New Method of Secret key Steganography in Bitmap Image Using Discrete Wavelet Transform

Alia Karim Abdul Hassan **Reem Majd**
University of Technology /Computer Science

Abstract

Steganography is the art and science of hiding communication; Steganography systems thus embed hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In this work, a new method of secret key steganography is introduced for hiding secret message in digital image; the proposed method uses Discrete Wavelet Transform (DWT) to embed a secret message with high data rate in Bit Mapped Image Format For Microsoft Windows (BMP) image. A new secret key which used to embed the secret message inside the image by converting the ASCII code of the secret message's characters into values suited to the coefficient of the image.

الخلاصة

أصبحت الاتصالات الرقمية جزء أساسي من البنية التحتية هذه الأيام, والكثير من التطبيقات معتمدة على الانترنيت وفي بعض الحالات تحتاج هذه التطبيقات ان تكون سرية وبالتالي أصبحت ضمان سرية البيانات مسألة أساسية. لفن وعلم اخفاء الاتصال (Steganography) مكانة مهمة في امنية البيانات, و بالتالي انظمة ال Steganography تعمل على تضمين البيانات السرية في داخل وسائط تعمل كغطاء لنقل هذة البيانات السرية بدون ان تثير اي شكوك بوجودها. في هذا البحث الطريقة المقترحة تستخدم طريقة تحويل المويجات المتقطع (Discrete Wavelet Transform) لاخفاء رسائل سرية داخل صور رقمية من نوع (BMP) بنسبة اخفاء عالية. الطريقة هي طريقة إخفاء بالمفتاح السري(secret key steganography) ، المفتاح السري الذي تم توليده بطريقة جديدة

1. Introduction

Information hiding in digital images, video or audio clips has drawn much attention in recent years. Some auxiliary information is implicitly combined with a piece of multimedia data, i.e. the host signal, to form a composite signal for certain interesting applications. Digital watermarking is one type of information hiding. The copyright related information about the media data is inserted to enforce intellectual property right protection. The other application is to transmit a large volume of information covertly in a multimedia file via information hiding techniques. The case of covert communication can also be termed as *steganography*, which is derived from the Greek words meaning *covered writing* [SC03].

Steganography is the art and science of hiding communication; a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper's suspicion. In the past, people used hidden tattoos or invisible ink to convey steganographic content. Today, computer and network technologies provide easy-to-use communication channels for steganography [PH03].

In this work a secure steganography system designed to hide a secret message with high capacity inside a Bitmap (BMP) image in such way that it is imperceptible to human observer then retrieve the secret message without loss by using wavelet transform technique**.**

2. Steganography

Steganography stands for techniques in general that allows secret communication, usually by embedding or hiding the secret information in other, unsuspected data. Steganographic methods generally do rely on the assumption that the existence of the covert communication is unknown to third parties and are mainly used in secret point-to point communication between trusting parties [HK99]. Each data hiding method consists of: *the embedding algorithm* and *the detector algorithm.*

(Or extract algorithm). The embedding algorithm is used to hide *secret message* inside a *cover* (or carrier); the *embedding process* is protected by a keyword so that only those who possess the secret keyword *(stegokey*) can access the hidden message. The *detector algorithm* is applied to a (possibly modified) carrier and returns the hidden secret message[HK99].

2.1 Secret key Stegangraphy

Secret Key Steganography is defined as a steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret Key Steganography takes a cover message and embeds the secret message inside it by using a secret key (stego-key). Only the parties who know the secret key can reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit of Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message [Dun02].

2. 2 Steganography System Requirements

All steganography algorithms have to comply with a few basic requirements. These requirements are as follows:

Invisibility (Perceptual Transparency): the invisibility of a steganographic algorithm is the first and foremost requirement, since the strength of steganography lies in its ability to be unnoticed by the human eye [ME00].

Robustness: refers to the ability of embedded data to remain intact if the stego-image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations, cropping or decimation, lossy compression, and conversion from digital to analog form and then re-conversion back to digital form (such as in the case when a hard copy of a stego-image is printed and then a digital image is formed by subsequent scanning the hardcopy) [LD99].

Capacity: is the size of information that can be hidden relative to the size of the cover [LD99].It is measured in bits (of payload) per byte (of cover) [BD05].

Security:A secure steganographic algorithm can be defined in terms of four requirements *first*, massages are hidden using a public algorithm and a secret key; the secret key must identify the sender uniquely. *Second*, only a holder of the correct key can detect, extract, and prove the existence of the hidden message. Nobody else should be able to find any statistical evidence of a message's existence. *Third*, even if the enemy knows (or is able to select) the contents one hidden message, he should have no chance of detecting others. And *finally*, it is computationally infeasible to detect hidden messages [BD05].

3. Information Hiding in Image

The onset of computer technology and the internet has given new life to steganography and the creative methods with which it is employed[JD01]. Given the proliferation of digital images, especially on the Internet, and given the large amount of redundant bits present in the digital representation of an image, images are the most popular cover objects for steganography [ME00]. There are several reasons why images are used for steganography. *First*, because of the high degree of redundancy in image data, it is possible to embed a great deal of hidden information without visibly affecting the cover image. *Second,* innocuous-looking images are commonplace throughout the internet and arouse little suspicion. By contrast, under current bandwidth availability, video files posted on web sites take too long to transfer effectively. Also, audio and video data are prone to be examined for copyright infringement. *Third,* the sheer volume of image data available online makes it difficult

to identify suspicious content. Thus, image data is commonly used for data hiding [BD05].

4. Steganography Techniques

Information hiding is accomplished either in the space domain or in the frequency domain [WW02]. The image domain methods modify their host files at the bit level, changing the file bit by bit to encode their message. The transform domain methods manipulate the algorithms and transformations inherent in the creation of the image itself [Mic03]. A number of ways exist to hide information in digital images. Common approaches include *Least significant bit insertion(LSB),Masking and filtering, and Algorithms and transformations*. Each of these techniques can be applied, with varying degrees of success, to different image files [JJ98]. Data embedding performed in the *transform* can also realize large-capacity embedding for steganography**.** Transform techniques can offer superior robustness against lossy compression because they are designed to resist or exploit the methods of popular lossy compression algorithms. Transform-based steganography also typically offer increased robustness to scaling and rotations or cropping, depending on the invariant properties of a particular transform[LD99].

4.1 High bit-rate and low bit-rate data hiding

Current methods for the embedding of messages into cover images fall into two main categories: *High bit-rate data hiding* and *low bit-rate data hiding,* where bit-rate means the amount of data that can be embedded as a portion of the size of the cover image [TG04]. In ***low bit-rate encoding,*** we expect a high level of robustness in return for low bandwidth. The emphasis is on resistance against attempts of data removal by a third party. On the other hand, with high bit-rate methods are usually designed to have minimal impact upon the perception of the host image, but they do not tend to be immune to image modifications. In return, there is an expectation that relatively large amounts of data can be encoded. All ***high bit-rate methods*** can be made more robust through the use of ***error-correction coding***, at the expense of data rate. So, high bit-rate codes are only appropriate where it is reasonable to expect that a great deal of control will be maintained over the images[TG04]. One form of high bit-rate encoding is embedding the message by modulating coefficients in a transform domain, such Wavelet Transform. The transformation can be applied to the entire image or to its subparts. The embedding process is done by modifying some coefficients that are selected according to the type of protection needed. If we want the message to be imperceptible then the high range of frequency spectrum is chosen, but if we want the message to be robust then the low range of frequency spectrum is selected. In high bit-rate data hiding we have two primary objectives: the technique should provide the maximum possible payload and the embedded data must be imperceptible to the observer. Fundamentally, data payload of a steganographic scheme can be defined as the amount of information its can hide within the cover media[TG04]. Hiding rate measured by the following function:

$$hiding \quad rate = \frac{Maximum allowable length of \ \text{sec} ret\ message}{Cover\ size} \quad .....(1)$$

Usually the invisibility of the hidden message is measured by Mean Square Error (MSE), this metrics can be used to measures the amount of error in the stego-image, in other words, they are useful measures to compare between the stego-image and cover image. MSE can measure by the following function:

$$MSE = \frac{1}{XY}\sum_{x,y}(p_{xy} - p'_{xy})^2 \quad ....(2)$$

where $p(x,y)$ represents a pixel, whose coordinates are (x,y) in the original image, and p'_{xy} represents the same pixel in the distorted image. The resulted percent estimate the degree of similarity between the two comparisons [WW02].

4.2 Wavelet Transform

A wavelet is a waveform of limited duration with an average value of zero. One-dimensional wavelet analysis decomposes a signal into basis functions which are shifted and scaled versions of a mother wavelet. Wavelet coefficients are generated and are a measure of the similarity between the basis function and signal being analyzed. There are different types of wavelet transforms, including the Continuous Wavelet Transform (CWT) and the Discrete Wavelet Transform (DWT). The CWT is used for signals that are continuous in time and the DWT is used when a signal is being sampled, such as during digital signal processing or digital image processing [JG03].

4.3 Discrete Wavelet Transform

The discrete wavelet transform (DWT) represents a 1-D, continuous time signal f in terms of shifted versions of a low-pass scaling function and shifted and dilated versions of a prototype band pass wavelet function.

4.4 Wavelet Transform of Image

The wavelet transform is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. The basic idea of the DWT for a two-dimensional image is described as follows. An image is first decomposed into four parts of high, middle, and low frequencies (i.e., *LL*1, *HL*1, *LH*1, *HH*1 subbands) by critically subsampling horizontal and vertical channels using subband filters. The subbands labeled *HL*1, *LH*1, and *HH*1 represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the subband *LL*1 is further decomposed and critically subsampled. This process is repeated several times, which is determined by the application at hand. An example of an image being decomposed into ten subbands for three levels is shown in figure (1). Each level has various bands information such as low–low, low–high, high–low, and high–high frequency bands. Furthermore, from these DWT coefficients, the original image can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). If *I[m,n]* represents an image, the DWT and IDWT for *I[m,n]* can be similarly defined by implementing the DWT and IDWT on each dimension *m* and *n* separately[HT01].

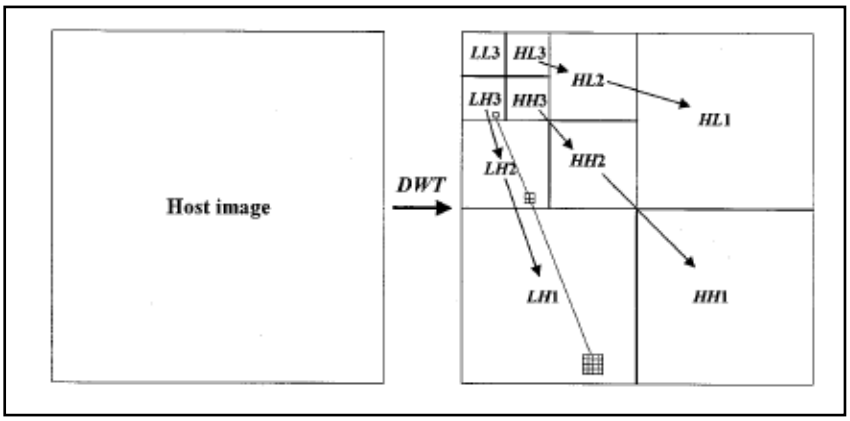


Figure (1) DWT decomposition of an image.

4.5 Haar Wavelet

The Haar wavelet (HT) is the simplest wavelet. HT detail coefficients can be obtained by high-pass filtering and down-sampling given as:

$$yD(n) = \frac{1}{\sqrt{2}}(x(2n) - x(2n+1) \quad \cdots(3)$$

HT approximation coefficients can be obtained by low pass filtering and downsampling given as:

$$yA(n) = \frac{1}{\sqrt{2}}(x(2n) - x(2n+1) \quad \cdots(4)$$

Simply, the Haar wavelet function is the two point derivative and the scaling function is the sum of two successive samples. HT detail coefficients are the downsampled version of the derivative and approximation coefficients are the downsampled version of the sum of two successive samples. HT detail coefficients are sensitive to changes in the first derivative of the signal. The HT is an orthogonal wavelet transform. Reconstruction of the details from the HT detail coefficients is performed by up-sampling and filtering with a high-pass filter given as:

$$D(n) = \frac{1}{\sqrt{2}}(y_{DU}(2n) - y_{DU}(2n+1) \quad \cdots(5)$$

Reconstruction of the approximations from Haar approximation coefficients is performed by up-sampling and filtering with low-pass filter given as:

$$A(n) = \frac{1}{\sqrt{2}}(y_{AU}(2n) - y_{AU}(2n+1) \quad \cdots(6)$$

where

$$y_{DU}(2n) = y_D(n), \quad y_{DU}(2n+1) = 0, \quad y_{AU}(2n) = y_A(n), \quad y_{AU}(2n+1) = 0$$

In fact, the combination of these two filters forms the Haar transform and it have been invented before the wavelets [Okt98].

5. Steganography, BMP Images and Wavelet Transform

Selection of the proper combination of steganography tools and covers is the key to successful information hiding, so the choice of cover images is important and influences the security in a major way. Most software available today neither supports nor recommends using Joint Photographic Experts Group (JPEG) images, but recommends instead the use of 24-bit images such as Microsoft Windows bitmap file (BMP). The next-best alternative to 24-bit images is to use 256-color or gray-scale images for embedding the hidden message, the images choice by many steganography experts are images featuring 256 shades of gray [KP00]. These gray-scale images are preferred because the shades change very gradually from byte to byte, and the less the value changes between palette entries, the less noticeable image color variation is. Information can be hidden by many different ways in images [JJ98]. Wavelet transform will be the tool used in this work. The wavelet can be regarded as the most efficient transform that deals with image, sound or any other pattern since it provides a powerful time space representation. The importance of the wavelet transform comes from its decomposition of the image into multi level of the independent information and steganography deals with finding the best place in cover media to hide data [Val99].

6.The Proposed method.

The proposed method could be used for hiding high data rate, but the embedded secret message cannot survive against modifications produces by an attacker. The proposed method embeds the secret message into the wavelet transform of a grayscale image of size (256×256) pixel. So, the proposed method shown in figure (2).

6.1 Embedding Process

In this stage all characters and symbols of the secret message will be embedded in a wavelet transform of a gray scale (256×256) pixels cover image. This process represents the main operation of steganography to hide secret message inside cover transfer media. The discrete wavelet transform generates four split resolutions after applying it on image (LL, LH, HL, and HH). The LL area contains smooth information of image transformed and HH area contains details information of image. The HH area of wavelet transform resulted after applying high pass filter on rows and columns for the data of image i.e. that only the sharp edges and high colored changes events are stored in this area because only these data are passed from high pass filter according to the high frequency representation for each of them.

The proposed embedding algorithm embeds the secret message with high-bit data rates in a suitable frequency band of the wavelet transform of the image. The selection of the frequency band is done according to the type of protection needed. The suggest method is a high- bit rate data hiding that needed two objectives:

- The maximum possible payload (capacity)
- The embedded data must be imperceptible to the observer (Invisibility).

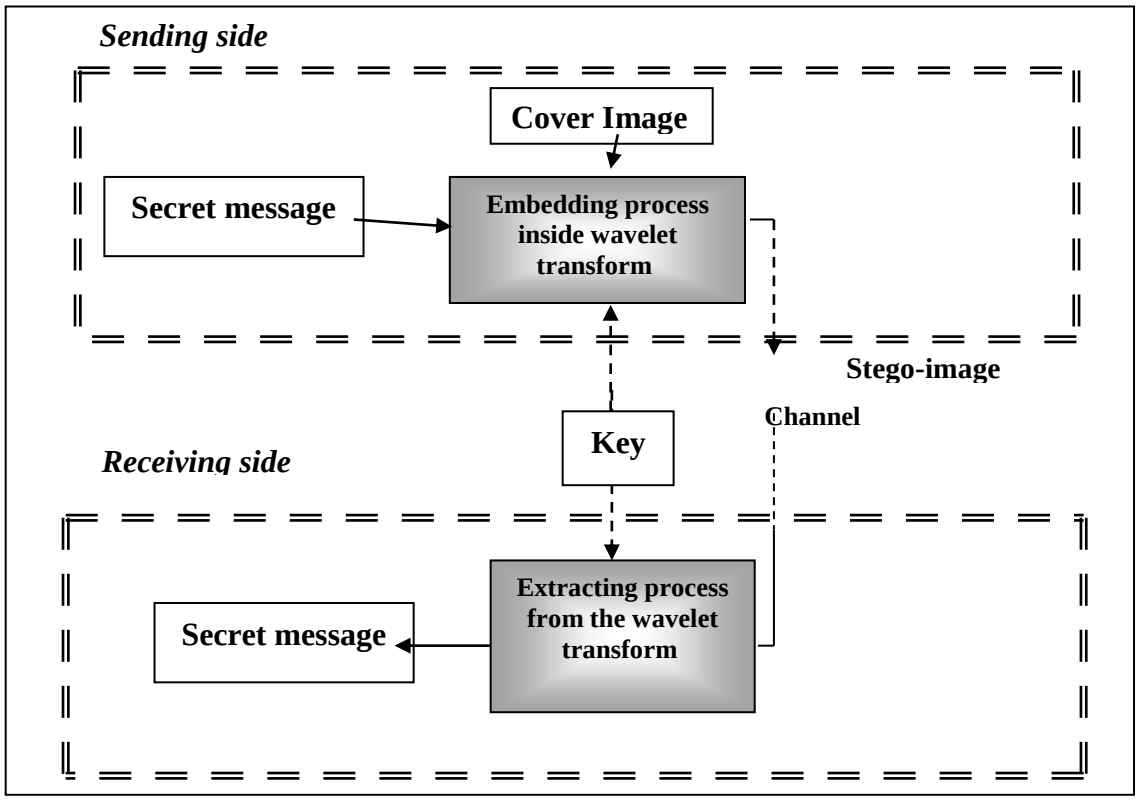


Figure (2) The proposed method

According to these objectives, a high frequency band (HH) is chosen. The suggested embedding method is considered as a secret steganography that requires the exchange of a secret key (stego-key) prior to communication. In the current work designed ***look up table*** that is shown in table (1) is considered as stego-key. The ***look up table*** is generated from two matrixes (ch) and (ky) each one of size (1×16) as shown in figure (3), the values of these two matrixes are range between (-14 and 16), by testing different BMP image theses values are chosen to suit the coefficients of discrete Haar wavelet transform, so the designed embedding method can have minimal impact upon the perception of the cover image. The look up table consist of three column and 256 rows, the first column are the values (0-255) which represents input number for the encryption character, and second and third column represent values range from (-14 and 16) which considered code (1&2), the algorithm(1) illustrates the generation of the look up table. Algorithm (2) illustrates how the proposed embedded method works.

-14	-12	-10	-8	-6	-4	-2	0	2	4	6	8	10	12	14	16

(a) Matrix (ch)

-14	-12	-10	-8	-6	-4	-2	0	2	4	6	8	10	12	14	16

(b) Matrix (ky)

Figure (3) a) Matrix (ch) b) Matrix (ky)

Algorithm (1) Look up table generation

Input: *Two matrixes ch and ky of size (1×16) as shown in figure(3).*
Output: *Matrix (w) of size (3×256) which represent look up table.*

Step 1*: Generates a matrix (w) of size (256×256).*
Step 2*: Let n, k=16 and i=1.*
Step3: *Fill the rows from (1-256) of the first column of the matrix (w) with values (0-255) which represent the input numbers of the encryption characters.*
Step4*: Fill the rows from (i to k) of the second column (code1) of matrix (w) with the elements from (1 to 16) of the matrix (ch) and fill the rows from (i to k) of the third column (code2) with element ch [n].*
Step5: *Increments i and k by 16 and decrement n by 1, if i equal to 256 continue to step 6 else return to step3.*
Step 6: *End.*

Algorithm(2) Embedding Process

Input: *Matrix(r) of size (64×64) which represents the secret message code, Cover image, And look up table (stego-key).*
Output: *Cover image hold secret data (stego-image).*
Step 1*: Decompose by one level the cover image using Haar wavelet filter.*
Step 2*: Generate new matrix (m) of size (128×128).*

Step 3*:Each element in matrix (r) which resulted from algorithm (1) is converted into four elements in the new generated matrix (m). The two values (m[i,j]) and (m[i,j+1]) are taking from the corresponding codes (1 & 2) form the look up table listed in table (1) and repeated the same codes for (m[i+1,j]) and (m[i+1,j+1]) .*

Step 4*: Replacing the data of HH wavelet area by the new matrix (m) resulted in step 3.*

Step5*: Reconstruct the final cover image using the inverse discrete wavelet transform.*

Step 6*: Send the stego-image and finish.*

As described in algorithm (2) step3 , every element in matrix (r) is converted into four elements from the look up table to generate matrix(m), the reason of that repetition is to provide **error correction** to the method in case any value in matrix (m) will change during the sending process.

6.2 Extracting Process

In this stage the secrete data inside stego-image are extracted using the inverse operations followed in the algorithm(1), so the receiver in this step needs only the values in this table to extract the secret data hiding inside the image without needed of the original image. This step also applies error correction process to correct every mistake detected by receiver; this ***error correction*** process is shown in step 3 of extracting algorithm (3).

Algorithm(3) Extracting Process

Input: *Receiving cover image (stego-image), look up table (stego-key).*

Output: *secret message.*

Step 1*:* Apply discrete wavelet transform to the receiving image using Haar wavelet filter.

Step 2*:* Read data in HH wavelet area and store the readied values in matrix (*m*) of size (128×128).

Step 3*:* Read four elements (2 pairs) from the new matrix at one time, first pair is (*m [i , j] and m[i , j+1]*) while second pair is (*m [i+1 , j] and m[i+1 , j+1]*) then compare each set separately with the same look up table used by sender to find the best (code 1 and code 2) in this table depending the lower error occur between the read codes and the designed codes in look up table then store the code value corresponding to the best codes in a new matrix (r) of size (64×64) (e.g. if the codes 1 and 2 satisfied are 6 and -10 then the code value is 218), i.e. that four values from matrix (m) are converted into one value in a new matrix (r) therefore matrix (r) takes half size of matrix(m) .

Step 4*:* Increase column index j by 2 and repeat the process in step 3 for next four elements (*m [i , j] and m[i , j+1], m [i+1 , j] and m[i+1 , j+1]*), if the column index j reaches to the final column then set column index j to 1 and increase row index i by 2 and continue until all rows are covered.

Step 5*:* matrix (r) that is filled with the resulted code from look up table represent the secret message code.

Step 6: finish.

Table (1) Look up table

Input No.	code 1	code 2	Input No.	code 1	code 2	Input No.	code 1	code 2	Input No.	code 1	code 2	Input No.	code 1	code 2	Input No.	code 1	code 2
0	-14	16	43	8	12	86	-2	6	129	-12	0	172	10	-4	215	0	-10
1	-12	16	44	10	12	87	0	6	130	-10	0	173	12	-4	216	2	-10
2	-10	16	45	12	12	88	2	6	131	-8	0	174	14	-4	217	4	-10
3	-8	16	46	14	12	89	4	6	132	-6	0	175	16	-4	218	6	-10
4	-6	16	47	16	12	90	6	6	133	-4	0	176	-14	-6	219	8	-10
5	-4	16	48	-14	10	91	8	6	134	-2	0	177	-12	-6	220	10	-10
6	-2	16	49	-12	10	92	10	6	135	0	0	178	-10	-6	221	12	-10
7	0	16	50	-10	10	93	12	6	136	2	0	179	-8	-6	222	14	-10
8	2	16	51	-8	10	94	14	6	137	4	0	180	-6	-6	223	16	-10
9	4	16	52	-6	10	95	16	6	138	6	0	181	-4	-6	224	-14	-12
10	6	16	53	-4	10	96	-14	4	139	8	0	182	-2	-6	225	-12	-12
11	8	16	54	-2	10	97	-12	4	140	10	0	183	0	-6	226	-10	-12
12	10	16	55	0	10	98	-10	4	141	12	0	184	2	-6	227	-8	-12
13	12	16	56	2	10	99	-8	4	142	14	0	185	4	-6	228	-6	-12
14	14	16	57	4	10	100	-6	4	143	16	0	186	6	-6	229	-4	-12
15	16	16	58	6	10	101	-4	4	144	-14	-2	187	8	-6	230	-2	-12
16	-14	14	59	8	10	102	-2	4	145	-12	-2	188	10	-6	231	0	-12
17	-12	14	60	10	10	103	0	4	146	-10	-2	189	12	-6	232	2	-12
18	-10	14	61	12	10	104	2	4	147	-8	-2	190	14	-6	233	4	-12
19	-8	14	62	14	10	105	4	4	148	-6	-2	191	16	-6	234	6	-12
20	-6	14	63	16	10	106	6	4	149	-4	-2	192	-14	-8	235	8	-12
21	-4	14	64	-14	8	107	8	4	150	-2	-2	193	-12	-8	236	10	-12
22	-2	14	65	-12	8	108	10	4	151	0	-2	194	-10	-8	237	12	-12
23	0	14	66	-10	8	109	12	4	152	2	-2	195	-8	-8	238	14	-12
24	2	14	67	-8	8	110	14	4	153	4	-2	196	-6	-8	239	16	-12
25	4	14	68	-6	8	111	16	4	154	6	-2	197	-4	-8	240	-14	-14
26	6	14	69	-4	8	112	-14	2	155	8	-2	198	-2	-8	241	-12	-14
27	8	14	70	-2	8	113	-12	2	156	10	-2	199	0	-8	242	-10	-14
28	10	14	71	0	8	114	-10	2	157	12	-2	200	2	-8	243	-8	-14
29	12	14	72	2	8	115	-8	2	158	14	-2	201	4	-8	244	-6	-14
30	14	14	73	4	8	116	-6	2	159	16	-2	202	6	-8	245	-4	-14
31	16	14	74	6	8	117	-4	2	160	-14	-4	203	8	-8	246	-2	-14
32	-14	12	75	8	8	118	-2	2	161	-12	-4	204	10	-8	247	0	-14
33	-12	12	76	10	8	119	0	2	162	-10	-4	205	12	-8	248	2	-14
34	-10	12	77	12	8	120	2	2	163	-8	-4	206	14	-8	249	4	-14
35	-8	12	78	14	8	121	4	2	164	-6	-4	207	16	-8	250	6	-14
36	-6	12	79	16	8	122	6	2	165	-4	-4	208	-14	-10	251	8	-14
37	-4	12	80	-14	6	123	8	2	166	-2	-4	209	-12	-10	252	10	-14
38	-2	12	81	-12	6	124	10	2	167	0	-4	210	-10	-10	253	12	-14
39	0	12	82	-10	6	125	12	2	168	2	-4	211	-8	-10	254	14	-14
40	2	12	83	-8	6	126	14	2	169	4	-4	212	-6	-10	255	16	-14
41	4	12	84	-6	6	127	16	2	170	6	-4	213	-4	-10			
42	6	12	85	-4	6	128	-14	0	171	8	-4	214	-2	-10			

6.3 Practical Results

This section will present the practical results obtained by embed two secret messages into four grayscale images of size (256×256) pixel. Test is taken to find the applicability of the proposed steganography method. Table (2) gives brief information about the tested images and the MSE in addition to the secret message length and hiding data rate. This section also offers a figure (4) shows the application of the proposed steganography method for several BMP images and secret messages.

Table (2) Practical results

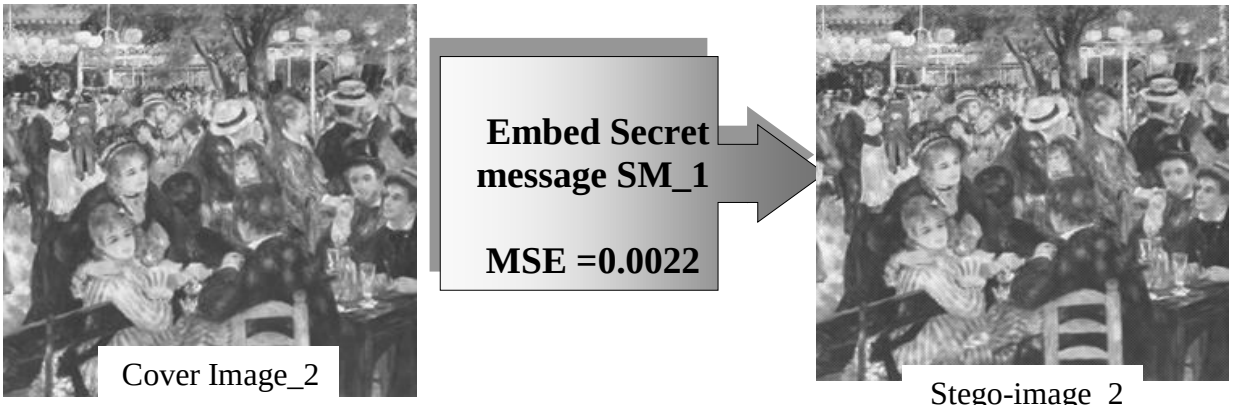
COVER IMAGE NAME	SECRET MESSAGE NO.	LENGTH OF SECRET MESSAGE (BYTE)	MSE (DB)
Cover Image_1	SM_1	2930	0.0024
Cover Image_2	SM_1	2930	0.0022
Cover Image_3	SM_2	4072	0.0030
Cover Image_4	SM_2	4072	0.0028

7. Conclusions

The proposed method offers high level of security in terms of transmitting the resultant stego-imge without raising suspicion, and the following conclusions can be derived from this work:

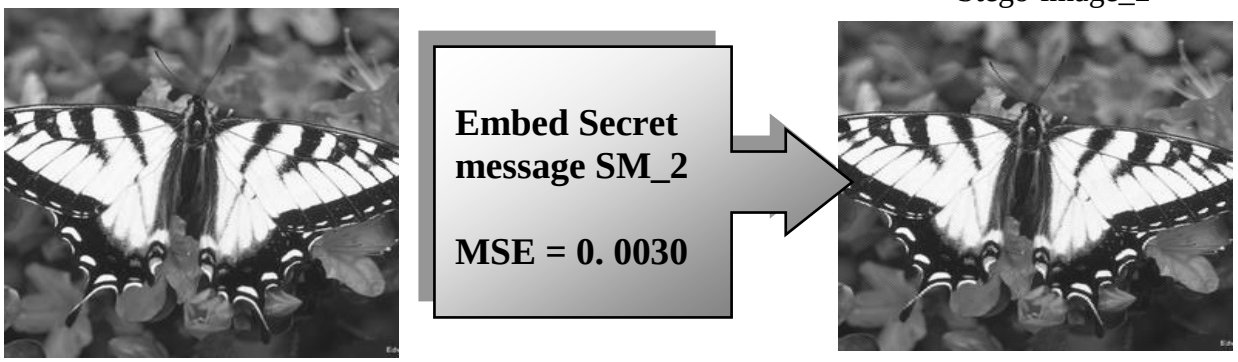
1. The proposed method can be defined as a secret key steganography system where the same key is used by sender and receiver. Table (1) shows the proposed new secret key which used to embed the secret message inside the image by converting the ASCII code of the secret message's characters into values suited to the coefficient of the image obtained form applying Haar filter to the image.
2. The embedded secret message is extracted directly form received stego-image, so there is no need for the original cover in the extraction process.
3. The hiding method is successful in hiding high data rate of bits; the maximum allowable secret message length is (4096 characters = 32768 bit), so the proposed method confirms the first objective of the high bit-rate data hiding which is the maximum possible payload (capacity).
4. From table (2) the results obtained from MSE test indicate that the stego-image is similar to its corresponding cover, this proved that the system is secure ,and also the proposed method confirms the second objective of the high bit-rate data hiding which is imperceptible to the observer (Invisibility).
5. The proposed method ensures data integrity and it is successful in retrieving the embedded secret message without loss because of using error correction in the receiving stage (step3 in algorithm (2)).

Stego-image_1



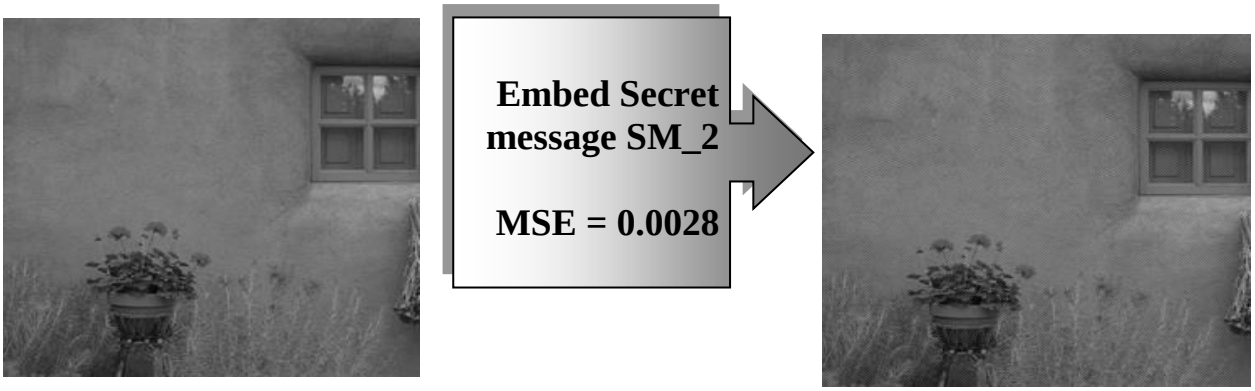
Cover Image_2

Stego-image_2



Cover Image_3

Stego-image_3



Cover Image_4

Stego-image_4

Figure (4) Tested cover images with related stego-images

References

[BD05] Bergman C., Davidson J.," ***Unitary Embedding for Data Hiding with the SVD***", Security, Steganography, and Watermarking of Multimedia Contents VII, SPIE Vol. 5681,San Jose, CA, Jan. 2005,URL:
http://orion.math.iastate.edu/cliff/manuscripts/svdstego.pdf

[Dun02] Dunbar B., **"*A detailed look at Steganographic Techniques and their use in an Open-Systems Environment*",** SANS Institute, 2002**.**

[HK99] Hartung F., Kutter M., **"*Multimedia Watermarking Techniques*",** PROCEEDINGS OF THE IEEE, Vol. 87, NO. 7, July 1999.

[HT01] Hsieh M., Tseng D., Huang Y., "***Hiding Digital Watermarks Using Multiresolution Wavelet Transform***", IEEE Transaction on industrial electronics, vol. 48, no. 5, October 2001.

[JD01]Johnson N. F., Duricn Z., Jajodia S., "***Information hiding: steganography and watermarking attack and countermeasures***", kluwer Academic publishers, USA, 2001.

[JG03] Jackson J. T., Gregg H., Claypoole R. L., Jr., Lamont G. B., "***Blind Steganography Detection Using A Computational Immune System Approach: AProposal***", 2003, URL:
http://www.dfrws.org/2002/papers/Papers/Jacob_Jackson.pdf

[JJ98] Johnson N. F., Jajodia S., "***Exploring Steganography: Seeing the Unseen",*** IEEE, 1998, URL: http://www.jjtc.com/pub/r2026.pdf

[KP00]Katzenbeisser S., Peticolas F., "***Information Hiding Techniques for Steganography and Digital Watermarking***", Artech House Inc, USA, 2000.

[LD99]Lin E., Delp E. J.,**" *A Review of Data Hiding in Digital Images***", System Conference, 1999.

[ME00] Morkel T., Eloff J., Olivier M**.,** ***"An overview of image Steganography"***, Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science University of Pretoria, 2000, URL:
http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/098_Article.pdf

[Mic03] Michaud E., "***Current Steganography tools and methods***", SANS Institute, 2003.

[Okt98] Öktem H., " ***Preprocessing and Parameter Extraction Algorithms for Diagnostic Analysis of EMCG***", M SC. Thesis, Department of Electrical Engineering, Tampere University of Technology, 1998, URL:
http://hybrid.iam.metu.edu.tr/hakanold/mscthesis.pdf

[PH03] Provos N., Honeymen P., "***Hide and Seek: An Introduction to Steganography",*** IEEE Computer Society,2003,URL:
http://niels.xtdnet.nl/papers/practical.pdf

[SC03] Su P., Kuo J., "***Steganography in JPEG2000 Compressed Images***", IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, November 2003.

[TG04] Tolba M., Ghonemy M., Taha I., Khalifa A., "***Using Integer Wavelet Transforms In Colored Image-Steganography***", IJICIS Vol.4 No. 2, July 2004, URL: http://www.ijicis.net/Vol4_No2%20No5.pdf

[Val99]Valens, C., "***A really friendly guide to wavelets***", 1999, URL: http://wandoo.fr/polyvalencs,

[WW02] Wang H., Wang S., "***Cyber Warfare: Steganography vs. Steganalysis ",*** Communication of the ACM, vol. 47, No. 10, October 2004, URL: http://portal.acm.org/citation.cfm?doid=1022594.1022597