Design and Implementation of Secure Public Key Steganography

Dr. Alia Karim Abdul Hassan & Ghadah Salim Mouhamad*

Received on: 13/11/2008
Accepted on:1/10/2009

Abstract

Several approaches and techniques have been proposed to make communication via the internet secure; one of these approaches is steganography. 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 this research the proposed method is a public key steganography technique and it embeds a secret message in digital image with multi level of security. The proposed method uses Discrete Cosine Transform (DCT) to embed a secret message in Bit Mapped Image Format for Microsoft Windows (BMP) image with high invisibility and high correlation between cover-image and stego-image acceptable hiding data rate.

Keywords: Steganography , public key steganography, Discrete Cosine Transform, Bit Mapped Image , invisibility ,cover-image ,stego-image , hiding data rate.

تصميم و تنفيذ تقنية كتابة مغطاة باستخدام المفتاح المعلن

الخـــلاصة

خلال هذه الفترة وفر الانترنيت اتصالات اساسية بين عشرات الملايين من الناس والامنية اصبحت حاجة ملحة للتعامل معه, حيث وجدت الكثير من التقنيات والطرق للتعامل معه وواحدة من هذه التقنيات هي تقنية (Steganography)تقنية الكتابة المغطاة وهي فن وعلم الاتصالات المخفيةلرسالة سرية بدون اثارة الشكوك لدى الاخرين .الطريقة المقترحةهي طريقة اخفاء باستخدام المفتاح المعلن تخفي رسالة سرية في صورة رقمية على عدة مستويات من الامنية. الطريقة المقترحة تستخدم (Discrete Cosine Transform) لأخفاء رسالة سرية في صورة من نوع (BMP) بمستوى عالي من imperceptibility وكذلك وجود ترابط قوي بين (cover-image)و(stego-image).

Introduction

Information hiding is the technology to embed the secret information in digital data so that it cannot be perceived visually or audibly [1]. Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly [2]. There are two main directions in information hiding: protecting only against the detection of a secret message by a passive adversary (steganography), and hiding data so that even an active adversary cannot remove it(watermarking)[3]

* Computer Science Department, University of Technology / Baghdad

https://doi.org/10.30684/etj.28.3.1
2412-0758/University of Technology-Iraq, Baghdad, Iraq

Steganography

It is the art and science of invisible communicating in such a way that the presence of a message cannot be detected [4]. The goal of steganography is to hide an information message inside harmless messages in such a way that it is not possible even to detect that there is a secret message present. Steganography in the modern day sense of the word usually refers to information or a file that has been concealed insides digital carriers [5].Digital carriers of such messages may resemble innocent images, audio, video, text, or any other digitally represented code or transmission [6]. Each data hiding method consists of:

The Embedding algorithm and *The Extraction algorithm.* The input to the embedding algorithm is secret message, the cover data and an optional public or secret key. The output is stego data, also called stego object, The embedding algorithm used to hide secret message inside a cover (or carrier); Inputs to the generic extracting algorithm are the tested data, the secret or public key depending on the method, the original cover data. The output is the hidden secret message [3].

Public Key Steganography

Public key steganography system requires the use of two keys, **one private** (secret key) and one **public key**; whereas the *public key* is used in the *embedding process*, the *secret key is* used to *reconstruct* the secret message [3].

Public key steganography utilizes the fact that the decoding function ***D*** in a steganography system can be applied to any cover ***c***, whether or not it already contains a secret message. In the latter case, a random elements of message ***M*** will be the result; it called "natural randomness" of the cover [6].The attacker cannot decide if the extracted information is meaningful or just part of the natural randomness, unless he is able to break the cryptosystem [6], so that Public Key Steganography provides a more robust way of implementing a steganographic system because it has multiple levels of security in that unwanted parties must first suspect the use of steganography and then they would have to find a way to crack the algorithm used by the public key system before they could intercept the secret message [7].

Steganography System Requirements

There are different requirements for all steganography algorithms depending on the purpose of steganography;these requirements are as follow:

1. **Capacity:** It is an important factor in captioning applications, when a lot of information should be embedded into a cover data, what is usually related to the current picture [3].
2. **Robustness:** The embedded information is said to be robust if its presence can be reliably detected after the image has been modified but not destroyed beyond recognition [8].
3. **Security:** The embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks based on a full knowledge of the embedding algorithm and the detector, and the knowledge of at least one carrier with hidden message [8].
4. **Perceptual transparency (invisibility):** It is based on the properties of the Human Visual System (HVS) or the Human Audio System (HAS). The embedded

information is imperceptible if an average human subject is unable to distinguish between carriers that do contain hidden information and those that do not [8].

5. **Undetectibility:** It is important when a secret communication occurs between two parties and the fact of a secret communication is kept to be secret [3].

Steganography in Images

Hiding information inside images is a popular technique nowadays . To hide a message inside an image without changing its visible properties, the cover source can be altered in ”noisy” areas with many color variations, so less attention will be drawn to the modifications. The most common methods to make these alterations on the cover image involve the usage of (LSB), masking, filtering and transformations. These techniques can be used with varying degrees of success on different types of image files **[9].**

Steganography Techniques

Information hiding is accomplished either in the Spatial domain or in the frequency domain. (Spatial domain techniques) embed messages in the intensity of the pixels directly, while for frequency domain, images are first transformed and then the message is embedded in the image. Each of these two techniques has its own advantage and disadvantage. In the spatial domain the message can simply inserted data into host the host image, but the inserted information may be easily detected using computer analysis. In the frequency domain the message can be insert data into the coefficients of a transformed image, for example using Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and wavelet Transform (WT). But cannot embed too much data in the frequency domain because the quality of the host image will be distorted significantly [10,11].

Transformations Domain Techniques

Transform domain methods hide messages in significant areas of the cover image which makes them more robust to attacks, such as compression, cropping, and some image processing, than the LSB approach. However, while they are more robust to various kinds of signal processing, they remain imperceptible to the human sensory system [6]. A more complex way of hiding a secret message inside an image comes with the use and modifications of (DCT) coefficientsm[9]. One of techniques which operate on DCT-encoded blocks of image is modulus-4(Mod 4) image steganography.

Transformation

The transformation should utilize the fact that the information content of an individual pixel is relatively small. Transform coding relies on the premise that pixels in an image exhibit a certain level of correlation with their neighboring pixels [12].

The Discrete Cosine Transform (DCT)

DCT is a widely used mechanism for image transformation and has been adopted by .JPEG to compress images [13]**.** It transforms a signal or image from the spatial domain to the frequency domain [14]. The general equation for a 2-D (*N* by *N* image) DCT is defined by the following equation [1]:

$$F(u,v) = \frac{2}{N} c(u)c(v) \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} p(i,j) \cos\left[\frac{(2i+1)up}{2N}\right] \cos\left[\frac{(2j+1)up}{2N}\right] \quad (1)$$

Where:

$$c(e) = \begin{cases} \sqrt{\frac{1}{N}} & if \quad e = 0 \\ \sqrt{\frac{2}{N}} & if \ e \rangle 0 \end{cases} \qquad (2)$$

And the corresponding **inverse** 2D-DCT transform is simple $F^{-1}(u,v)$

Where

$$p(i,j) = \frac{2}{N}\sum_{u=0}^{N-1}\sum_{v=0}^{N-1} c(u)c(v)F(u,v)\cos\left[\frac{(2i+1)u\pi}{2N}\right]\cos\left[\frac{(2j+1)v\pi}{2N}\right] \quad (3)$$

DCT has the property that, for typical image, most of the visually significant information about the image is concentrated in just few coefficients of DCT, for this reason the DCT is used in image compression applications [15].

Quantization

Quantization is simply the process of reducing the number of bits needed to store an integer value by reducing the precision of the integer. In .JPEG compression the "drastic" action used to reduce the number of bits required for storage of the DCT matrix is referred to as "Quantization", where the DCT output matrix takes more space to store than the original matrix of pixels[16]. For every element position in the DCT matrix, a corresponding value in the quantization matrix gives a quantum value. The actual formula for quantization is quite simple:

$$\text{QuantizedValue}(I,J) = \text{Roundedtonearestinteger}\left(\frac{\text{DCT}(I,J)}{\text{Quantum}(I,J)}\right) \quad (4)$$

The dequantization formula operates in reverse.

$$\text{DCT}(I,J) = \text{Quantizedvalue}(I,J) * \text{Quantum}(I,J) \quad (5)$$

Once again, from this it can be seen that when large quantum values are used , this will run the risk of generating large errors in the DCT output during dequantization. Fortunately, errors generated in the high-frequency components during dequantization normally don't have a serious effect on picture quality [16].

Selecting a Quantization Matrix

The quantization tables that are used in this work are created using algorithm (1) where the user inputs a single "quality factor" which should range from one to about twenty-five. In the proposed method we use quality factor 1 to obtain the best quality of image.

Algorithm : Create quantization table [16].

Input: Quality factor

Output: 8 ×8 Quantum matrix

Begin

- Set N=8, For i = 0 to i < N; For j=0 to j < N.
- Quantum [i][j] = 1 + ((1 + i + j) . quality factor).
- Next i.
- Next j
- End

Mod 4 image steganography

Mod4 is a blind steganographic method. The 8×8 blocks of (Quantization Discrete Cosine Transform Coefficients) qDCTCs is divided into 16 groups (sub block) of 2×2 spatially adjacent quantized DCT coefficients (GQC). A GQC (which consists of four elements) is characterized as a valid GQC (vGQC) if it satisfies the following conditions:

$$\left| \{x : x \in GQC, x > f_1\} \right| \geq t_1,$$

$$\left| \{x : x \in GQC, x < -f_2\} \right| \geq t_2,$$

Where |x| denotes the cardinality of the set x. ϕ_1 And ϕ_2 are magnitudes that govern the coefficients to be modified. t_1 and t_2 are the positive thresholds indicating

if the candidate (GQC) is a (vGQC) [17]. The embedding process is performed by modifying the quantized DCT coefficients of (vGQC) so that $\mathrm{mod}(\sigma Q, 4) = xy_i$ .where (σQ) is the sum of the elements of the (vGQC) where ($\sigma_Q = \sum_{i=1, x \in Q}^{i=4} x_i$ (i: is the index of the elements in (vGQC), x ∈ Q, Q is (vGQC))), and xy_i is the ith pair of message bits from the secret message[17].

Shortest Route Modification (SRM).

Mod 4 embeds pairs of message bits into the ordered vGQC. Denote the ith pair of message bits from the secret message by xy_i I {00; 01; 10; 11}. The **(SRM)** is employed to embed each xy_i into the corresponding vGQC. Unlike the ordinary direct modification method, **SRM** leads to lower expected number of modification on the coefficients. The embedding scheme is constrained by SRM [17]. Table (1) shows representative example to embed xy_i=”00”. The first column refers to **Mod (σ_Q, 4)** and it indicates the remainder of the sum of the elements of vGQC divided by 4. The second column $\pm X$ indicates the positive value needed to modify vGQC to hide the secret message and made **Mod (σ_Q, 4)**=”00”.similarly,the third column $\mp X$ indicates the negative value needed to modify vGQC to hide the secret message .To ease understanding to this method there are some definitions that are used [17] :

$$P := (p : p \in Q, p > \phi_1)$$
$$N := (n : n \in Q, p < -\phi_2)$$

And reliable the elements in P and N so that $p_1 \geq p_2 \geq p_3 \geq p_4$ And $|n_1| \geq |n_2| \geq |n_3| \geq |n_4|$ it oblivious that t_1+t_2 £ |N|+|P| £ 4

SRM determines the route for modification(s) as follows:

1. If $\pm X = \mp X$ no changes are made. Done
2. If $\pm X > \mp X$, subtracting 1 from n_1 is the shortest subtraction route.
3. If $\pm X < \mp X$, adding 1 to p1 is the shortest addition route.
4. If $\pm X = \mp X = 2$ there are six case to consider

Case1: if (|P|, |N|) = (1, 1) only P_1 and n_1 exist.
If $P_1 >= |n_1|$, $P_1 = P_1+2$. Otherwise $n_1 = n_1-2$

Case2: if (|P|, |N|) = (2, 1) only P_1, P_2 and n_1 exist.
Let $P_1 = P_1+1$, $P_2 = P_2+1$, n_1 is left unmodified.

Case3: if (|P|, |N|) = (2, 2) only P_1, P_2, n_1 and $n_2$exist.
If $P_1 >= |n_1|$, $P_1 = P_1+1$and $P_2 = P_2+1$.
$n_1 = n_1-1$ and $n_2 = n_2-1$

Case4: if (|P|, |N|) = (1, 2) only P_1, n_1 and n_2 exist. Let $n_1 = n_1-1$, $n_2 = n_2-1$, P_1 is left unmodified.

Case5: if (|P|, |N|) = (3, 1) only P_1, P_2, P_3 and n_1 exist.
Let $P_1 = P_1+1$, $P_2 = P_2+1$.
P_3 and n_1 are left unmodified.

Case6: if (|P|, |N|) = (1, 3) only P_1, n_1, n_2 and n_3 xist.
Let $n_1 = n_1-1$, $n_2 = n_2-1.n_3$ and p_1 are left unmodified. The most important part of Mod-4 embedding algorithm is the modification of quantized DCT coefficients. The following rules are enforced during modifications of the quantized DCT coefficients vGQC:

1. Ordering the positive coefficients in (vGQC) in decreasing order.

2. Ordering the negative coefficients in (vGQC) in ascending order.
3. Coefficient with magnitude less than 2 is ignored.
4. Magnitude of a coefficient is always increased, i.e., addition to positive coefficient, and subtraction from negative coefficient.
5. Coefficients with larger magnitudes are modified first [17].

Proposed public key Steganography method

For most images, much of the signal energy lies at low frequencies (corresponding to large DCT coefficient magnitudes); these are relocated to the upper-left corner of the DCT. Conversely, the lower-right values of the DCT array represent higher frequencies, and turn out to be smaller in magnitude, especially as *u* and *v* approach the sub image width and height, respectively [181].Low frequency in transformed image is more sensitive to modifications of the histogram, such as contrast/brightness adjustment, gamma correction, histogram equalization, and cropping [19]. In general, the (HVS) is much more sensitive to the values in the Low-frequency components than those in the higher frequencies; distortion in high-frequency components is visually acceptable and non imperceptible [13].the proposed method which consists of four phases:

1. **Secret key Generation and Coding Process**
2. **Public key Generation and Embedding process.**
3. **Extracting process.**
4. **Decoding process.**

Secret key Generation and Coding Process

A proposed equation is used to generate the secret key described in equation (6)

Secret key= 2*NL (6)

Where NL represent the length of the a string of a predefined number (n) of bits of the binary secret message. To increase the levels of the security in the proposed method a proposed coding algorithm is used. This algorithm will add some of complexity on receiver side in extraction of secret message because if the attackers can make successful attack on the system and extract the binary secret message, the resulted binary string can not give the exact message, because it is not direct representation of decimal values of secret message

Algorithm : Coding Process

Input: Decimal value the character of secret message, n, positive integer number

Output: secret key

*Step1: Take the decimal values of binary character of secret message called it (**DV**).*

*Step2: Convert (n) from decimal form to binary form and compute the length of the resulted string and called it **(NL).***

*Step3:Compute and save the product of division the **(DV)** by (n) and call it **(R1).***

*Step4:Compute and save the product of the reminder of division the **(DV)** by **(n)** and called it* **(R2).**

*Step5:Convert **(R1)** from decimal form to binary form and denote the resulted string of bits by **(S1)** and make its length equal to **(NL)** by adding **0's** to the left of it.*

*Step6:Convert **(R2)** from decimal form to binary form and denote the resulted string of bits by **(S2)** and*

*make its length equal to **(NL)** by adding **0's** to the left of it.*
*Step7:Make concatenation between two resulted strings **(S1)** and **(S2).***
Step8:Save the resulted string.
Step9:End.

Public key Generation and Embedding process

The general structure of the embedding algorithm is considered as **public key** used in embedding process. The main operation of the embedding process in cover transfer media is that embedding will be performed in frequency domain in general and in discrete cosine transform of gray scale cover image, the embedding processes which consist of sub processes which are:

1. **Transformation process.**
2. **Quantization process.**
3. **Hiding process**.
4. **Dequantization process.**
5. **Inverse Transformation process.**

In this stage the cover image is divided into 8×8 non –overlapping blocks that are transformed using 2-D (DCT). The embedding will be performed in YC_rC_b color space.

1. Quantization Process.

The quantization process here is not for the purpose of data reduction such as it is used in data compression, but here it is used for frequencies recognize.

These numbers are considered middle and low frequencies and it is exploit during embedding process (This ensures that information is stored in significant parts of cover-image, and if stego image is compressed the embedding information will not be damaged completely

Hiding Process

At this process the quantized transformed block is divided into 16 groups (sub block) of 2×2 non-overlapping spatially adjacent quantized DCT coefficients (GQC). Each time one of 2×2 sub blocks will check if it satisfies the conditions in (1) to be (vGQC).

$$\left| \{x: x \in GQC, x > \phi_1\} \right| \geq t_1, \quad \text{and} \quad (1)$$
$$\left| \{x: x \in GQC, x < -\phi_2\} \right| \geq t_2,$$

In the proposed system that uses mod 4 in embedding algorithm the value of (ϕ_1 and $-\phi_2$) will be secret key used to determine the location to be valid for modifying to contain 2-bits of secret message or not, If it's valid for embedding the system takes 2-bits from the binary form of secret message file and codes them using **Not logic operation** for example if the 2-bits of binary form of secret message are ="00" (input to **Not logic operation**) and the output will be"11". and the output will be used in modify (vGQC) using mod 4 technique and SRM. During implementation of the mod 4 technique the 2-bit of binary message is converted to decimal form (Decimal Message (DM)). Then compute (σQ)(where $(\sigma Q)$is the sum of the elements of the (vGQC) where ($\sigma Q = \sum_{i=1, x \in Q}^{i=4} x_i$ (i: is the index of the elements in (vGQC), x ∈ Q, Q is (vGQC))), then compute the remainder of division sum by 4 (**Mod (σQ , 4)**).After that check if **Mod (σQ , 4)**is equal to (DCM), if yes then there are no modifications carried out**,** Otherwise using Mod 4 and SRM scheme.

Dequantization

In this stage the dequantization process will be performed on quantized transformed block after it passes through the process of modification, where the inverse of operations that are performed in quantization stage will be performed here. To perform dequantization process equation (5) will apply using this block and the same quantization table that is used in quantization process.

InverseTransformation Process

The dequantized 8×8 block is considered input to this stage, IDCT is applied to each block to retrieve the data of image from transformed DCT coefficients using equations (2),(3).

Algorithm:TheEmbedding Algorithm

Input: Message (Plain text), Image (cover).

Output: Stego-image.

Step1:Get color of pixels(R, G, B).

Step2:Converted RGB values of the original image into YC_rC_b color space

Step3:Luminance (Y) domain is divided into blocks of size 8x8.

Step4:

4.1Set **j** to the number of blocks,

4.2 for i = **0 to j-1 do**

· of 2×2 non-overlapping spatially adjacent quantized DCT coefficients (Apply 2-D discrete cosine transform (DCT) using equation (1), (2) to the taken block to produce DCT-coefficients.

· Apply quantization to transform block using equation (4).

· Quantized transformed 8×8 blocks is divided into 16 group **(sub block**) GQC).

· **for N= 0 to 15 do**

· Check if (GQC) is valid for modification to contain the 2-bits of binary secret message (vGQC) (it is considered valid if it satisfies the Specific conditions)then

- Take 2-bits from secret message and input them to **Not logic operation** where **(10 →01, 01→10,11→ 00,00→11).**
- Apply the modification scheme to (vGQC) using **SRM**

End if.

Next N

· Apply dequantization to quantized transformed 8×8 block by applying equation (5).

· Apply IDCT to the block of image using equation **(**2), (3) without loosing of data. Step1:

Next i

Step5:YC_rC_b color space is converted back to RGB color space Save the resulted Stego-image.

Step6:End.

Extracting Process

On the other hand the secret data inside stego-image is extracted using Extracting algorithm. This step is the first step on the receiver side. When the receiver receives the image, he loads it in the proposed system, the proposed system automatically applies Extracting algorithm, it searches for hidden secret message in image and the search begins by dividing the image into 8×8 blocks. Then each time one block is taken and (DCT), quantization process is applied to this block and the system begins the extraction of secret message.

Algorithm:Extraction Algorithm.

Input: Received stego - image.

Output: Binary form of secret message.

Step1:Get color of pixels(R, G, B).

Step2:Convert RGB values of the original image into YC_rC_b color space

Luminance (Y) domain is divided into blocks of size 8x8.

Step3:

3.1 Set **j** to the number of blocks,

3.2 **for i = 0 to j-1 do**

3.2.1Apply 2-D discrete cosine transform (DCT) to the taken block to

produce DCT-coefficient.

3.2.2Apply quantization to transform block using equation (4).

3.2.3Quantized transformed 8*8 blocks is divided into 16 groups (sub block)

of 2×2 non- overlapping spatially adjacent quantized DCT coefficients

(GQC).

3.2.4For **N= 0 to 15**

3.2.4.1Check if GQC is valid (vGQC) if it satisfies the condition(1)

3.2.4.2 compute the sum of coefficients.

3.2.4.3 Take the remainder of division this sum by 4 (**Mod (∝Q , 4)**) and convert it to binary.

3.2.4.4 Take the extracted 2-bits from secret message and input them to **Not logic operation** where (**10→01, 01→10,11→00,00→11**)

3.2.4.5 Add the 2-bits to string of bits of binary secret message

3.2.5**Next N**

Step4:Next i

Step5:End

Decoding process.

The receiver after completely extracting the binary secret message must find out the secret number that helps in retrieve the secret message , this secret key using equation (6).The extracted binary string that is resulted from extraction process is considered input to this sub process, it is used with **n** (public key of encryption method) to be input to decoding algorithm that uses equation () to extract the decimal values that represent values to the characters and symbols of secret message.

Decimal value of secret character= n*R1+R2 (7) Where R1the decimal value of first secret character, and R2 the decimal value of second secret character.

Algorithm: Simple Decoding

Input: Binary string, n , positive integer generated

Output: Decimal value represent character of secret message.

Step1:*Convert (n) from decimal form to binary forms and computes the length of the resulted string and denote it* ***(NL).***

Step2:*Cut a string with length equal to* ***secret key(*** *equation* ***(6))*** *from input binary string and denote it* ***(S).***

Step3:*Divide* ***(S)*** *into two string each one with length equal to* ***(NL)*** *and denote the resulted two strings* ***(S1)*** *and* ***(S2).***

Step4*:Convert* ***S1 (That represents the product of secret character divide (n))*** *from binary form to decimal form and denote the resulted decimal value by* ***(R1)****.*

Step5*:Convert* ***S2 (that represents the remainder of the first value of secret message divide (n))*** *from binary form to decimal form and denote the resulted decimal value by* ***(R2)****.*

Step6*:Use n, (R1) and (R2) as input to the equation (7) to extract the exact decimal secret message* ***[n*(R1) + (R2)]***

Step7:end

Practical Results

This section will present the practical results obtained by embedding secret messages into 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 SNR, PSNR in addition to the secret message length and hiding data rate.

Cover-image-1: From the Table (2) the value of PSNR of cover-image-1 when embedding message with length 346 can quantify the invisibility of embedded secret message in this tested cover by applying the proposed system, these values indicate that these embedded secret messages are imperceptible to the observer and these will lead the system to be secure. Also the values of SNR of cover-image-1 are greater than empirical value for detectability of these cover images if contained secret message embedded or not, where the hiding rate (0.44) of Cover-Image-1 is acceptable. it depends on the noisy area also on the texture in cover-image and last the value of similarity test.(0.9993792) refers to high correlation between cover-image and stego-image. Also from Table (2) for the same cover (cover-image-1) notice length of secret message 129 byte and it less than the number of (vGQC), so the value of PSNR (43.65019) is increased because the modification in cover-image is less ,also the value of SNR (38.35887) will improved and the correlation between cover-image and stego-image increased. So it's clear that as the embedded secret message increases, correlation and PSNR decrease where according to conflict requirements of steganography they are mutually competitive and cannot be clearly optimized at the same time. If a large message is be hidden inside an image. Absolute undetectibility and large robustness cannot require at the same time. A reasonable compromise is always a necessity. On the other hand, if robustness to large distortion is an issue, the message that can be reliably hidden cannot be too long. So the proposed steganographic method will not stress the high payload (capacity) but that should provide imperceptibility to observer and robustness to attack on it.

Cover-image-2: This tested cover image has texture more than cover-image-1 so the capacity will increase and hiding rate of this cover is (0.52) where PSNR and SNR also the correlation between cover-image and stego-image will decrease.

Conclusions

In this work the proposed method of public key information hiding is developed and implemented and the following results are concluded:

1. The proposed system can be defined as a public key steganography system where the key that is used by sender differs from the key that is used by receiver. The general structure of the embedding algorithm is considered as public key used in embedding process, and the secret key that is used in extraction process is represented by (no. bits) and it is computed from equation (6) also the secret parameters (ϕ_1, ϕ_2)are ,used to determine the location of embedded secret message

2. The proposed system is secure where the results obtained from similarity test refer to the correlation values which are obtained is 1. This indicates that the stego-image is similar to its corresponding cover-image.

3. The proposed system is imperceptibility to the observer (Invisibility) and this is indicated by the values of SNR and PSNR.

4. The proposed system have multi level of security for data hiding, First level is achieved by using the proposed coding and secret key generation algorithm, second level is achieved by using proposed embedding algorithm to embed secret messages in the cover image.

5. The proposed method is flexible because the embedded secret message is extracted directly form received stego-image using decoding algorithm and extracting algorithm, so there is no need for the original cover in the extraction process.

6. The capacity of the proposed method depends on the selected cover-image if it has high or middle or low texture and also on the noisy area in cover image.

References

[1] Jennifer Davidson, "An Introduction to Information Hhiding in Digital Data and Some Underlying Mathematics ",Electrical & Computer Engineering Department of Mathematics ,Mathematics Colloquium,2003.

[2] Petitcolas F. A. P., Anderson R. J. and Kuhn M.G., "Information Hiding-a Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, Vol. 87,no.7, PP. 1062-1078, July 1999.

[3] József lenti ,"Steganography Methods", Department Of Control Engineering And Information Technology Budapest University Of Technology And Economics H–1521 Budapest, Hungary ,2000.

[4]W. Stallings," Cryptography and Network Security, Principle and Practice ", Addison Wesley, 1999.

[5]Mangarae A. ,"Steganography FAQ", March 18th 2006 URL:http://www.infosecwriters.com/text_resources/pdf/Steganography AMangarae.pdf

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

[7]Dunbar B., "A detailed Look at Steganographic Techniques and Their Use in an Open-Systems Environment", SANS Institute, 2002.

[8]Rastislav hovančák, peter foriš, dušan levický," Steganography Based on DWT Transform", Department of electronics and multimedia telecommunications Technical University of košice,2007.

[9]Krenn R.," Chapter 1:Steganography and steganalysis", 2004. http://www.krenn.nl/univ/cry/steg/article.pdf

[10]Wang H., Wang S., "Cyber Warfare: Steganography vs. Steganalysis ", Communication of the ACM, vol. 47, No. 10, October 2004,

[11]Anil Kumar, and Navin Rajpal, "Secret Image Sharing using pseudo-Random Sequence" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.2B, February 2006 ,

[12] Syed Ali Khayam ," Seminar-1:The Discrete Cosine Transform (DCT): Theory and Application1",Department of Electrical & Computer Engineering,Michigan State University , (ECE 802 – 602: Information Theory and Coding),March 10th 2003.

[13]Chin-Chen Chang, Chia-Chen Lin , Chun- Sen Tseng , Wei Liang

Tai ,"Reversible hiding in DCT-based compressed images", Information Sciences 177 (2007) 2768–2786 AN (International Journal),2007.

[14]Dave Marshall "The Discrete Cosine Transform (DCT)",2001
URL: http://www.cs.cf.ac.uk/Dave/Multimedia/node231.html - Cached

[15]Pennebeaker ,W.B., J.L.Mitchell, "JPEG: Still Image Data Compression Standard",New York ,Van Nostrand Rrinhold,1993

[16] Mark Nelson And Jean-Loup Gaily ," The Data Compression Book", second Edition , 2000.

[17]Wong K. [a,] , Qi X., Tanaka K. ,"A Dct-based mod4 steganographic method", [a]Faculty of Engineering, Department of Electrical and Electronics Engineering, Shinshu University, 4-17-1 Wakasato,Nagano 380-8553, Japan ,[b]Department of Computer Science, Utah State University, 84322 Logan, Utah, USA , Signal Processing Journal 87 (2007) 1251–1263, (2006) .

[18]Ayhan Yilmaz, "Robust Video Transmission using Data Hiding", M.SC. Thesis , The Department Of Electrical And Electronics Engineering, The Graduate School Of Natural And Applied Sciences Of The Middle East Technical University, September 2003.

[19]Chirag N. Paunwala and Mita C. Paunwala,"Secure Information by Digital Data Embedding in Transform Domain Techniques" , Conference on Next Generation Communication Systems : ICONGENCOM-2006.

Table (1) Modification SRM scheme for xyi=00			
$\mathrm{mod}(\sigma Q, 4)$	$\pm X$	$\mathrm{m}\ X$	**Possible routes**
00	**0**	**0**	**No change**
01	**+3**	**-1**	**-1 or +3**
10	**+2**	**-2**	**+2 or -2**
11	**+1**	**-3**	**+1 or -3**

Table (2) Results of applying the proposed method

Cover Image Name	Length Of Secret Message (BYTE)	Signal To Noise Ratio (SNR) (DB)	Peak Signal To Noise Ratio (PSNR) (DB)	Similarity	Hiding Rate
Cover-Image-1	342	37.30304	42.59436	0.9993792	0.44
Cover-Image-1	129	38.35887	43.65019	0.9995525	0.44
Cover-Image2	342	35.19387	40.67392	0.9990941	0.52
Cover-Image2	129	36.85172	42.32631	0.9993608	0.52

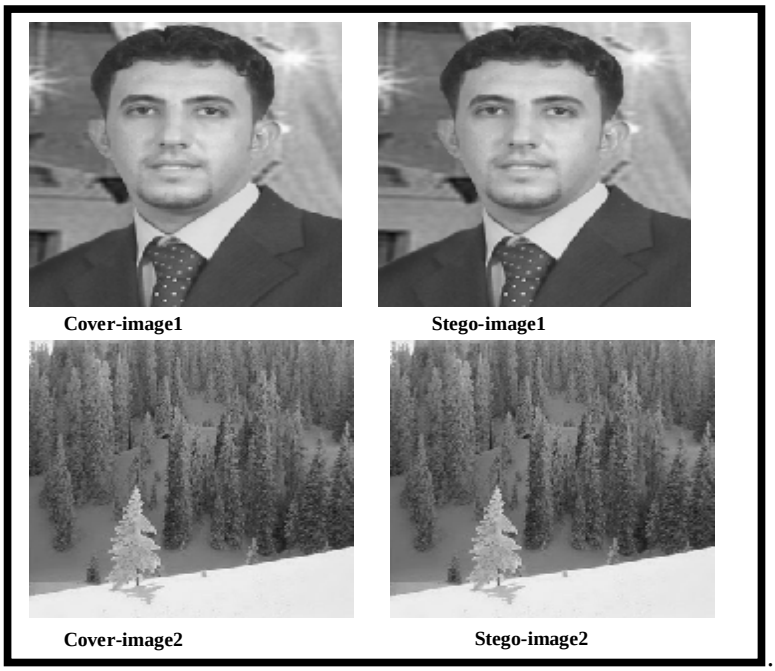

Figure (1) cover and stego-image that result from applying the proposed