# Concealment of Information in Digital Image

**Aladdin Jamel A. Al-Naji** **Maysaa Hameed Abdul Ameer**

Received on :3/7/2005
Accepted on :4/5/2006

**Abstract**

Transmission of secret information provides an interesting problem space for investigating information hiding. In this paper we present a proposed hiding system **"Single and Double Hiding (SDH)",** which can be used to embed text file in digital image and all will be hide in cover image or hide text file in cover image only. **SDH** is a flexible system, because its used variety types of image file format with different size such as (BMP, JPEG, GIF, and GIF-Animation), the proposed system gives a good result instead of sending encrypted message that draw suspicion, this is where Steganography can come into play.

The system use cryptography, compression, and image filtering as auxiliary processes to recover the weakness in the previous methods, and its used three invented methods for hiding, which are Hiding in Edge Points, Direct Hiding, and Hiding with Reference Images.

We present a comparison between (stego and cover) image through using the histogram and the difference distortion metrics, which are (**MSE**, **SNR**, **LMSE**, **PSNR**, **NC**, and **CQ**). Finally from the evaluation step the **SDH** system achieved the main goal of Steganography, since the resulting images didn't draw any suspicion.

**الخلاصة**

نقل المعلومات السرية يوفر مجال شيق لدراسة علم الإخفاء. في هذا البحث نستعرض نظام إخفاء وهو **"الإخفاء الفردي والمزدوج "**,يستخدم هذا النظام لاخفاء نص صريح في صورة وسطية ثم نخفي هذه الصورة في صورة اكبر منها حجما أو أن نخفي النص الصريح مباشرة في الصورة. النظام المقترح هو نظام مرن يستخدم انواع مختلفة من ملفات الصور ذات الاحجام المختلفة مثلا (BMP,JPEG,GIF,GIF-animation )، وكذلك اعطى النظام المقترح نتائج جيدة لاخفاء المعلومات وارسالها بدل من ارسال رسالة مشفرة التي تثير الشكوك عند ارسالها ولهذا السبب وجد علم الاخفاء.

النظام المقترح يستخدم التشفير والضغط ومعالجة الصور لتجنب الضعف في الطرق السابقة, واقترحت في النظام ثلاث طرق لإخفاء البيانات وهي: الإخفاء في مناطق الحدود والإخفاء المباشر والإخفاء بواسطة مرجع الصور.

النظام المقترح حقق الهدف من الاخفاء وهو ان الصورة الناتجة لاتدعو الى الشك ابدا وذلك من خلال تقييم النظام عن طريق المقارنة مابين الصورة الأصلية والصورة التي حصل فيها الإخفاء وذلك باستخدام المدرج التكراري وبعض المقاييس الاحصائية(MSE, SNR, LMSE, PSNR, NC, and CQ) التي أثبتت ان النظام حقق هدف الاخفاء.

## 1. Introduction

The Internet and the World Wide Web (WWW) have revolutionized the way in which digital data is distributed. The wide spread and easy access to multimedia content has motivated development of technologies for information hiding [1]. The only way to hide the fact that you are sending a secret message is to pass it off as something boring and ordinary so it does not arouse suspicion [2].

Information hiding is the practice of making imperceptible changes in digitized media to hide message [3]. Two basic approaches of information hiding "Steganography" and "Digital Watermark", Steganography is an important sub-discipline of an information hiding, it is the art and science of hiding data into innocent-looking cover-data so that no one except the intended receiver can detect the very existence of the hidden data [4, 5, 6]. Steganography utilize the digital media such as text, image, audio, video and multimedia to be the cover-data to hide the private message [7], the private message could be plaintext, cipher text, image or any thing that could be embedded into bit stream [8].

Two types of Steganography **Classical** and **Modern**, the security of the classical Steganographic system relies on the secrecy of the encoding system, but the modern Steganography relies on the secret information shared such as the stego-key [9], Figure (1) shows the Steganographic system (Stegosystem)

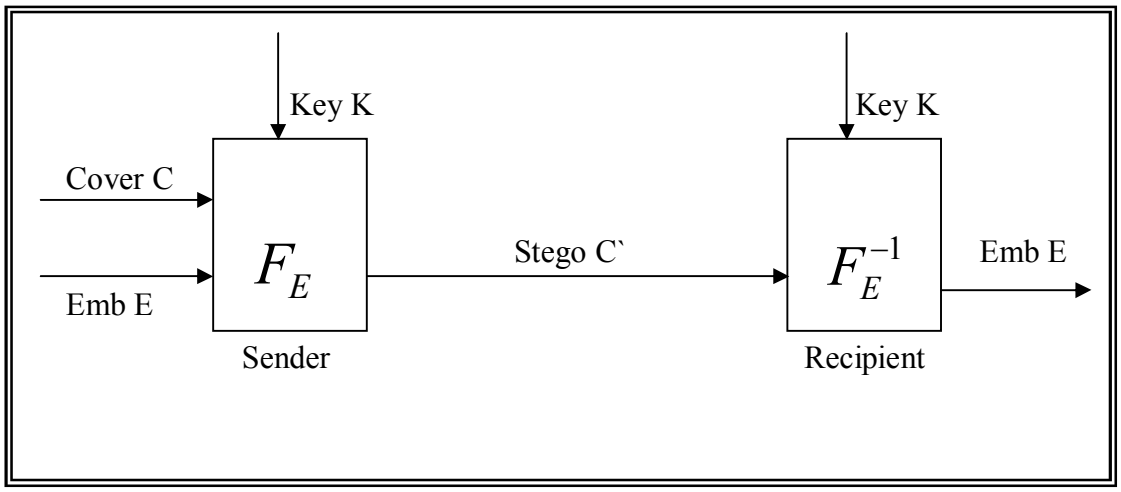


**Figure (1) The Stegosystem**

The Stegosystem has the following components:

*Emb* The message to be embedded.

*Cover* The data in which emb will be embedded.

*Stego* A modified version of cover that contains the embedded message.

*Key* Additional secret data that is needed for the embedding and extracting processes and must be known to both.

$F_E$ A Steganographic function to produce the stego cover as output.

$F_E^{-1}$ The inverse Steganographic function [10, 11].

Steganography in digital image has come quite far in recent years so digital image is a good candidate for hiding information, because there are a lot of redundant portions in image data that can be changed with out altering the image quality [12]. Hiding in image is non causal and data hiding techniques can have access to any pixel or block of at random [13, 14].

Hiding in digital image, is a highly multidisciplinar field that combines image and signal processing with cryptography, communication theory, coding theory, signal compression. Tremendous recent interest in this field is a quite understandable because of the wide spectrum of applications it addresses [15].

## 2. The Proposed System

The proposed system called **Single and Double Hiding (SDH),** that capable of hiding two types of text file (Arabic and English) text file. In **Single Hiding (SH)** one secret file is hidden in cover image, but in the **Double Hiding (DH)** two different files are hidden in the cover image, they are text file and image file.

**SH** is designed for hiding information in one step. This step will hide the secret message in cover image by providing one of the three techniques, which are Hiding in Edge Points, Direct Hiding, or Hiding with Reference Images. They are different from each other in the manner of hiding process and in the number of bits that are used for hiding.

**DH** is designed for hiding information in two steps, the first step hide the text file in image file (cover1) as in **SH**, this cover could be BMP, JPEG, GIF file format, and the second step hide the produced stego image in cover image (cover2) by using two hiding techniques which are Hiding in Edge Points, or Hiding with Reference Images. In **DH** the text file is the secret file that the sender wants to transmit to the receiver but the image file (cover1) is a middle media used to hide the fact of the secret file if there is a chance to retrieve the secret file from the cover image.

The cover image for both types of hiding, will be a still-image (BMP, JPEG, GIF) or an animated GIF image to produce the final stego image, and the pixel format of the used image is either 8-bit or 24-bit color image.

Compression and encryption are two secondary processes which are implemented before each hiding step, the sender and the recipient are agree on the compression, encryption, type and method of hiding, and the number of the reference images (if its needed) by using a signature. The basic steps of hiding and extracting in the **SDH** system are:

Compression ⟶ Encryption⟶ Hiding [Single or Double]⟶Stego-Image

Stego-Image⟶ Extracting [Single or Double]⟶Decryption ⟶ Decompression

Figure (2) express the block diagram of the hiding process in the **SDH** system.

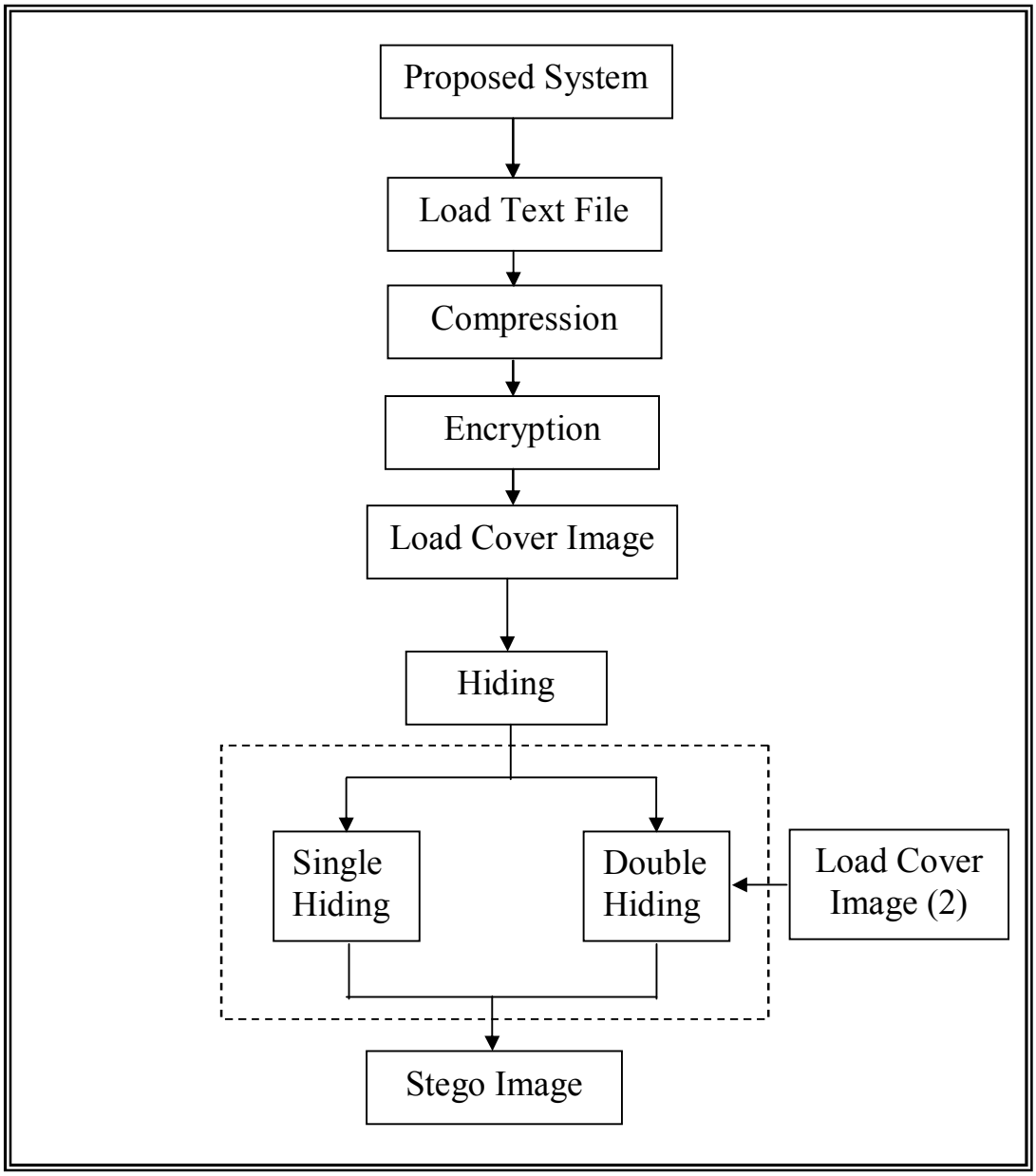


**Figure (2) The Block Diagram of the Hiding Process**

Finally the proposed system uses an e-mail server to send the stego image between the sender and the receiver, the stego image will be sent as an attachment file. The **SDH** system includes three common phases, in the following a description of each phase:

## 2.1 Compression Phase

In this phase, the secret text file (Arabic or English) will compress by using one of the three compression methods, which are: ZIP, RAR, or LZH. The sender is free in choosing the type of the compression method.

This phase is used to support the secret message by reducing its size to achieve better hiding, when we reducing the size of the message, we will get better hiding [16].

## 2.2 Encryption Phase

The compressed text will be encrypted using one of the encryption

algorithms, which are: DES, IDEA, Blowfish, and RSA (for more information see [17]). The sender is free in choosing the encryption algorithm, this phase will increase the system's security.

Each encryption algorithm needs a secret key for example ***"My Thank for supervisor"*** as a secret key to be used with the chosen algorithm, this key could be changed but the sender and the receiver have agreed first on the changed key.

## 2.3 Hiding Phase

This phase will hide the encrypted file in cover image to gain stego image. The hiding operation in BMP and GIF images will be in pixel domain, but in JPEG image the hiding operation will be in the transform domain, because if the hiding process is in pixel domain the secret information will be damaged from the lossy compression.

The sender and the receiver have a CD of images (reference images) that was agreed between them to hide and extract the information. In the following a description of both types of hiding (**SH** and **DH**) used in the proposed system:

*A. Single Hiding (SH)*

This type consists of three methods to hide the encrypted data in cover image, in the following a description of each method used in **SH**:

**1) Hiding in Edge Points**

In this method the hiding operation is expressed by the following steps:

**i) Edge detection test algorithm**

The testing process is done by applying the edge detection filter (Frei-Chen) on the cover image, because its produce more edge points that will help us in the hiding process. Figure (3) is a Frei-Chen filter the white color in the edge detection image is the edge points.

The test algorithm will check the produced image if the percentage of the white color is greater than the percentage of the black color then this image is suitable for hiding process, because the secret message will be hidden in the edge points, so as much as the edge points (white color) are greater than the black color as much as we get better hiding.

**ii) Hiding step**

This step will hide a byte from the compressed/encrypted text in the cover image, it will search for the appropriate edge pixel that met the condition of hiding, this condition is:
"The pixel before **P**b and the pixel after **P**a of the edge pixel are must be an edge pixels too", when this condition is met in the chosen pixel, then store the position of the pixel in an array to help us when we return to the original image and use it to hide a byte from the secret file in the pixel of that position, the hiding process is illustrated below:

**If** (pixel format 8-bit) **Then**
**S**ubstitute the secret byte in the index values.
**Else**
**If** (pixel format 24-bit) **Then**
**S**ubstitute the secret byte in the blue values.

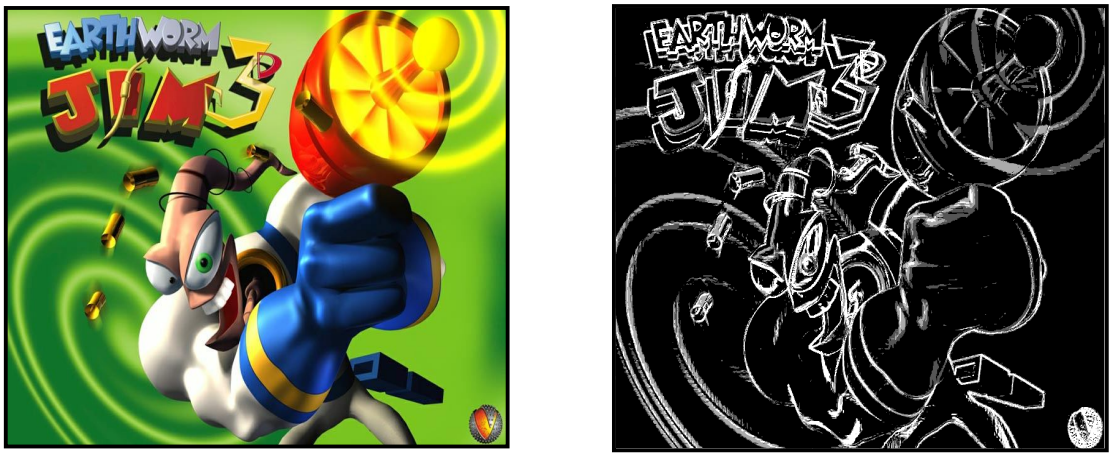


**Figure (3) The Original Image and its Edge Detection**

**2) Direct Hiding**

In this technique, the hiding process start when we partitioned the cover image into blocks, each block encodes exactly one bit from the secret message. The hiding operation in this method is illustrated in the following steps:

**i) Block test algorithm**

In this test the cover image is partitioned into blocks of size 8*8 and if the number of the blocks are greater than or equal the number of the bits in the secret message, then this image is suitable for hiding operation.

**ii) Hiding step**

The hiding operations of the message bits begin with using the secret key of the encryption phase to select randomly the block **b**i. After choosing the block, the hiding operation need two pixels in the same block, the first pixel **P**1 chosen randomly by using the same key and the pixel followed by the first pixel **P**1 is the second pixel **P**2. To hide the secret bit in the block, apply the hiding condition:

**If** (the secret bit = 0) **Then**

$P_1 < P_2$

**Else**

**P**1 > **P**2

**3) Hiding with Reference Images**

This method depends on extracting the positions of the hidden information by using CD of images (reference images) that was agreed between the sender and the receiver. The testing and the hiding steps are explained below:

**i) Reference images test algorithm**

This test consists of finding which of the reference images that have all the values of the secret information.

**ii) Hiding step**

This method will take a byte from the secret information and look for a match of this byte in reference images, after finding the match, we take the position of the pixel and then hide the secret positions in the borders of the cover image.

There is a new method for hiding the secret text in the animation cover. This method doesn't need the reference images but the reference images would be from the cover itself, the first image from the file could be the cover image for hiding the positions and the reference images are the rest of the images in the same file.

*B. Double Hiding (DH)*

**DH** is the second type of hiding phase, this type consists of two methods, each method need two cover images they are cover1 and cover2, the cover1 must be smaller than cover2 and these covers could be of different size. In the following a description of each method used in **DH**:

**1) Hiding in Edge Points**

This method hide the encrypted text file in an edge detection image, and then the produced stego image will be compressed and encrypted again to be ready for hiding in the second cover image (cover2), to produce the final stego image. The hiding process is the same as in **SH**.

**2) Hiding with Reference Images**

This method depend on reference images to hide the encrypted text in cover1, after the first hiding process (as in **SH**) the produced stego image1 is compressed and encrypted again to be ready for the second hiding after loading the cover image (cover2).

Generally the hiding process in GIF animation file for both (**SH and DH**) is done by partitioned the secret data into several parts, these parts are equal to the number of the images in GIF file.

In the extracting process the extractor must have the stego image and apply the steps of the system in a reverse manner to extract the secret text file.

## 3. The Results of the Proposed System

In this section the results of the **SDH** system is expressed in the following points:

1- Open the secret text file as in Figure (4), then compress and encrypt the text file, to produce the secret data.

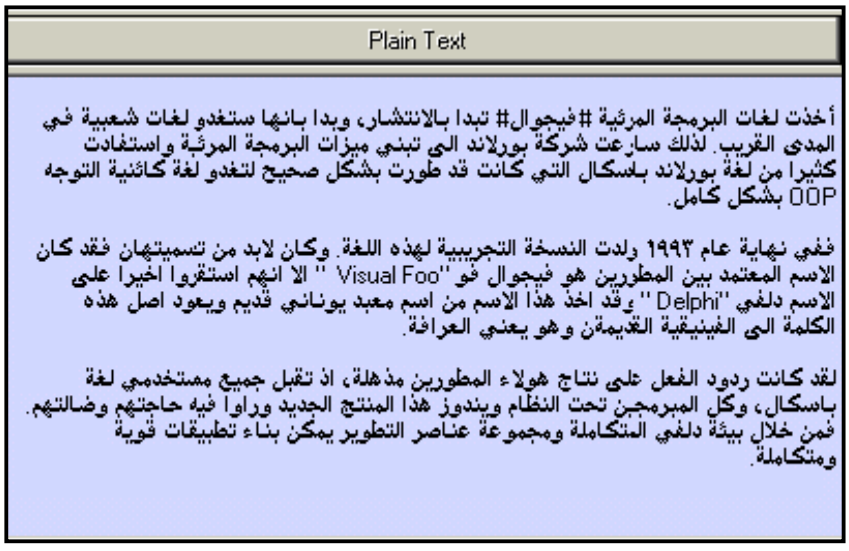


**Figure (4) The Secret Text File**

2- The secret data will be hidden in cover image. Figure (5) to Figure (7) explained the cover image and the stego image of the proposed system.


**Figure (5) The Direct Hiding**


**Figure (6) E.D Method for DH**


**Figure (7) Reference Method for DH**

3- In this step, the hiding method (Direct Hiding) that expressed in Figure (5) will be evaluated by using the histogram and the quantitative metrics as in Figure (8) and table (1). The quantitative metrics are considered as means of signal measurement that can be used to measure the amount of the error in the stego image, in other word they are useful measures in comparing between the stego image and cover image, and they offer a simple and convenient for evaluating the information loss [18].

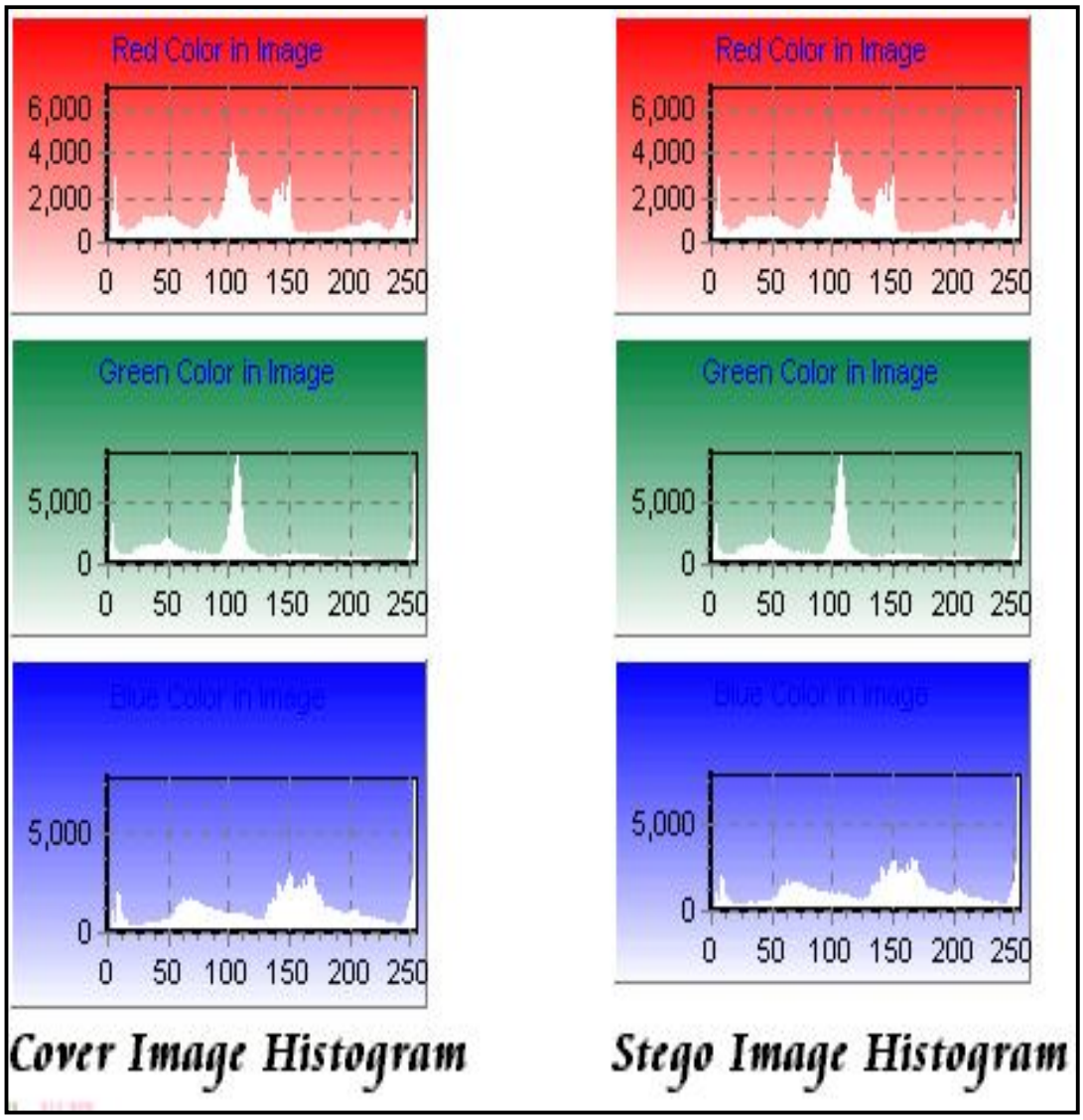


**Figure (8) The Histogram of Hiding Process**

From Figure (8) the histogram of the stego image is quite similar to the cover image.

**Table (1) The Quantify Measures**

| | Red | Green | Blue |
|---|---|---|---|
| **MSE** | **1** | **3** | **2** |
| **LMSE** | **330** | **370** | **240** |
| **SNR** | **6653319** | **5504389** | **33243124** |
| **PSNR** | **6355389** | **6964552** | **55242191** |
| **NC** | **2** | **2** | **2** |
| **CQ** | **111** | **112** | **113** |

- **MSE (Mean Signal Equation)** in this measure, the smaller value of the MSE, the better stego image represents the cover image, as in the table the **SDH** is not detected.
- **LMSE (Laplace Mean Signal Equation)** this measure is mixed between the Laplace operator and MSE measure, with this measure the small number represent the better hiding method, but the **SDH** system will be detected.

- **SNR (Signal to Noise Ratio)** with this measure a large number implies a better stego image, the **SDH** will not be detected.
- **PSNR (Peak Signal to Noise Ratio)** the same as in SNR, the **SDH** system will not be detected.
- **NC (Normalize Correlation)** this metrics shows the amount of correlation between the original and the stego image, The **SDH** will not be detected.
- **CQ (Correlation Quantity)** as in the table the **SDH** system will be detected, because the pixel values are big numbers.

## Conclusions

In the following some points concluded from the **SDH** system:

1. The **SDH** system can be defined as modern Steganography, since it shares secret information between sender and the receiver, and in this system there is no need to transmit the original cover image and the secret key to extract the secret information.

2. The **DH** gives to the secret information (text-file) a high ratio of protection, because the system repeat the hiding process twice, beside this the proposed system used compression and encryption which used to increase the difficulty for the attacker to rend the hidden data from any type of hiding proposed in the system, not just from **DH**.

3. **SDH** system use more than one compression tool and encryption method to compress and encrypt the secret information before hiding it, so this processes increasing the security of the system, getting better hiding, increasing the hiding ratio for the secret information, and it is more difficult for the attacker to reach the original information.

4. The hiding operation in animated cover file is better than hiding in still cover image, because of the large capacity of this cover that improved the hiding process by hiding very little data in each frame of the cover.

5. The size of the embedded text does not affected the speed of the system, and the system improved it's flexibility by using different types of image file formats, which are BMP, JPEG, GIF, and animated GIF file.

6. From the evaluation of the system, the hiding methods improved their activity in the embedding, by using the histogram and the difference metrics

7. Hiding in JPEG file image make the proposed system to be immune against the compression attack.

## References

[1] J. J. Chae, and B. S. Manjunath, "Data Hiding in Video", University of California, 2000.

[2] J. Rimell, "Data Hiding Inside TIFF Images", Tohn's College, Cambrige, England, 1997. { http:// ban.Joh.com.ac.uk/~jjr23 }

[3] M. L. Miller, and J. A. Bloom, "Computing the Probability of False Watermark Detection", Information Hiding, Third International Workshop, Lecture Notes in Computer Science, Vol. 1768, PP. 146-156, Springer, 2000.

[4] N. Provos, and P. Honeyman, "Detecting Steganographic Content on the Internet", University of Michigan, 2001.

[5] S. Katzenbeisser, and F. A.Petitcolas, "Information Hiding Techniques for

Steganography and Digital Watermarking", Artech House,2000.

[6] T.Mittelholzer, "An Information-Theoretic Approach to Steganography and Watermarking", Information Hiding, Third International Workshop, Lecture Notes in Computer Science, Vol. 1768, PP. 1-16, Springer, 2000.

[7] S. Areepongsa, Y. F. Syed, N. Kaewkamnrd, and K. R. Rao, "Steganography For A Low Bit-Rate Wavelet Based Image Coder", University of Texas at Arlington, 2000, PDF.

[8] N. F. Johnson, and S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", Information Hiding, Second International Workshop, Lecture Notes in Computer Science, Vol. 1525, PP.273-289, Springer, 1998.

[9] N. Provos, and P. Honeyman, "Detecting Steganographic Content on the Internet", University of Michigan, 2001.

[10] S. Hetzl, "A Survey of Steganography",2002.{http://steghide . sourceforge.net/steganography/ survey/ }

[11] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wike, G. Wolf, "Modeling The Security of Steganography Systems", Information Hiding, Second International Workshop, Lecture Notes in Computer Science, Vol. 1525, PP. 344-354, Springer, 1998.

[12] E. Kawaguchi, "A Large Capacity Steganography", Knowledge Engineering Lab, Kyushu Institute of Technology, Japan,2001. {http:// www. Know.comp. kyutech.ac.jp/BPCSe/ }

[13] T. M. Blacke, "Steganalysis",2001 , PDF. {http://rr.sans.org/topappers/ topapers_list.php }

[14] D. Sellars, "An Introduction to Steganography",Internet survay, 2000.

[15] J. Fridrich, "Application of Data Hiding In Digital Images", 1998, PDF. {http://ssie.Binghamton.edu/~jirif }

[16] D. Saloman, "Data Compression", California State University, Springer, 1998.

[17] B. Schneier, "Applied Cryptography Protocols, Algorithms and Source Code in C", John Wiley And Sons, Inc. Publishing, 1997.

[18] S. Katzenbeisser, and F. A. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, 2000.