A New Algorithm for a Steganography System

Dr. Atheer Alaa Sabri
Electrical Engineering Department, University of Technology/ Baghdad.
Email :atheeralaa@yahoo.com
Marwa Jaleel Mohsin
Electrical Engineering Department, University of Technology/ Baghdad.
Email:Marwa.jaleel@yahoo.com

Received on: 24/12/2014 & Accepted on: 11/6/2015

Abstract

Steganography is the workmanship and study of concealing mystery information to provide a safe communication between two parties. This paper, displays other steganographic algorithms for implanting encoded secret image in grayscale and color images to give abnormal state security of information for correspondence over unsecured channels. The proposed algorithms first analyze the secret image using 1level -DWT and SLT respectively. It will be then encrypted the low frequency components of the secret image only using AES method and then embedded in the insensitive mid and high sub-bands gotten from the cover image in the wake of applying 2level- DWT and SLT on it, The embedding method used in this paper is LSB, the resulting image called stego-image form different algorithms are then compared. .By using the proposed algorithms the capacity of the hidden secret data and stego image quality are improved. The embedding image reaches to half the size of cover image at same time PSNR reach to 62 dB and MSE about 0.36. The language used for testing the algorithms is MATLAB 2013a.
Key words: Steganography, Cover image, Stego-image, Wavelet Transform.

خوارزمية جديدة لنظام أخفاء المعلومات

الخلاصة:

الكتابة المخفية هو فن وعلم إخفاء البيانات لتوفير اتصال آمن بين طرفين. هذه الورقة ،تقدم خوارزمية جديدة لتضمين صورة مشفرة سرية في صور ملونه وغير ملونة لتوفير مستوى عالي من أمن البيانات للاتصال عبر قنوات غير آمنة. تستند الخوارزمية المقترحة على تنفيذ مستوى واحد من تحويل الموجية وتحويل ال slatlet للصورة السرية على التوالي, ثم تشفير مكون التردد المنخفض فقط لها بطريقة AES وبعد ذلك تضمن في مكونات الترددات المتوسطه والعاليه من صورة الغطاء بعد تحليلها بأستخدام مستويين من تحويل المويجة والSLT. طريقة التضمين المستخدمة في هذه االورقة هو البت الاقل اهمية , صورة الستيكو الناتجة من مختلف الخوارزميات يتم مقارنتها فيما بعد . الصورةالمضمنة تصل إلى نصف حجم صورة الغلاف في نفس الوقت PSNR تصل إلى 62 ديسيبل وMSE حوالي 0,36 اللغة المستخدمة لاختبار الخوارزميات هي MATLAB R2013a.

INTRODUCTION

Steganography is the strategy of concealing secret data in a communication channel in such a way, that every existence of the data is covered. So, no one from the planned recipient knows the existence of the message [1]. The term of "steganography" is made up of two Greek word “steganos” means 'secret ' and

https://doi.org/10.30684/etj.2015.108835
2412-0758/University of Technology-Iraq, Baghdad, Iraq

"graphy" which means ' writing', Steganography means literally" covered writing." [2].

The essential guideline lies in implanting the secret message into a cover media to guarantee that a unintended gathering won't be mindful of the presence of the installed secret data in stego-media, Therefore, steganography is the methodology of concealing secret information inside public data [3]. Figure (1) demonstrates the square chart of a basic steganographic framework.

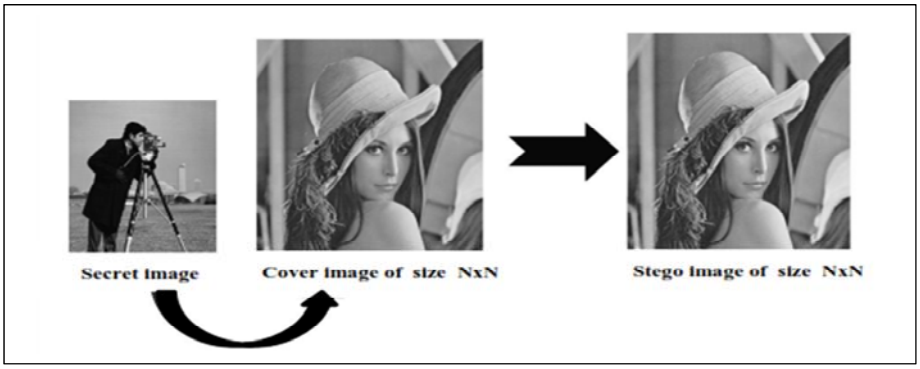


Figure (1) the block diagram of a basic steganographic framework [4].

The Basic Model of Steganographic System:

Cover or host- object(C): It is defined as the original object into which the obliged data is installed. It is likewise termed as carrier object.

Stego-object(S): Alludes to the object which is conveying a concealed message.

Payload: is the measure of data that can be put away in the cover or host object. Regularly, the more noteworthy payload is the more noteworthy danger of discovery [5].

Key (K): is an additional secret data which may be needed in embedding data in a cover object and extracting this data from stego object [5].

Various types of steganography:

Almost all digital media or file formats can be utilized for steganography, but the formats that are more suitable are those with a high level of redundancy [6]. Figure (2) demonstrates the four primary classes of file formats that can be utilized for steganography.

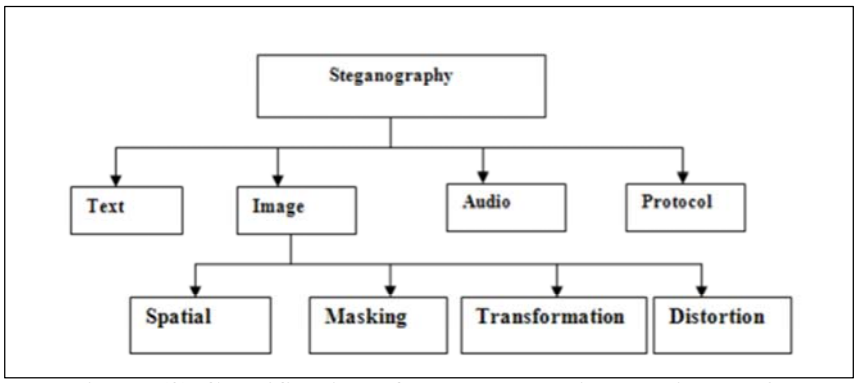


Figure (2) Classification of steganographic techniques [6].

Steganography measurement:

As shown in Figure (3) , important steganography measurements are as follow:

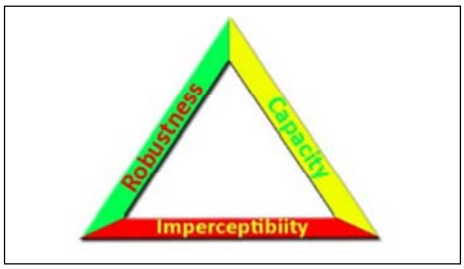


Figure (3) Measurement triangular of steganography [7]

Capacity is the most extreme measure of secret data that can be shrouded or installed in the cover medium .Capacity value relies on upon both embedding function and cover properties [8].

Imperceptibility: Is the powerlessness of an aggressor to recognize the cover object and the steganographic object. Stego object ought not to have imperative perceptual artifact. The higher devotion of stego object, will give the best imperceptibility. This property would be fulfilled if distinction of resultant stego object is not discernable from unique cover for superintendent. There are different assessment methods for diverse steganography sorts yet the principle assessment strategy is PSNR [9]**.**

Robustness: It alludes to the measure of adjustment the stego medium can withstand before a foe can crush the concealed data. Strength is a property of harness of eliminating secret data from a stego file [10].

Essential sorts of stego frameworks:

Three essential sorts of Stego frameworks are accessible:

- Pure Stego frameworks - no key is utilized.
- Secret-key Stego frameworks - mystery key is utilized.
- Public-key Stego frameworks - open key is use

Image steganography:

A image steganographic plan is one sort of steganographic frameworks, where the secret message is covered up in a digital image with some concealing system. Digital images make good stego-objects because changes in them are imperceptible to human eyes. In particular, the human eye has a very little sensitivity to changes in brightness across an image. Finally, the omnipresence of images on the internet makes them an excellent choice for cover objects in covert communications [11]. Figure (4) demonstrates the general image steganography system.

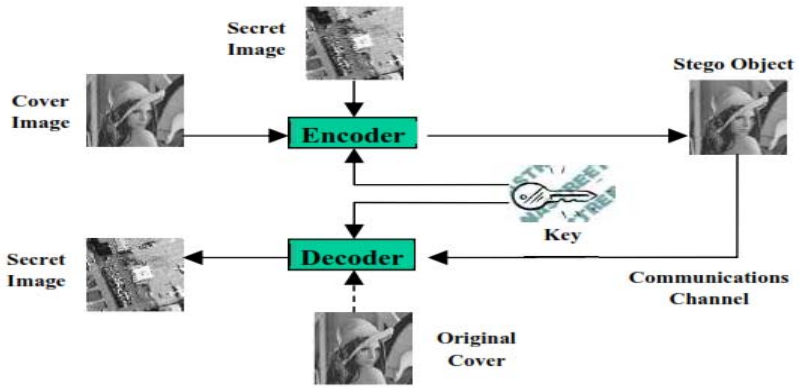


Figure (4) The general image steganography system[11]

Image steganography methods can be categorized into two groups:
The first one is spatial domain and the second is frequency domain. In the first group, the secret message is embedded directly in a lot of pixels; the most widely used technique to hide data on spatial domain image steganography is LSB. While in the second group, at first the images are converted to frequency domain and then the secret message is inserted in the transform coefficients. The frequency domain techniques are viewed as more vigorous to attacks than spatial domain techniques. There are many type of transforms used to map a signal into the frequency domain like: Discrete Wavelet Transform (DWT), Wavelet Packet Transform (WPT), Multiwavelet Transform (MWT), and Slantlet Transform (ST) [11].

Discrete wavelet Transform DWT:

The discrete wavelet transform (DWT) has become one of the most used methods for signal analysis and the applications of image processing. The discrete wavelet transform (DWT) performs a multiresolution signal analysis which has movable region in both time and frequency domains [12]. The basic one-dimension (DWT) can be acknowledged by convolution utilizing two FIR (Finite Impulse Response) filters, one low pass filter (LPF) and one high pass filter (HPF)[13]. Figure (5) shows a 1-DDWT:

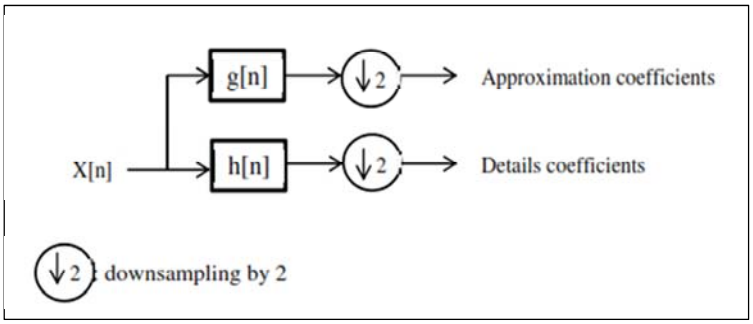


Figure (5) Block diagram of filter analysis[14].

The Haar wavelet transform is one of the most punctual illustrations of what is currently called a compact support, dyadic or orthonormal wavelet transform [12]. In Haar-DWT the low frequency wavelet coefficients are created by averaging the two pixel values and high frequency coefficients are generated by taking 50% of the difference of the same two pixels. The DWT filter bank that dissects the input signal is called analysis filter bank, and filter bank that recover the original input signal is called synthesis filter bank [13]. Image-processing applications require two-dimensional implementation of wavelet transform. For images, given by a matrix of size nxm, the processes of analysis and synthesis are the same as for one dimensional signals but applied first for rows and then for columns of that matrix[14]. Figure (6) shows 2D-DWT for image. This structure creates three detailed sub-images (HL, HL, HH) relating to three different directional-orientations (Horizontal, Vertical and Diagonal) and a lower resolution sub-image LL. The filterbank structure can be iterated in a comparable way on the LL channel to provide multilevel decomposition [15].

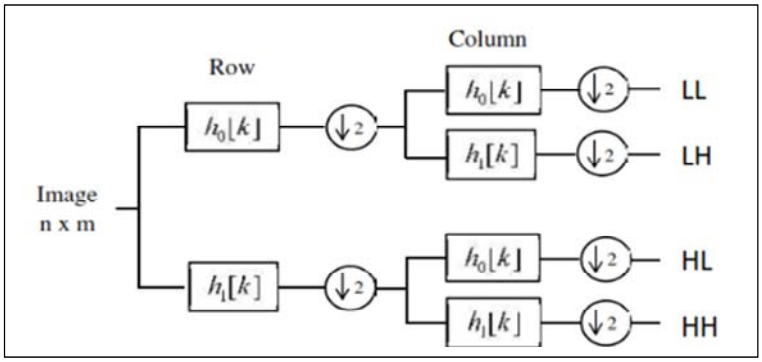


Figure (6) Single level analysis filterbank for 2-D DWT[15].

The hierarchy of multilevel decomposition of an image is illustrated in figure (7).

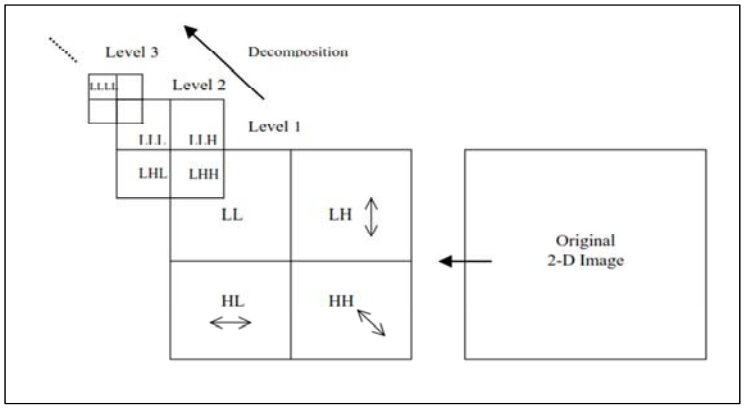


Figure (7) The hierarchy of Multilevel decomposition of an image with 2-D DWT[13]

The human eyes are not delicate to the little changes in the edges (high frequencies) and textures of an image but extremely touchy to the small changes in the smooth parts. This allows the secret message/image to be embedded at high frequency coefficients without being seen by the human eye [16] .

Slantlet Transformation (SLT):

Slantlet transform (SLT) has been recently proposed as a change over the established DWT. SLT is an equivalent form of the DWT implementation but gives better time-localization due to the shorter supports of component filters. The slantlet transform (SLT) is an orthogonal discrete wavelet transform (DWT) with two zero moments and with enhanced time localization [14]. SLT is a set of digital filters, which incorporates low pass filters (LPF), band pass filters (BPF) and high pass filters (HPF). Figure (8) shows comparison of 2-level iterated Db4 filterbank and 2-level slantlet filterbank.

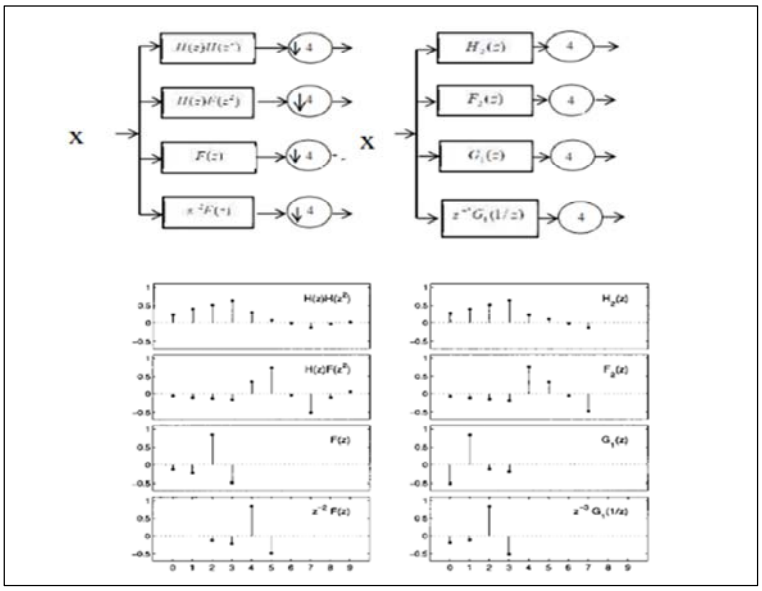


Figure (8) Comparison of level 2 iterated Db4 filterbank (left-hand side) and level 2 slantlet filterbank (right-hand side) [17].

The proposed algorithms:

The proposed algorithms in this paper is composed of two stages, first stage is encrypting the secret image (Cryptography) using AES (Advances encryption standard) method for increase the security of the proposed algorithm . And second stage is Steganography, to hide up a gray scale image inside a gray scale covered-image of size (512x512) pixels and a color image inside a color covered-image of size (512x512) pixels using DWT and SLT.

Ciphering the secret image:

The secret image decrypted using AES method as the following:

1-Dividing the secret image to(4 x 4) blocks of byte called State.

2- The SubBytes function, it is forward substitute byte transformation. Each individual byte of **State** is mapped into a new byte from X-box, as shown on figure (9).

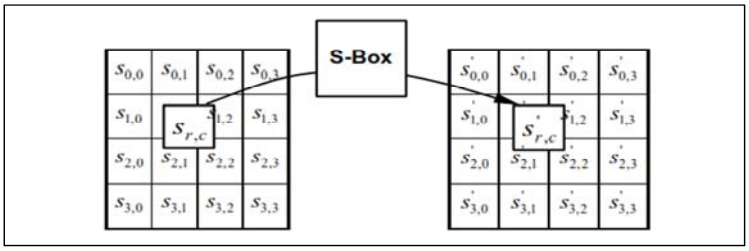


Figure (9) The SubBytes function[18]

3- The ShiftRows **function**, it is forward shift row transformation of the State. The first row of **State** is not altered. For the second row, a 1-byte circular left shift is performed. For the third row, a 2- byte circular left shift is performed. For the fourth row, a 3-byte circular left shift is performed, as shown on figure (10).

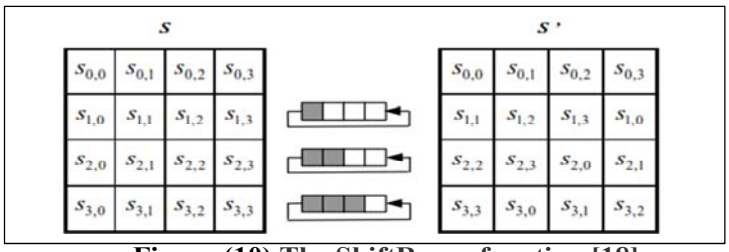


Figure (10) The ShiftRows function [18]

4-The MixColumns function , it is forward mix column transformation, operates on each column individually. Each byte of a column is mapped into a new value that is a function of all four bytes in that column. The figure below shows the MixColumns function.

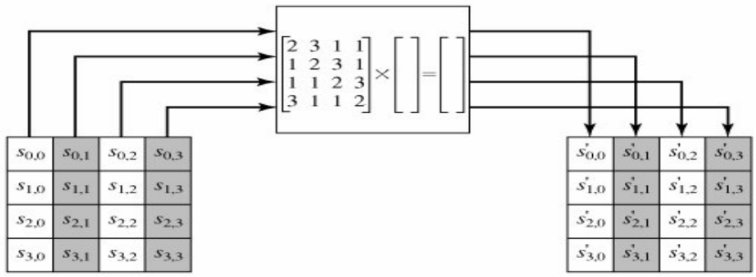


Figure (11) The MixColumns function [18]

5- In the AddRoundKey function **,** forward add round key transformation, the 128 bits of **State** are bitwise XORed with the 128 bits of the round key, the operation is viewed as a columnwise operation between the 4 bytes of a **State** column and one word of the round key. For more informations, see ref. [18].

The sending part :

Many stages and algorithms are proposed in the sending process to achieve the information-hiding goal. The proposed algorithm in sending part is illustrate in the figures (12) and (13) , these figures show the block diagram of whole suggested algorithms for steganography of gray and color images respectively.

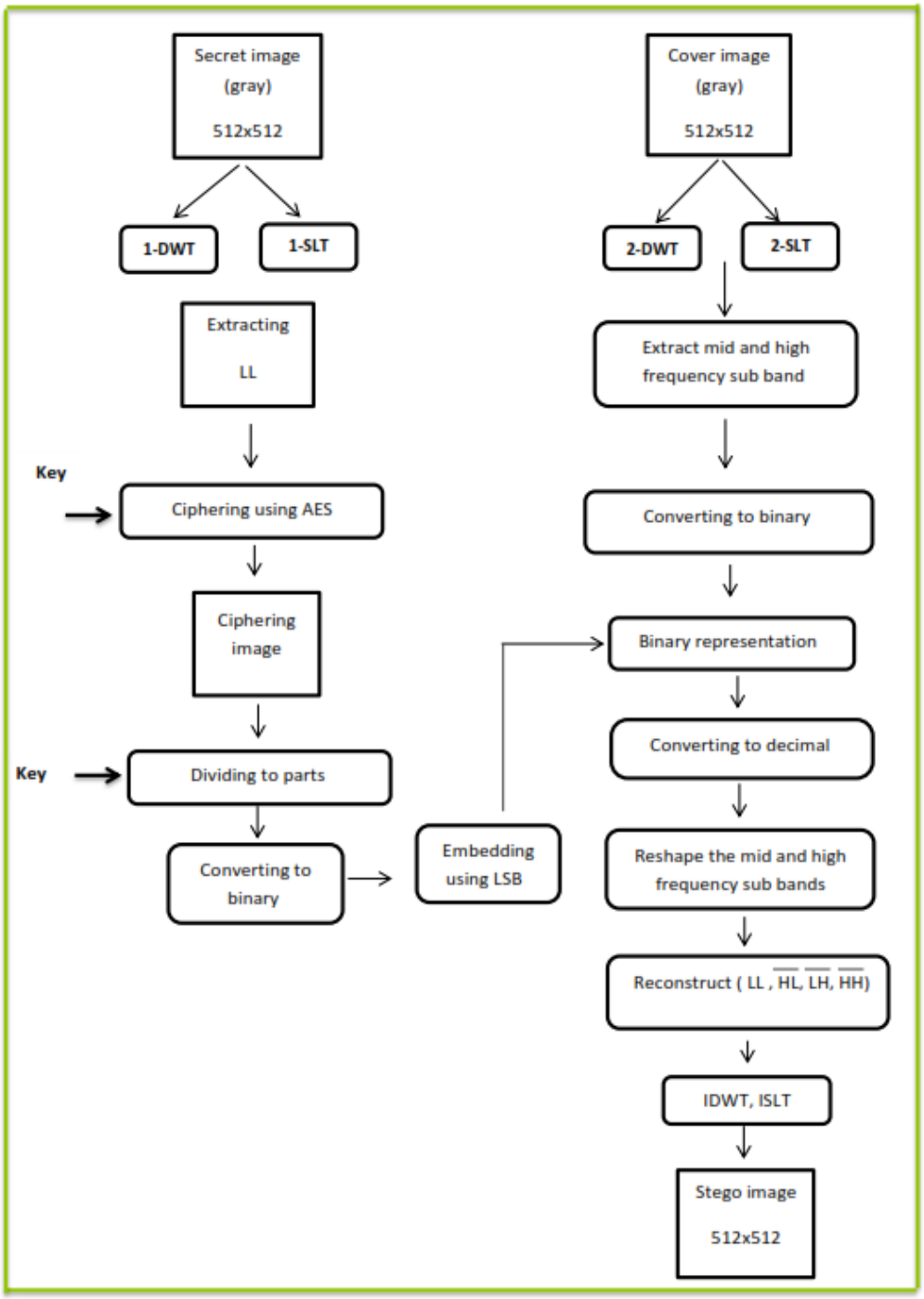


Figure (12) the block diagram of proposed algorithm for gray image in sending part

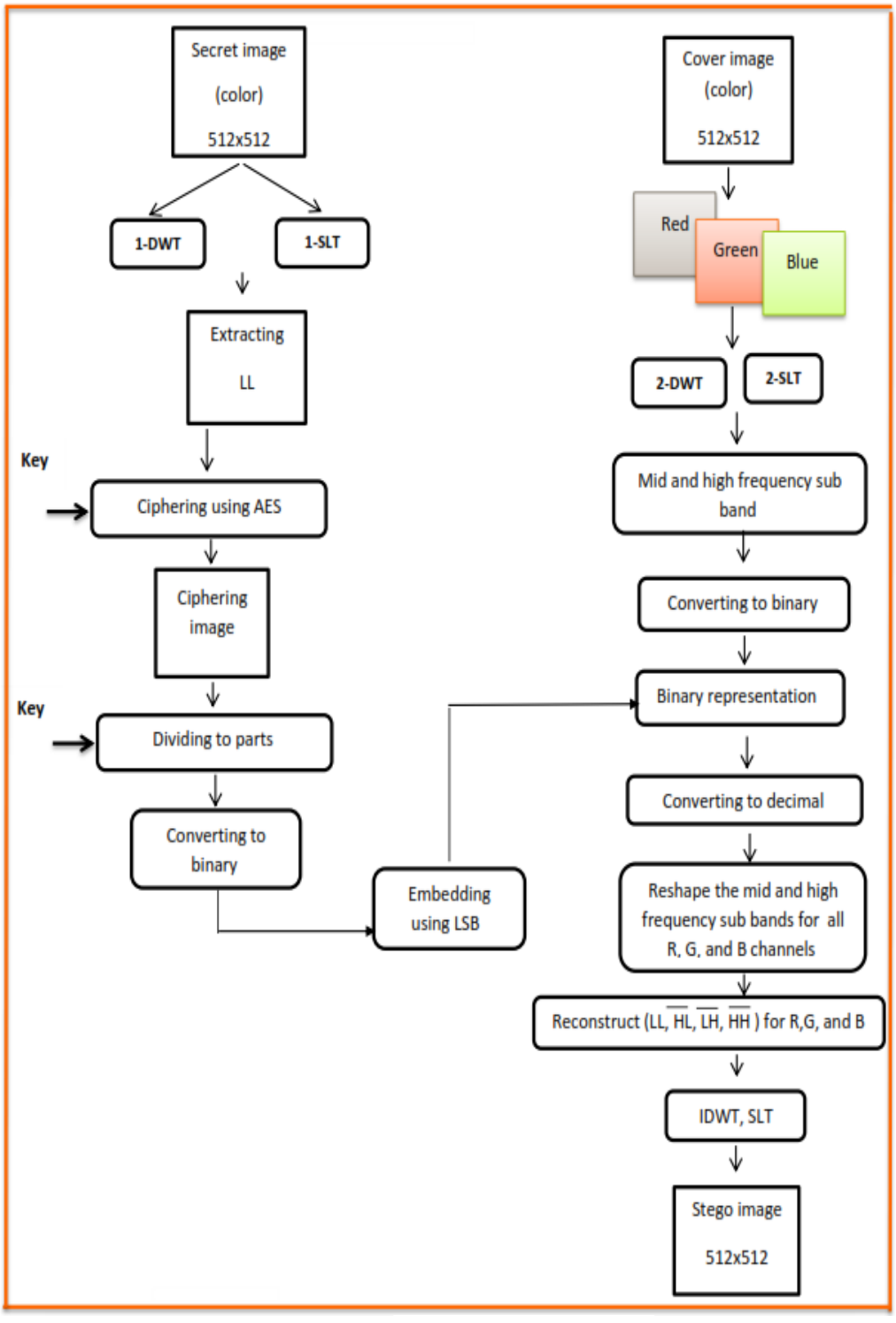


Figure (13) the block diagram of proposed algorithm for color image in sending part

1- The (512 × 512) gray scale cover image or color image are decomposed using 2-levels DWT. This results low, mid and high frequency sub bands. For color image, the cover image first decomposes to RGB channels and then applies 2-level DWT for each channel. The type of filter used is haar .
2- The mid and high frequency coefficients are extracted for embedding process.
3- The mid and high frequency coefficients are converted to a binary form.
4- Decomposing the (512 × 512) gray scale or color secret image using 1 -level DWT decomposition. This results low, mid and high frequency sub bands.
5- Only low frequency coefficient (LL) is extracted for ciphering process, because it approximates the original secret image and has less data.
6- After extracting the LL of the secret image, applying it to the ciphering process using AES method.
7-The ciphering image is divided into parts (row(R) X column (C)), which will be the the input key. The value of R & C will be the size (rows and columns) of each part part, one condition must require on the value of R & C, that is:
RxCx8 <= the size (rxc) of each band after applying the mentioned transformation
8- Each part is converted into bit form. The result data will be ((RxC) x 8).
9- Each part will be reshaped to (1 x (R x C x 8)).
10- Each bit of each part of ciphering secret image will be embedded (replaced) in the bit form of mid and high frequency coefficients of cover image using LSB method .In this paper 1, 2, and 3 LSB are used depending on how many data will be embedded in the chosen coefficients of cover image.
11-The mid and high frequency coefficients resulting from step (10) are converted to decimal values.
12-The mid and high frequency coefficients are then reshaped.
13- After all bits of the ciphered image are successfully embedded in the mid and high frequency coefficients, taking inverse transformation of the original low coefficient and the resultant coefficients from the embedding process(for color image after that reconstruct the three channels RGB), that resulting the stego image. As a result, the stego-image is completely similar to the original cover.
14-Step (4) is repeated but applying a 1-level SLT transform to secret image to show the effect on stego-image.
15- Then (LL) only is extracted for ciphering process.
16- Steps (6 to 13) are repeated.

The recipient part:

The recipient will certainly get the stego-image. The secret image will be extracted from stego image only, without need to cover image. In order to extract the embedded image exactly, only the following keys are required:

- The size of each part (R and C).
- The ciphering key (K).

The extracting process will be started. This can be done by:
1- After receiving the stego – image, for a gray image take a 2-levels DWT decomposition using the same filters used in the sender stage.

For a color image the received stego - image decomposed to RGB channels and then apply 2-level DWT are taken for each channel.

2- The mid and high frequency coefficients are extracting, and converted to bit forms.

3- The least bits (or second or third bits according to the Embedding process) from 1to (R x C) (that are used in the sender stage) are extracted.

4- The extracted data are reshaped to ((R x C)/8) rows and (8) columns.

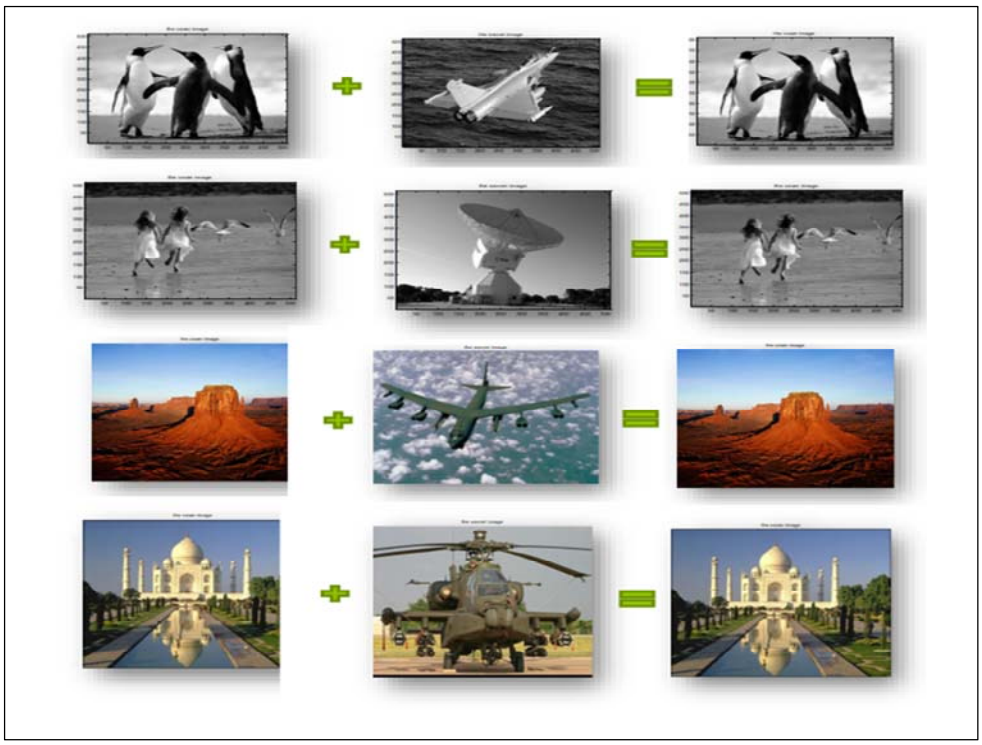
5- The result data are converted to decimal values.

6- The results data are reshaped again to parts (R, C). The same sizes of these parts are used in the sender.

7- Constructing the parts result the ciphering secret image. By entering the key, deciphering the image, result the secret image without any degradation. These resulting image will be LL of secret Image, Appling IDWT with (LH, HL, HH) set to zeros.

Experimental Results and Evaluation:

The language used for testing these algorithms is MATLA



Cover images Secret images Stego images

Figure (14) the cover ,secret ,and stego images

Many parameters are used to compare the proposed algorithms. These parameters are SNR, PSNR, MSE, and the capacity.

Signal to noise ratio (SNR) test:

It was utilized to quantify the bending between the cover image and the image containing information. A low SNR implies that the image has been significantly misshaped.

$$SNR = \frac{\sum_{x,y} Cov_{x,y}^{2}}{\sum_{x,y} \left(Cov_{x,y} - stego_{x,y}\right)^{2}} \quad ...(1)$$

Where

SNR is the signal to noise ratio, Cov ***x,y*** is a pixel in the original image with coordinates (x,y), and Stego***x,y*** is a pixel in the image containing data with coordinates (x,y). The signal to noise ratio is usually measured in decibels and converted using equation (2) .

$$SNR\ (dB) = 10\ \log_{10}(SNR) \quad \ldots(2)$$

Peak signal to noise ratio (PSNR) test:

As per the human visual framework, some measure of bending between the cover image and the adjusted one is permitted. PSNR is typically measured in *dB* [10].

$$PSNR = 20\log_{10}\frac{255}{\sqrt{MSE}} \quad \ldots(3)$$

Where

MSE is defined as the square of error between the stego and cover images. The mutilation in the image can be measured utilizing MSE [16].

$$MSE = \sum_{i=1}^{allpixels}\sum_{j=1}^{allpixels}\frac{(Cov(i,j) - stego(i,j))^{2}}{N * N} \quad \ldots(4)$$

$N * N$: is the image size.

Capacity:

It can be expressed as a percentage rate of the secret image from the full cover image size.

The simulation results:

Table (1) the results of proposed algorithm .

Secret image \ cover image 512x512 DWT				MSE	SNR	PSNR	No. of embedding bits (Kbyte)	Capacity%
Gray	DWT	Image1	128x128 (R=32&C=64)	0.0024	35.2592	74.3834	4.096	1.56%
			256x256 (R=32&C=128)	0.0090	32.3696	68.6109	16.384	6.25%
			512x512 (R=64&C=256)	0.0358	29.3623	62.6045	65.536	25%
		Image2	128x128 (R=32&C=64)	0.0027	34.7861	72.4371	4.096	1.56%
			256x256 (R=32&C=128)	0.0094	31.2692	67.4032	16.384	6.25%
			512x512 (R=64&C=256)	0.0434	28.3627	61.5962	65.536	25%
	SLT	Image1	128x128 (R=16&C=32)	0.0007	37.7861	79.4371	1.024	0.39%
			256x256 (R=32&C=64)	0.0024	35.2692	74.4032	4.0960	1.56%
			512x512 (R=32&C=128)	0.0090	32.3627	68.5962	16.384	6.25%
		Image2	128x128 (R=16&C=32)	0.00069	37.2651	79.8792	1.024	0.39%
			256x256 (R=32&C=64)	0.0022	34.9872	75.1793	4.0960	1.56%
			512x512 (R=32&C=128)	0.0087	32.9765	69.5997	16.384	6.25%
Color	DWT	Image1	128x128 (R=32&C=64)	0.0042	33.1933	71.9079	12.288	1.56%
			256x256 (R=32&C=128)	0.0107	31.1549	67.8303	49.152	6.25%
			512x512 (R=64&C=256)	0.0368	28.4789	62.4894	196.608	25%
		Image2	128x128 (R=32&C=64)	0.0041	33.1879	71.5674	12.288	1.56%
			256x256 (R=32&C=128)	0.0105	31.4351	67.1653	49.152	6.25%
			512x512 (R=64&C=256)	0.0376	28.7623	62.4978	196.608	25%
	SLT	Image1	128x128 (R=16&C=32)	0.0026	34.1950	73.9096	3.072	0.39%
			256x256 (R=32&C=64)	0.0042	33.1903	71.8994	12.288	1.56%
			512x512 (R=32&C=128)	0.0120	30.9070	67.3345	49.152	6.25%
		Image2	128x128 (R=16&C=32)	0.0026	34.1950	73.9096	3.072	0.39%
			256x256 (R=32&C=64)	0.0042	33.1903	71.8994	12.288	1.56%
			512x512 (R=32&C=128)	0.0120	30.9070	67.3345	49.152	6.25%

On reception part, the secret image will extracted from stego- image without the need for the cover image. After deciphering, the extraction of secret image will be exactly the same as the embedded image. Figure (15) shows the extraction images.

Figure (15) the extraction images.

The extracted image will be the low frequency bands of secret image; the mid and high frequencies bands will take zeros matrixes and then apply invers transformation. Table (2) shows PSNR between the secret image and extraction of secret image after applying invers transformations.

Table (2) PSNR between the secret image (sending part) and extraction of secret image (reception part)

The secret image	PSNR
fly1	20.2511
antenna	19.3672
fly2	21.3451
fly3	20.4398

Conclusion:

In this paper, a new image data hiding algorithm based on 2-level DWT and SLT for the cover image and 1-level DWT and SLT for the secret image. Using the edges of cover image (mid and high frequency coefficients) which are less visible on human eyes for imbedding process increased PSNR between the cover and stego images. The cover image and secret image reach to the same size, in the proposed algorithm only (LL) of secret image is used. This will approximate the original image and has less data. The stego-image is looking consummately in place and has high value of peak signal to noise ratio (PSNR) reach to 62dB when secret image half size of the cover image and that is better than many existed methods . In this paper the security is increased by ciphering the secret image using AES method and then embedding on cover image coefficients after applying DWT and SLT. The proposed algorithms do not need the original cover image to extract the embedded secret image. The extracted secret image is exactly similar to the original secret image ,but we will then apply invers transformation of the reception image which be the low frequency coefficient, with mid and high frequency coefficients which set to zero, this will produce degradation between secret image and extraction of secret image.

Refrences

[1] M. Al Rababaa, "Colored Image-In-Image Hiding" 2009, Polyana-Svalyava (Zakarpattya), UKRAINE.

[2] A. Cheddad," A New Image Steganography Algorithm", Doctor thesis submitted to School of Computing & Intelligent Systems Faculty of Computing & Engineering University of Ulster.

[3] N. Jain et al. , "ImageSteganography Using LSB and Edge – Detection Technique", International Journal of Soft Computing and Engineering, Volume-2, Issue-3, July 2012

[4] A.Nag et al., "A novel technique for image steganography based on Block-DCT and Huffman Encoding", International Journal of Computer Science and Information Technology, Volume 2, Number 3, June 2010.

[5] Y. Zheng et al. , " A Method Based on Feature Matching to Identify steganography software", IEEE Transactions On security , 978-0-7695-4852-4/2012.

[6] C.Gayathri & V.Kalpana ,"Study on Image Steganography Techniques", International Journal of Engineering and Technology , Vol 5 No 2 ,Apr-May 2013.

[7] A. Altaay et al. , "An Introduction to Image Steganography Techniques", IEEE Transactions On Advanced Computer Science, 978-0-7695-4959-0/13.

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

[9] T. Morkel et al. ,"An overview of image steganography", (ICSA) Research Group ,Department of Computer Science ,University of Pretoria, Pretoria, South Africa,2002.

[10] M. Sabokdast & M. Mohammadi , "A Steganographic Method for Images with ModulusFunction and Modified LSB Replacement Based on PVD", IEEE Transactions On Information and Knowledge Technology, 978-1-4673-6490-4/2013.

[11] M..Juneja and P. Sandhu," An improved LSB based Steganography with enhanced Security and Embedding/Extraction", 3rd International Conference on Intelligent Computational Systems , January 26-27, 2013 Hong Kong (China).

[12] Mr. N. Raut & Prof. R. Chauhan," Neural Signal Compression With Multiwavelet Transform Using Video Compression Techniques", International Journal of Engineering Research and Applications, Vol. 2, Issue4, pp.2233-2236, July-August 2012.
[13] P. SHUKL, "A complex wavelet transforms and their applications", A dissertation submitted to the signal processing division,
Demartmant of electronic engineering, university of Strathclde,2003
[14] M. AL-Kanany, "A steganography system using slantlet transform",M.Sc. Submitted to the College of Engineering of the University of Baghdad, 2007.
[15] Md. Islam et al. , "Performance analysis of Coiflet-type wavelets for a fingerprint image compression by usieng wavelet and wavelet packet transform", International Journal of Computer Science & Engineering Survey , Vol.3, No.2, April 2012.
[16] S. Benchikh & M. Corinthios, "A Hybrid Image Compression Technique Based on DWT and DCT Transforms", Department of Electrical Engineering, Ecole Poly technique de Montreal, Montreal, Qc, Canada.
[17] I. Selesnick," The Slantlet Transform", IEEE transaction on signal processing, VOL. 47, NO. 5, MAY 1999.
[18] Federal Information Processing Standards Publication 197 ,"Advanced Encryption Standard (AES)", November 26, 2001.