

Modifying Randomized Transform Image Steganography Using IDWT

Maisa'a Abid Ali Kodher: lec

Bushra Abdul-Kareem Abdul-Azeez: Ass.Lec

Computer Sciences

Medical Institute of Technology/Baghdad

University of Technology /Iraqi

Foundation of Technical education /Iraq

maisaa_ali2007@yahoo.com

Bushra.a_azeez@yahoo.com

Abstract:

The rapid developments in communications system and networks of the internet have led to propose a new algorithm to hide the image over the internet network. The new approach hides the image or text or voice or message to be transmitted. This message is hidden within image with the use of a secret key. The secret key is a fusion of two images after they are compressed in 2D discrete wavelet transform for the second level (L2) and third level (L3). After merge of the two images, the inverse discrete wavelet transform is considered as a final result of secret key with the cover image to hide the original image as well as the data transferred under this image.

The results obtained in this proposed algorithm depends on the hidden image and the secret key is generated that it can restore the original image after receipt without losing any information of image by recipient in the network.

Key word:, Steganography, Transform dynamically random image , Image fusion, Inverse discrete wavelet transform, Secret key.

1-Introduction:

Steganography is the art and science of writing hidden message in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity.

The term steganography refers to the art of covered communication. By implementation of steganography, it is possible for sender to send a secret message to the receiver in such a way that no-one else will know that the message exists. The message is embedded within another object known as a cover work, by tweaking its properties. With the rapid development of the internet technologies, digital media need to be transmitted conveniently over the network. Attacks, unauthorized access of the information over the network have become greater issues nowadays. The main purpose of steganography is to hide the fact of communication. The sender embeds a message into digital media where only receiver can extract this message.

2-Steganography:

Steganography is the science of hiding information by embedding the hidden (secret) message within a cover media such as an image, audio, and video carrier file. In such a way that the hidden information cannot be easily perceived to exist for the unintended recipients of the cover media [1] [4]. Steganography hides the fact that the communication exists. Steganography hiding model takes advantage of the redundancy of data that there could be no perceptible change to the cover media, see Fig. (1).

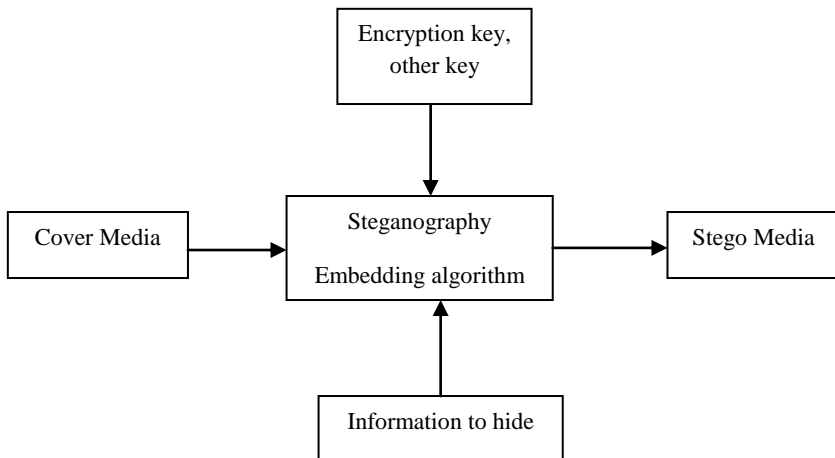


Fig. (1) Hiding Model

In the steganography extraction model, the extraction process should be possible without the cover, the extraction algorithm can also be applied to any cover, whether or not it contains a secret message. In the latter case, the output of the extraction process is considered as a "natural randomness" of the cover [1] [4], see Fig. (2)

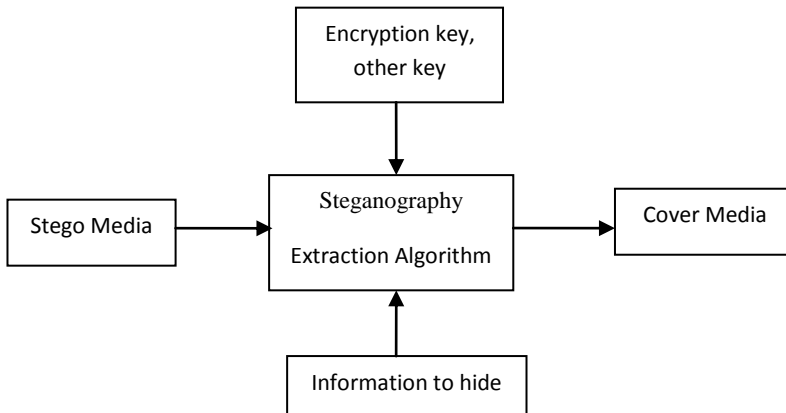


Fig. (2) Extraction Model

3-Secret Key Steganography:

A secret key steganography system is similar to asymmetric cipher, where the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message [3]. Anyone who doesn't know the secret key should not be able to obtain evidence of the encoded information [2].

The secret key steganography can be defined as the quintuple (C, M, K, DK, EK)

where

C: the set of possible covers.

M: the set of secret message.

K: the set of secret keys.

$E_k: C \times M \times K \rightarrow C$

With the property that

$DK(EK(c,m,k),k)=m$ for all $m \in$

$M, c \in C$ and $k \in K$, see Fig. (3)

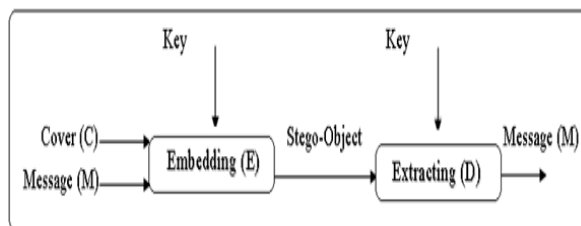


Fig. (3) Secret Key Steganography.

4-Steganographic Techniques :

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or message in image in such a manner that the alterations made to the image are perceptually indiscernible [4] [5]. Common approaches include Fig. (4).

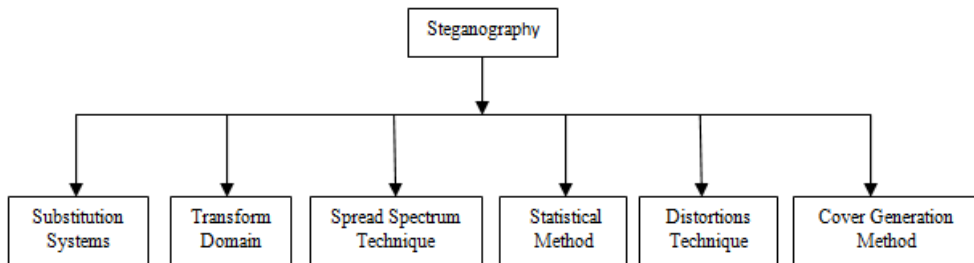


Fig. (4) SteganographicTechniques.

5-Image Fusion:

Image fusion is the process that combines information from multiple images of the same scene. These images may be captured from different sensors, acquired at different times, or having different spatial and spectral characteristics. The objective of the image fusion is to retain the most desirable characteristics of each image. With the availability of multisensor data in many fields, image fusion has been receiving increasing attention in the researches for a wide spectrum of applications [6].

Image fusion schemes are similar to Discrete Wavelet Transform (DWT) fusion schemes which is the basic and simplest transform among numerous multiscale transforms and other types of wavelet based fusion schemes are usually similar to the DWT fusion scheme [6].

6-Image Steganography:

As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist, most of which are for specific applications. For these different image file formats, different steganographic algorithms exist [7].

To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels [7]. Most images on the Internet consist of a rectangular map of the image's pixels (represented as bits) where each pixel has location and colour. These pixels are displayed horizontally-row by row.

The number of bits in a colour scheme, called the bit depth, refers to the number of bits used for each pixel. The smallest bit depth in current colour schemes is 8, meaning that there are 8 bits used to describe the colour of each pixel [7].

7-Proposed Algorithm:

First Step:

The original color image with fixed dimensions 96×96 is used as a cover under which the image will be hidden, shown in Fig (5). The original image is divided into 9 numbers of blocks of each of which is defined. In other words the original image is divided into nine blocks each of which has dimension of 32 pixels as shown in Fig (6-a,b). After image division, random points are taken from the image using dynamic random generating function. The function takes random points from the image every time, that is, it takes nine points from each block, these point have color values of the original image consisting of (X,Y), which have values in RGB. These random points generate one– dimensional matrix as shown in Fig. (6-c).

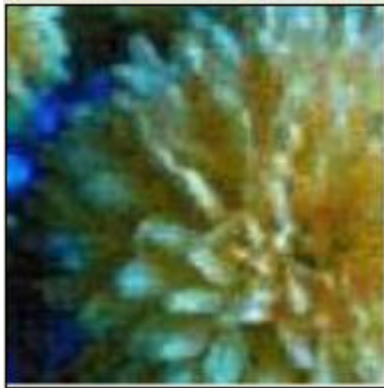


Fig. (5)Original Image 96×96

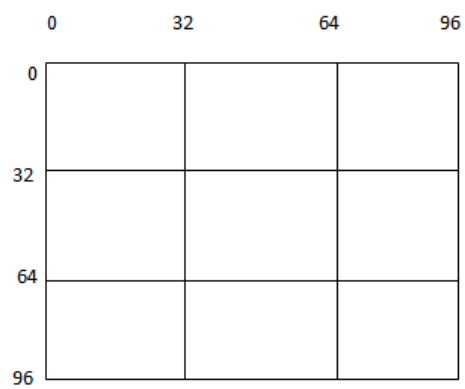


Fig. (6-a) Block of Original Image 96×96

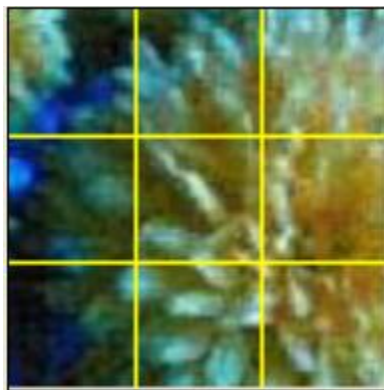


Fig. (6-b) Block of Original Image

Random point of original image $X=RGB$, $Y=RGB$

Random point matrix one – dimension

RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB
X1,Y1	X2,Y2	X3,Y3	X4,Y4	X5,Y5	X6,Y6	X7,Y7	X8,Y8	X9,Y9

RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB	RGB
5,12	38,0	82,23	17,43	31,46	94,83	71,13	88,50	90,71



Fig. (6-c) Image Random Point

Second Step:

Generate a secret key to hide random image. The key consists of two images compressed into the same size of 45×45 but with different data and information. Each image is compressed separately from other manner DWT at the second level (L2) or third level (L3) as well as for both of the two images shown in Fig. (7-a, b). After that the two images are split into L2 or L3 and merged to convert image fusion. And the final product to integrate the images produces an image IDWT shown in Fig. (8-a, b) L2 and L3. The resulting final image is as a secret key used to hide the image to be sent in a random way in a message or voice or text, etc.

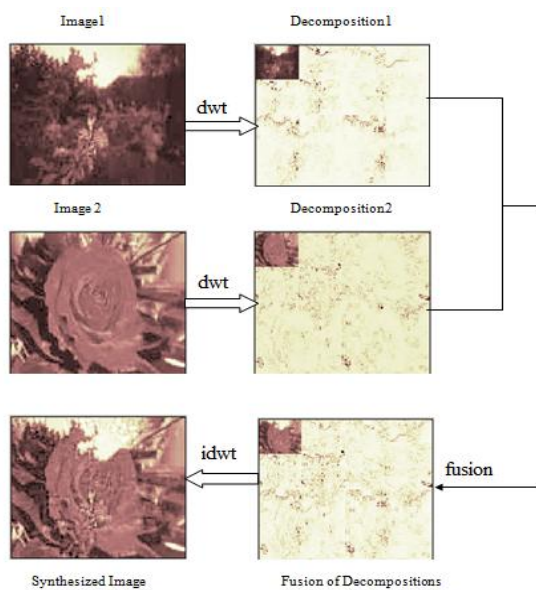


Fig (7-a) Compressed Image DWT L2

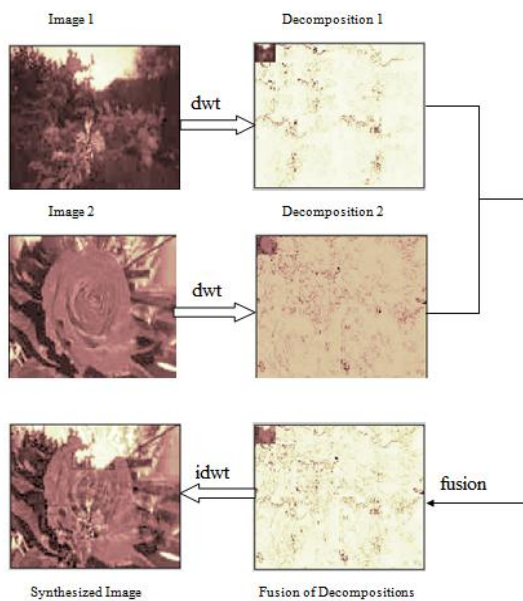


Fig. (7-b) Compressed Image DWT L3

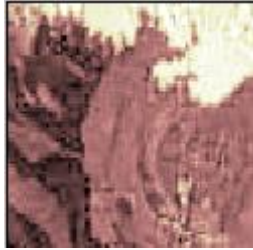


Fig. (8-a) Image IDWT L2



Fig. (8-b) Image IDWT L3

Third Step:

Transform original image of 96×96 to stego image using the function of multiply random image (cover) with inverse discrete wavelet transform in L2 and L3. After passing the function, it becomes the stego image in small size which is the same size as random image shown in Fig. (9-a, b).

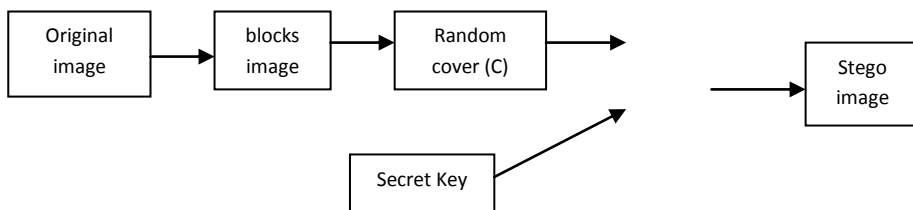


Fig. (9- a) Transform of original Image to Stego Image

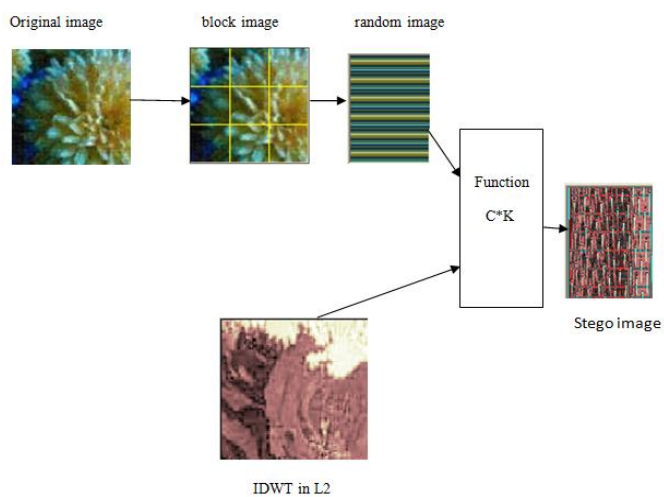
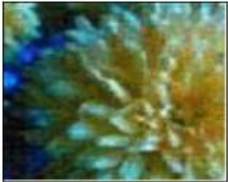
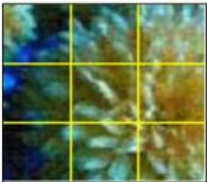








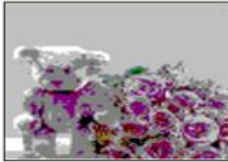
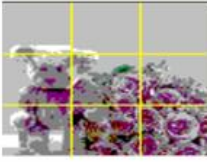
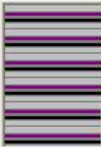





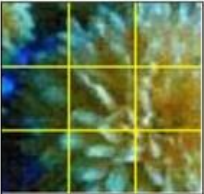













Fig. (9-b) Transform of original Image to Stego Image

9.1- Algorithm

<i>Process:</i>
Input: Original image.
Output: Stego image.
Initial:
A = Load Original Image 96×96.
B = Load Block Image 3×3.
C = Load Random Image (Cover Image) 1-D.
D = Load Inverse Discrete Wavelet Transform image (Key Secret) 45×45.
E = Stego Image.
Step 1: Divide original image 3×3 to equal 9 blocks of original image in B.
Step 2: Find cover image from elements of matrix one dimension random from each block of image in C.
Step 3: Selection two image in the same size.
Step 4: Image compression in DWT in L2 or L3.
Step 5: Merge two DWT image in L2 or L3 in fusion image.
Step 6: Find key secret from inverse discrete wavelet transform image in L2 or L3 in D.
Step 7: Multiple 1-D cover image with inverse discrete wavelet transform image in L2 or L3 in D.
Step 8: Result (Put the result Stego Image in E).

9.2- Test of the Result:

Original Image 96×96	Block Image 96×96	Random Image 1-D	No. of Level	IDWT 2-D	Stego Image
			1 L2		
			2 L2		
			3 L2		

Original Image 96×96	Block Image 96×96	Random Image 1-D	No. of Level	IDWT 2-D	Stego Image
			1 L3		
			2 L3		
			3 L3		

9.3- Test of Distortion and Correlation:

No. of image	MAE	MSE	RMAE	PSNR	SNR	Correlation
Stego 1 L2	-103.729	16296.85	127.6591	1.4267	1.5952	2112.1762
Stego 2 L2	-108.221	16649.77	129.034	1.4015	1.054	2164.343
Stego 3 L2	-108.019	17672.94	132.939	1.3320	1.0227	2082.3844
Stego 1 L3	-104.245	16385.39	128.005	1.4200	1.4482	2129.8265
Stego 2 L2	-100.199	14954.06	122.286	1.5290	1.9300	2091.4108
Stego 3 L3	-98.3400	15657.68	125.130	1.4741	2.0163	2134.0462

10-Conclusions:

This research provides a good and efficient method for image steganography by reducing image size for transmission of image and it converting to block and take in point and sending it to the destination in a safe manner across internet network in a secured way.

In this system image data are in static size and transformed to a set of image blocks point's pixel are selected from the data on static image which is random because it is small. Secret key is selected from data image of static size then the secret key becomes very robust in hiding image.

The steganography technique presented in this research is very robust hiding original data of image, when sent across network depending on IDWT static randomized and secret key.

Randomization technique transform is compared with LSB and DCT, can it return original image, but LSB and DCT cannot return original image.

This state indicates the system is very efficient because it is keeping the image without loss of any information during transmission.

11- Reference:

1. Kanchan Patil, Ravindra Gupta, and Gajendra Singh," Digital Image Steganalysis Schemes for Breaking", International Conference on Advances in Communication and Computing Technologies (ICACACT), 2012.
2. Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi, " Main Fundamentals for steganography", Journal oF Computering, vol 2, No 3 MARCH 2010.
3. Hamid.A.Jalab, A.A Zaidan, B.B Zaidan, "New Design for Information Hiding With in Steganography Using Distortion Techniques", International Journal of Engineering and Technology (IJET)), Vol 2, No. 1, 1793-8236, Feb (2010).
4. Eric Cole, and Ronald D. Krutz, "Hiding in Plain Sight: Steganography and the Art of Covert Communication", Wiley publishing, Inc, 2003.
5. R.Chanderamouli, and Nasir Mamon, "Analysis of LSB based image steganography techniques", 2001 IEEE.
6. V.P. Sawant," Fusion Algorithm for Images based on Discrete Multi-wavelet Transform". IOSR-JVSP, Volume 2, Issue 3 (May. – Jun. 2013), PP 22-27 e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197.

7. M. Sitaram Prasad, S. Naganjaneyulu, CH. Gopikrishna .C. and Agaraju , "A novel information hiding technique for security by using image steganography". Journal of Theoretical and Applied Information Technology © 2005 - 2009 JATIT.

تعديل اخفاء التحويل العشوائي للصورة باستخدام معكوس تحويل الموجة الثنائية المتقطعة

م. ميساء عبد علي خضر
قسم علوم الحاسوب
الجامعة التكنولوجية\العراق

م.م. بشرى عبد الكريم عبد العزيز
المعهد الطبي التقني \
هيئة التعليم التقني

الخلاصة:

أدت التطورات السريعة في نظم الاتصالات وشبكة الإنترنت لاقتراح خوارزمية جديدة لإخفاء الصورة عبرالانترنت. يتم إخفاء هذه الرسالة داخل صورة باستخدام مفتاح سري. المفتاح السري هو مزيج صورتين بعد ضغطها في موجة متقطعة ثنائية الابعاد 2D ثم تحويلها للمستوى الثاني (L2) والمستوى الثالث (L3). بعد دمج الصورتين يُعتمد معكوس تحويل الموجات الثنائية المتقطعة النتيجة النهائية للمفتاح السري مع صورة الغلاف لإخفاء الصورة الأصلية فضلا عن البيانات التي تم نقلها بموجب هذه الصورة.

تعتمد النتائج التي تم الحصول عليها في هذه الخوارزمية المقترحة على الصورة المخفية وتوليد المفتاح السري الذي يمكن عن طريقه اعادة الصورة الاصلية بعد استلامها من دون ان يفقد المستلم البيانات في الشبكة.

مفتاح الكلمات: الاخفاء ، التحويل الديناميكي العشوائي للصورة، انشطار الصورة ، معكوس تحويل الموجة الثنائية المتقطعة ، المفتاح السري.