image. The second indication is that the coefficients values of the details subspaces are low, since they appear black in Figure3b. So that the data to be embedded in these subspaces should be low in order to make the resulting stego_image more similar to the cover image.

4.The Proposed Hiding System

The proposed hiding system deals with gray scale images for each secrete and cover images. It assumes that the size of secrete image (in pixel) is one quarter the size of the cover image. For example the size of secret image is (256×256), (M×N), and the size of the cover image (512×512), (2M×2N).

The proposed system uses the DWT to decompose the cover image into subspaces to represent it in different frequency bands. The data elements of the secrete image is placed within DWT subspaces after simple treatment. There are two goals of the treatment that is done on secret image data elements. The first is to reduce its significance on the cover image that leads to more similarity between cover image and resulting stego-image. The second is to increase security by placing data unit that is derived from secret image coefficients and not the coefficients themselves.

4.1 The Procedure of the Proposed Hiding System

The steps of the proposed hiding approach are:

1- compute the coefficients of the secret image to be embedded within the cover image. Each data element (s) in secret image is represented by two numbers (t and r) as :

$$s = t^2 + r \qquad \ldots(1)$$

Where t is the integer part of the square root of data element (s) and r is the remainder. The two numbers t and r are computed for each element of the secret image, two matrices will be produced T (the root matrix) and R (the remainder matrix) each of size (M×N), the size of the secret image.

For example if the element in pixel (i , j) of the secret image is 200 then the data element T(i,j)= 14(the integer of the square root of 200) ,and R(i,j)= 4 (the remainder $200-14^2$). The main goal of this step is to represent the coefficient of the secret image with small numbers in order to minimize their significance on the cover image and producing stego_image very closed to the cover image.

2- Compute the DWT of the cover image using one of the known wavelet decomposition such as Haar wavelet. It resulting four subspaces each with size(M×N), one approximation 'a' subspace and three details subspaces 'h' ,'v', and 'd'.

3- Take one of the details subspaces of the DWT of the cover image to embed the coefficient of root matrix T, for example subspace 'd'. The root matrix T coefficients will replace the coefficients of wavelet subspace 'd'.

4- Compute the DWT of each of the remaining two details subspaces ('h' and 'v'). The DWT of these signals (Second level) may use different wavelet type from that of the first level. It resulting four subspaces for 'h' labeled (a_h ,h_h , v_h , and d_h), and four subspaces for 'v' labeled (a_v , h_v , v_v , and d_v) each with size (1/2 M×1/2 N).

5- Embed the coefficient of remainder matrix R in four of the eight subspaces

computed in step 4 (by replacing). Matrix R needs four subspaces because its size is (M×N).

6- Compute inverse DWT to reconstruct the image matrix from its subspaces. This can be done by reconstructing each of subspaces ('h' and 'v') from second level subspaces (a_h ,h_h , v_h , and d_h) and (a_v , h_v , v_v , and d_v) respectively. Then inverse DWT is done on 'a' 'h' ,'v', and 'd'. The resulting image is the stego_image that is the cover images within which the secret image is hidden.

4.2 The Procedure of the Reconstruction

The steps that reconstruct the secret image from the stego-image are:

1- Compute the DWT of the cover image to one level.

2- Extract the coefficients of root matrix T from the details subspace in which these coefficients are embedded, such as subspace 'd'. .

3- Compute the DWT for each of the remaining two details subspaces ('h' and 'v'). It resulting four subspaces for 'h' labeled (a_h ,h_h , v_h , and d_h), and four subspaces for 'v' labeled (a_v , h_v , v_v , and d_v).

4- Extract the coefficients of remainder matrix R from the subspaces in which these coefficients are placed.

5- Regenerate the elements of the secret image matrix by applying Equation 1 on the coefficients of matrices T and R.

5. The Results

The procedure of proposed hiding system is applied on several cover images and secret images arranged in three groups shown Figures 4, Figures 5 and Figures 6. Each group contains a cover image of size (512×512) pixels and secret image of size (256×256).The secret image is to be hidden in the cover image of the same group.

After the hiding steps are applied, the resulting stego-image of group1 is shown in Figure 7a. This image is closely related to the cover image (shown in Figure 4b) and does not show any details of the secret image that is hidden in which. The stego_images of group2 and group3 are shown in Figure 8a and Figure 9a respectively.

The reconstruction steps are applied on the three stego_images. The reconstructed images (shown in Figure 7b, Figure 8b and Figure 9b) are identical to the secret images.

Image energy is used to measure the similarity between the cover image and the stego_image resulting from hiding a secret image within which. Energy is also used to measure the similarity of the original and reconstructed secret image. Table1 listing the energies of cover image, stego_image, secret image, and reconstructed image and for the three groups.

The Mean Square Error (MSE) is used as metric to measure the distortion between the resulting stego_image and the original cover image. Table2 lists the MSE for the three used groups.

The equation that evaluating the energy is [10]:

$$E = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} I^2(r,c) \qquad \ldots (2)$$

And the MSE is evaluated as:

$$MSE = \frac{1}{M \times N} \sum_{r=1}^{N} \sum_{c=1}^{M} [I(r,c) - \bar{I}(r,c)]^2 \ldots (3)$$

Where:
E: is the energy, MSE: Mean Square Error
I: is the Image,
$\bar{I}$: is the stego_image,
And M×N: Is Image size in pixel.

6. Conclusions

The procedure of proposed hiding has a good algorithm to hide a gray scale image in other gray scale image. It produces a stego_image that is close to the cover image so that outside observer cannot recognize that the hidden (secret) image is present.

The proposed system has many keys of security. The first is the type of wavelet that is used for DWT such as (Haar , Daubechies, Coifman, symlets, or Morlet). The second is that the type of wavelet that is used for the second level may be different from that used for the first level DWT. The third is that the representation of the secrete image elements in other form (root and remainder) rather than the use of the elements themselves as with other hiding systems that use element values themselves[2,9,10]. The fourth is that the first level subspaces in which the root matrix coefficients are placed can be selected as one of three details subspaces 'h' ,'v', or 'd'. And the fifth key of security is that any four of the eight subspaces (a_h ,h_h ,v_h , d_h ,a_v ,h_v ,v_v , andd_v) can be used to embed the coefficients of the remainder matrix R.

7. References

[1] S. Li and X. Zheng, “Cryptanalysis of A Chaotic Image Encryption Methods ", Institute of Image Processing, School of Electronics and Information Engineering, Jiaotong University, China, 2002.

[2] H.T Haider, "Evaluation of Information Hiding for Still Images", MSc Thesis, Electronic Engineering Department , College of Engineering, University of Baghdad, 2003.

[3] S. Katzenbeissers and F. A. Petitcolas, "Information Hiding Techniques for Steganography and Digital Water Marking", Artech House, London, 2000.

[4] S. Boukhonine, "Cryptography: A Security Tool of the Information Age", 2002.

URL:http://www.phoas.com/proucts/crypto /crypto data.Pdf

[5] F. N. Jhonson, Z. Duric, S Jajodia, "Information Hiding: Steganography and Water Marking Attacks and Counter Measured”, Klwer Academic Publishers, 2001 .

[6] Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS International Journal of Computer Science and Network Security, vol. 7 no. 4, April 2007.

[7] H. Gou and M. Wu, "Data Hiding in Curves with Applications to Map Fingerprinting,", IEEE Trans. on Signal Processing, Special Issue on Secure Media, vol. 53, no. 10, pp. 3988-4005, Oct. 2005.

[8] T. E. Lin and J. E. Delp, "A Review of Data Hiding in Digital Images", Purdue University, Wast Lafayehe, India, 1999.

URL:http://www.Ece.Purdue.Edu/~ace.Pdf
.

[9] Min Wu, and Bede Liu, “Data Hiding in Binary Image for Authentication and Annotation”, IEEE Transaction on Multimedia, vol. 6 no. 4, pp 528-538, August 2004.

[10] H. H. Al _Obaidy, "Encryption Using Wavelet Coded Image Data", MSc Thesis, Computer Engineering Department, College of Engineering, University of Basrah, 2004.

[11] R Polikar, "The Wavelet Tutorial", Electrical and Computer Engineering Department, Rowan University, 1996.

URL:http://www.engineering.rowan.edu/p olikar/WAVELETS/WTtutorial.ht ml .

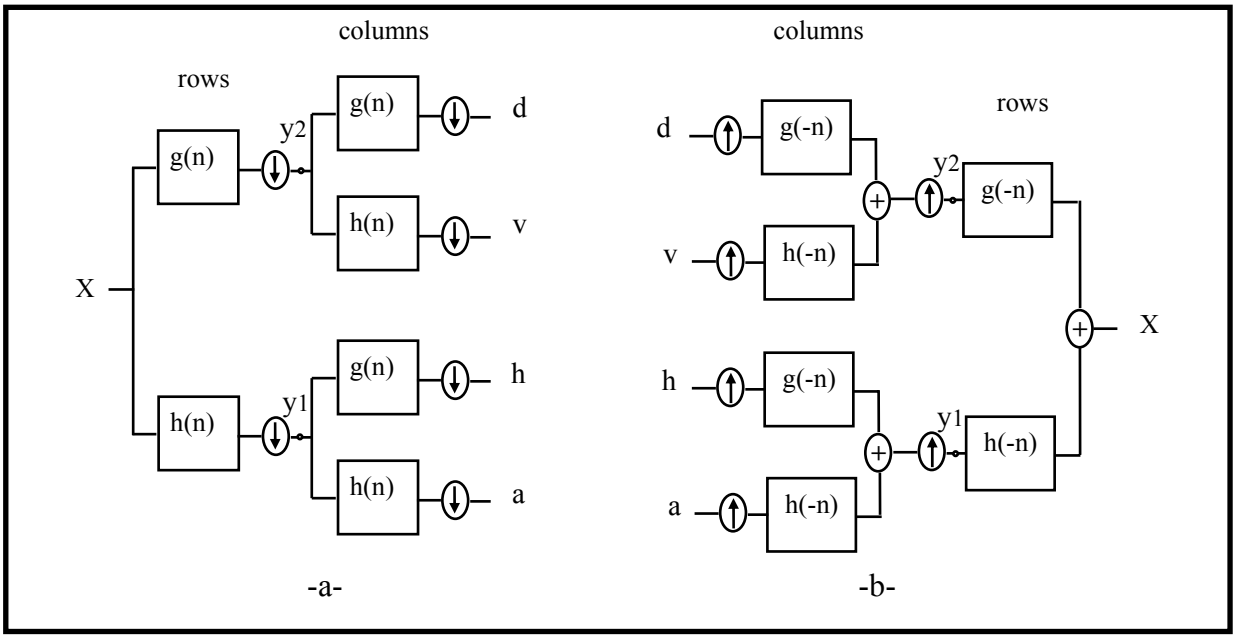

Figure 1 :1_Level 2D_DWT (a)Decomposition , (b)Reconstruction

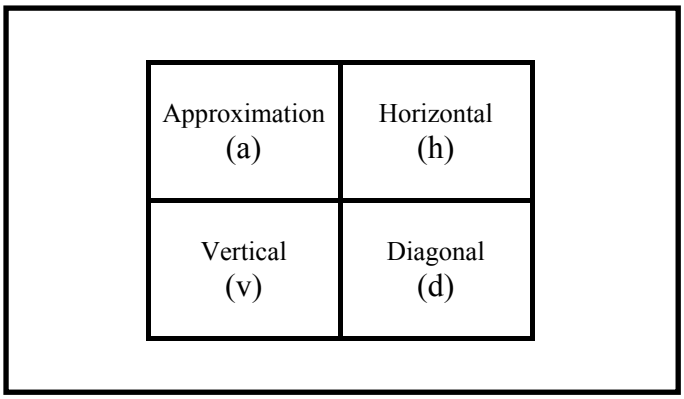

Figure 2: 1_Level 2D_DWT representation of an image

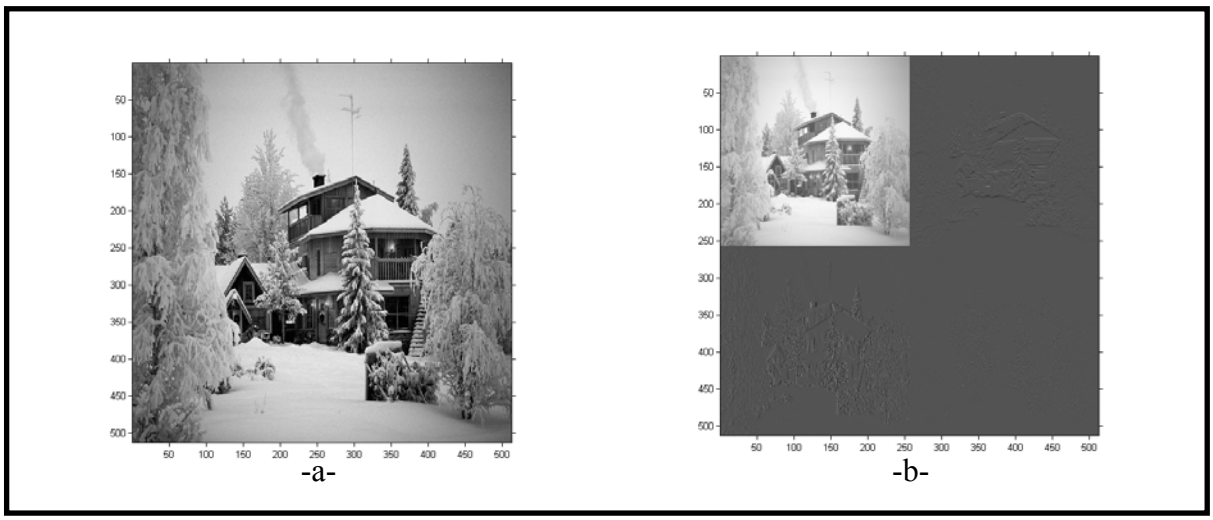

Figure 3: An image with its DWT (a)The image, (b)Its 1_Level 2D_ DWT

-a- -b-

Figure 4: Group 1 secret and cover images (a)Secret image, (b)Cover image

-a- -b-

Figure 5: Group 2 secret and cover images (a)Secret image, (b)Cover image

-a- -b-

Figure 6: Group 3 secret and cover images (a)Secret image, (b)Cover image

-a- -b-

Figure 7: Group1 stego_image and reconstructed image
(a) Stego_image, (b)Reconstructed image

-a- -b-

Figure 8: Group2 stego_image and reconstructed image
(a) Stego_image, (b)Reconstructed image

-a- -b-

Figure 9: Group3 stego_image and reconstructed image
(a) Stego_image, (b)Reconstructed image

Table 1

Group	Cover Image Energy	Stego_Image Energy	Secret Image Energy	Reconstrected Image Energy
Group 1	0.28430493523096	0.28407048214773	0.31798598767973	0.31798598767973
Group 2	0.30371194955504	0.30330747206198	0.58138671171014	0.58138671171014
Group 3	0.37421792775006	0.37210064000316	0.61221244392551	0.61221244392551

Table 2

Group	Mean Square Error (MSE) between Cover Image and Stego_Image
Group 1	0.00029480948442
Group 2	0.00146046991579
Group 3	0.00214235885837