Ministry of Higher Education & Scientific

Research University of Babylon

Science College for Women

Computer Science Department

Secret Data Hiding Based on Encryption and Hash Function

Research presented to College of Science for Girls
In Fulfillment of the Requirement For the Degree
of B.SC. Of Science in Computer

BY

Zaynab Saad

Supervised by

Dr. Suhad Ahmad Ali

1443 هجري

2023 م

بسم لله الرحمن الرحيم

إنّا فتحنا لك فتحاً مبينا (١) ليغفر لك الله ما تقدم من ذنبك وما تأخر ويتمّ نعمته عليك ويهديك سراطاً مستقيما (٢) وينصرك الله نصرا عزيزا(٣) هو الذي أنزل السكينة في قلوب المؤمنين ليزدادوا إيمانا مع إيمانهم ولله جنود السموات والأرض وكان الله عليما حكيما (٤) ليدخل المؤمنين والمؤمنات جنات تجري من تحتها الأنهار خالدين فيها ويكفر عنهم سيئاتهم وكان ذلك عند الله فوزا عظيما (٥)

صدق الله العلي العظيم

شكر وتقدير

من علمني حرفا ،،، ملكني عبداً

أحمد اللّٰه عز وجل وأشكره على كل نعمه التي منَ بها عليَّ فهو المنعم المعطي ،،

كما وأتقدم بأجمل عبارات الشكر والتقدير الى كل من قدم لي العلم

وأخص بالشكر الجزيل أولاً :

أستاذتي التي تحملت مني الكثير الدكتورة الطيبة "سهاد احمد علي "

الاهداء

اليك دون غيرك ...... يابن فاطمة البتول

لا لشيء .... الا لأنك قران تنير العقول

و لأنك ياحسين..... إمام تواصل بعد الرسول

إليك يامن استمطرت من نحره:

آيات السماء

وقيم وإباء

وهمم وعطاء

حينها.... نعم حينها كان ختام النزول

إليك يا أمة الشموخ.... من عبد عاشق خجول

يسعى بكل جوارحه يريد اليك الوصول

لا لشيء .... الا لأنك قران تنير العقول،،

......

والى مولاي بقية الله الأعظم

ولي نعمتي سيدي الحجة بن الحسن العسكري "عجل الله فرجه الشريف"

Abstract

Steganography is a branch of data-hiding science which aims to reach a desirable level of security in the exchange of private military and commercial data which is not clear. In this project, a study was made of hiding binary image in another image which is called the cover image . The system have two main Participants which are the sender and reciever. Sender will apply embedding method, this method consist of many stages. The binary image will encrypted using Arnold encryption method which is applied to incresed the security. To obtain the sego image, the encrypted image is embedded in cover image using random location based on hash function. At the reciever side, the extracting method will be applied in order to extract the secret message (embedding image). This method consist of the same stags in the embedding method but it applied inversly.

Chapter One
Introduction

Chapter One

Introduction

1.1 Introduction

The word steganography is derived from the Greek words stegos meaning cover and grafia meaning writing defining it as covered writing. In image steganography the information is hidden exclusively in images. Steganography is the art and science of secret communication .It is the practice of encoding / embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stegomedium. A stego-key is used for hiding/encoding process to restrict detection or extraction of the embedded data. The various applications of steganography include secure military communications, multimedia watermarking and fingerprinting applications for authentication purposed to curb the problem of digital piracy.

1.2 The Related Works

In the last few years, a large number of schemes have been proposed for hiding information in digital picture, video, audio and anther multimedia objects.

We describe some contenders that have appeared in the search literature.

The substitution method has to be performed cautiously as overloading the cover image may lead to visible changes leaking the presence of the secret information [1].

With the LSB method as the baseline, a number of related methods have been proposed. For example, a slight variation in converting the secret message into binary codes is undertaken in [2].

In [3], another version of the LSB method is used for RGB images. The cover image is in 3 channels and they are bit sliced. The secret message is embedded in all the three planes in the 2:2:4 ratios for R, G and B planes.

A combination of cryptography and steganography is utilized where the LSB of the cover image is replaced with the most significant bits of the secret image [4].

In 2020, Wang and et.al. a "hybrid steganography" technique based on the replacement of the "least significant bit (LSB)" and "Hamming code (HLAH)" was introduced. Two different methods of steganography are often used to improve information security. Since sharp areas in an image can withstand more changes than smooth areas, more confidential messages are included in the edge areas of the image and a small amount of information is embedded in them
[5].

In 2020, Delmi *and et.al.* Presented steganography, The method was used with Less Important Bit Matching (LSBMR) review. The embedding area was at the edge of the digital images to ensure that the message in the image was not detected by the image. The method used for edge area detection using Canny Edge Detection [6].

1.3 problem statement

Image steganography is an engineering term defining a different and significant discipline for information hiding. This project proposes the algorithm for embedding and extracting the secret message (image) embedded behind the cover gray scale image. Also, the analysis of performance measurement methods such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), gives us the experimental summary for four different cases where each case spans different sizes of cover and secret image, comparing the cover image and stego image at the sender‟s side and embedded secret and extracted secret at the receiver‟s side.

1.4 Project Layouts

This research is organized as follows:

Chapter Two (Theoretical Background)

The overall objective of this chapter is to present fundamentals details, and characteristics of all approaches which have been used steganography method, where the chapter starts with short introduction to image steganography, then it gives an explanation about the methods have been used.

Chapter Three(The Proposed Method):

This chapter presents the designed steps of the entire system's stages and the description of all algorithms that have been used to implement the system.

Chapter Four (Experiential Results and Discussions)

This chapter displays the implementation results, and a discussion on obtained results. The derived conclusions from the proposed system and some suggestions to enhance the proposed system have been presented in this chapter.

Chapter two

Theoretical Background

Chapter two

Theoretical Background

2.1 Image definition:

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics . An image stored in raster form is sometimes called a bitmap . An image map is a file containing information that associates different locations on a specified image with hypertext links. An image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels (picture element). Grey scale images use 8 bits for each pixel and are able to display 256 different colors or shades of grey. Digital color images are typically stored in 24-bit files and use the RGB color model, also known as true color. All color variations for the pixels of a 24-bit image are derived from three primary colors: red, green and blue, and each primary color is represented by 8 bits . Thus in one given pixel, there can be 256 different quantities of red, green and blue [7].

2.2 Data Hiding Classifications:

The main categories of data hiding separated into two classes, the Digital Watermarking and Steganography. Note: in our research we shall use the Steganography line [8].

2.2.1 Steganography:

Steganography is the art of hiding transmitting data through apparently innocuous carries in effort to conceal the existence of the data. Though steganography is an ancient craft , the onset of computer technology has given it new life . Computer-based steganography techniques introduce change to digital cover to embed information foreignto the native cover. Such information may be communicated in the form of text, binary file , or provide additional information about the cover and its owner such as digital watermark or fingerprint.

Steganography is based on the fact that artifacts like bitmaps and audio files contain redundant information. Hiding a message with steganography reduces the chance of a message being detected . if the message is also encrypted , it must also be decrypted if discovered thus providing another layer of protection. Steganography can be viewed as akin to cryptography. Both have been used throughout record history as means to add elements of secrecy to communication. Cryptography techniques "scramble" a message so that if it is intercepted , it cannot be understood.

This process is known as encryption and the encrypted message is sometimes referred to as ciphertext . Steganographic, in essence, "camouflages" a message to hide its existence and make it seem "invisible" thus concealing the fact that a message is being sent altogether . A cipher text message may draw suspicion while an invisible message will not.

Although steganography has been used since ancient time ,little is generally understood about its usage and detection[3].

2.2.2 Steganography Definitions

The following are most widely used definitions:

- Steganography is the art and science of hiding data in to innocent-looking cover-data so that no one can detect the very existence of the hiding data.
- Steganography is the art and science of communicating in a way which hiding the existence of the communication.
- Steganography encompasses methods of transmitting secret message in such a manner that the existence of the embedded message is undetectable.
- Steganography is the study of methods of concealing data in the noise of another data set.

-*Text steganography* Hiding information in text file is the most common method of steganography. The method was to hide a secret message into a text message. After coming of Internet and different type of digital file formats it has decreased in importance. Text stenography using digital files is not used very often because the text files have a very small amount of excess data.

-*Image steganography* Images are used as the popular cover medium for steganography. A message is embedded in a digital image using an embedding algorithm, using the secret key. The resulting stego image is send to the receiver. On the other side, it is processed by the extraction algorithm using the same key. During the transmission of stego image unauthenticated persons can only notice the transmission of an image but can't see the existence of the hidden message[3]. Figure(2.1) shows the steganography system overview [9]. A general Steganography system is assumed that the sender wishes to send via Steganographic transmission a message to a receiver. The sender begin with a cover message, which is an input to the stego-system, in which the embedded message will be hidden. The hidden message is called the embedded message. A Steganographic algorithm combines the cover massage with the embedded message, which is something to be hidden in the cover .The algorithm may, or may not, use a Steganographic key (stego key), which is additional secret data that may be needed in the hidden process. The same key (or related one) is usually needed to extract the embedded massage again. The output of the Steganographic algorithm is the stego message. The cover massage and stego message must be of the same data type, but the embedded message may be of another data type. The receiver reverses the embedding process to extract the embedded message [10],[11],[12],[13].

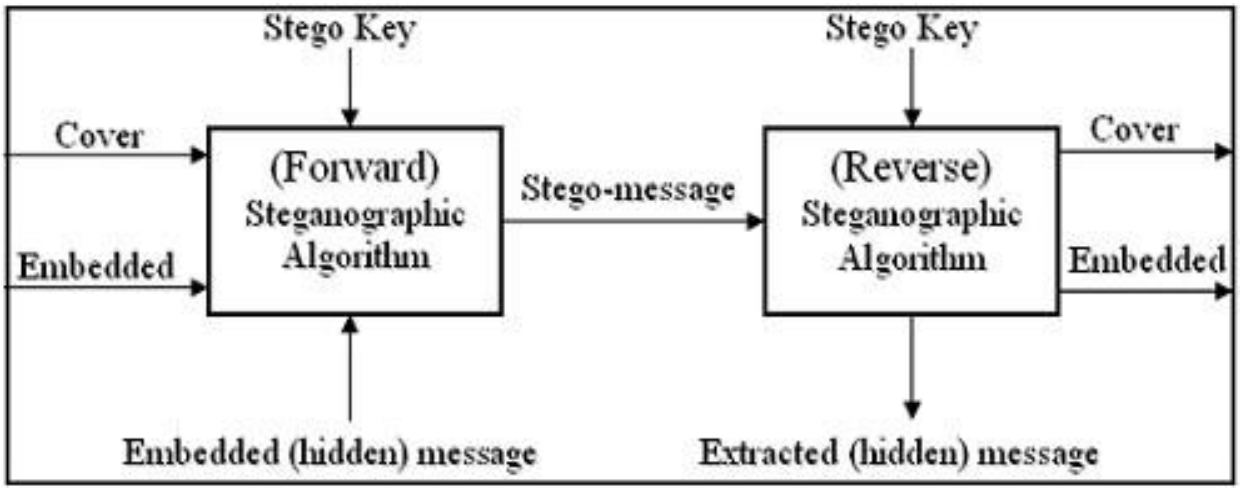


Figure (2.1): Steganography System

2.2.3 Applications of Steganography:

This section list some applications of steganography as follows: (i)Secret Communications the use steganography does not advertise secret communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive information can be transmitted without alerting potential attackers.

(ii) Feature Tagging Elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.

(iii) Copyright Protection Copy protection mechanisms that prevent data, usually digital data, from being copied. The insertion and analysis of watermarks to protect copyrighted material is responsible for the recent rise of interest in digital steganography and data embedding [1].

2.2.4 Image Steganographic Techniques:

There are several Steganographic techniques for image file format which are as follows:

2.2.4.1 Spatial Domain Technique:

There are many versions of spatial steganography, all directly change some bits in the image pixel values in hiding data. Least significant bit (LSB) based steganography is one of the simplest techniques that hides a secret message in the LSBs of pixel values without perceptible distortions. To our human eye, changes in the value of the LSB are imperceptible. Embedding of message bits can be done either simply or randomly. Least Significant Bit (LSB) replacement technique, Matrix embedding, are some of the spatial domain techniques.

Advantages of spatial domain LSB technique are:

1.Degradation of the original image is not easy.

2.Hiding capacity is more i.e. more information can be stored in an image.

Disadvantages of LSB technique are:

1.robustness is low.

2.Hidden data can be destroyed by simple attacks [1].

2.2.4.2 Masking and Filtering:

Masking and Filtering is a steganography technique which can be used on gray scale images. Masking and filtering is similar to placing watermarks on a printed image. These techniques embed the information in the more significant areas than just hiding it into the noise level. Watermarking techniques can be applied without the fear of image destruction due to lossy compression as they are more integrated into the image.

Advantages of Masking and filtering Techniques:

This method is much more robust than LSB replacement with respect to compression.

Disadvantages: Techniques can be applied only to gray scale images and restricted to 24 bits[3].

2.2.4.3 Statistical Preservation

Statistical un detectability is one of the main aspects of a steganography algorithm. To maintain statistical un detectability, the steganography techniques are designed with the aim of minimizing the artifacts introduced in the cover signal by the embedding technique. The main emphasis is on minimizing the noise added by embedding while increasing the payload. This is an important consideration in the design embedding algorithms, since the noise added effects the statistical properties of a medium. For a given medium, the steganography algorithm which makes fewer embedding changes or adds less additive noise will be less detectable as compared to an algorithm which makes relatively more changes or adds higher additive noise.

From the point of view of the steganoanlyst, the steganoanlytic attacks try to examine a signal and look for statistics which get distorted due to embedding. These statistics range from marginal statistics of first and second order in case of targeted attacks to extremely high order statistics (up to 9th order) in the case of blind steganalytic techniques which use machine learning techniques for estimating a model of the cover image from these high order statistics and reports an image to be containing steganographic embedding if it does not conforms to this model. So, in order to defeat the steganalytic attacks, there has been a shift from the above mentioned data hiding paradigm. Algorithms have been proposed which try to restore the statistics which get distorted during the embedding procedure and which may be used for steganalysis [2].

2.3 Asymmetric Key Encryption

The asymmetric key encryption is commonly referred to as public key encryption in which different keys are employed for the encryption and decryption of the message. The encryption key is also said as the public key and can be utilized to encrypt the message with the key. The decryption key is said to as secret or private key and can be used to decrypt the message. The strength of the asymmetric key encryption is utilized with digital signature then it can provide to the users through message authentication detection. To add more durability and robustness to image steganography, a secret image is scrambled and will be as chaotic image. The Arnold scrambling equation (2.1) is used for scrambling the watermark image [14].

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} \pmod N \quad \dots (2.1)$$

Where X,Y,X',Y are dimensions of original and scrambled watermark respectively ,∈ {0,1,2,……,N-1}, N is the order of digital image matrix., N is the order of digital image matrix.

For descrambling, inverse Arnold equation (2.2) is applied on chaotic image [15].

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \pmod N \quad \dots (2.2)$$

Where X,*Y*,*X'*,*Y'* ∈ {0,1,2,……,N-1}, (*X*,*Y*) are dimensions of original watermark ,(*X'*,*Y'*) are dimensions of scrambled watermark, N is the order of digital image matrix.

2.4 Performance Analysis: As a performance measure for image distortion due to hidding of message, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images. It is defined as [16]:

$$\text{SNR}_{\text{PEAK}} = 10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)-I(r,c)]^2} \qquad ...(2.3)$$

Where N are the dimensions of the image, L : the number of gray levels (e.g., for 8 bits L =256).

The root-mean-square error is found by taking the square root of the error squared divided by the total number of pixels in the image

$$RMSE = \sqrt{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[g(r,c)-I(r,c)]^2} \qquad ...(2.4)$$

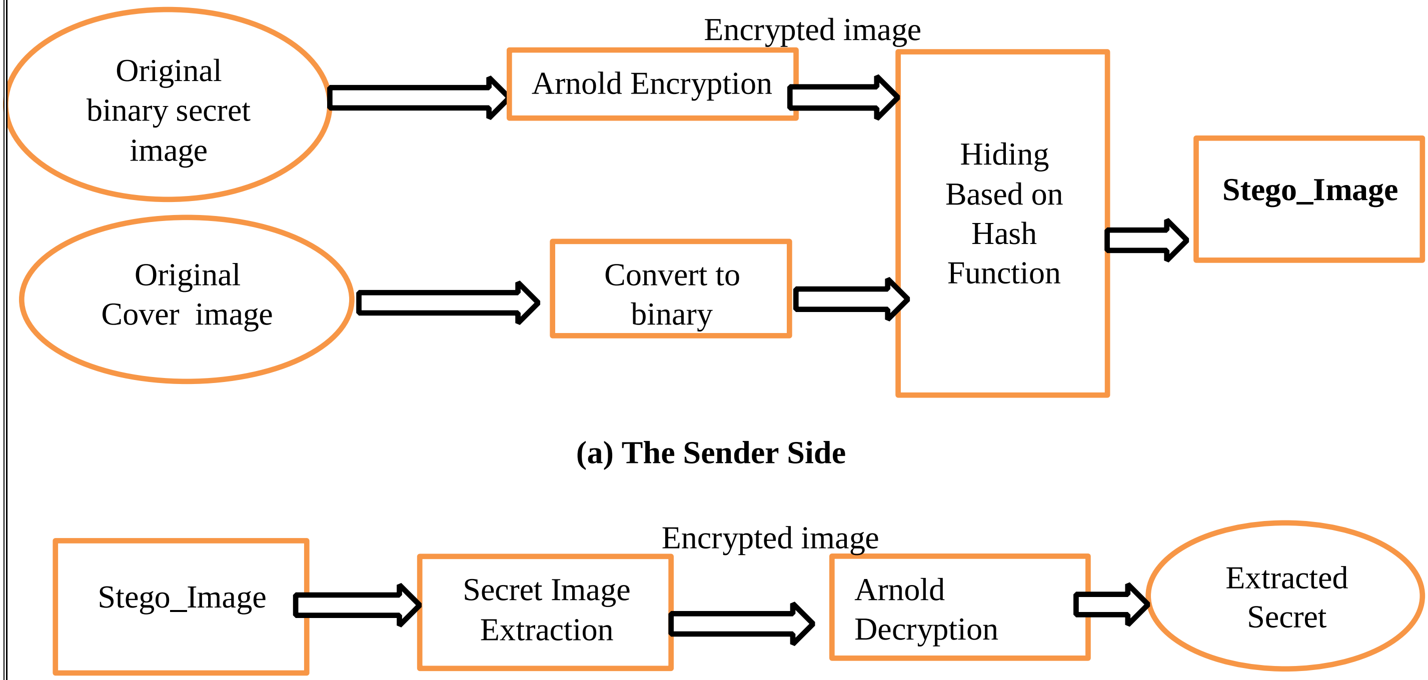
Chapter Three

The Proposed Method

Chapter Three

3.1 Introduction

The method that is suggested in this project embeds the binary image the cover image to obtain the stego image. In other words, it first applies a preprocessing technique on the secret image, and then puts it into the cover image. To increase the security, the secret image is encrypted using ARNOLD method and then embeds it in the cover image based on hash function to add second layer of security. After that, the results are evaluated using different measures. The below block diagram in figure (3-1) depicts the stages and procedures.



(a) The Sender Side

(b) **The Receiver Side**

Figure (3-1) the proposed method stages

The following parts of this section explain the encryption and decryption stages of the image.

3.2.1 Encryption

To provide a second level of security, a stream cipher encryption algorithm is applied on embedding image as describe in algorithm (3.1).

```
Algorithm (3.1): Encryption Secret Image

Input: Secret Image (SImg)
Output: encrypted image(Enc_SImg)
Step 1: convert image to array of pixels.
Step 2:Select number of iteration(itrno)
Step 3:appliyed the Arnold law on (SImg, itrno)and save the result in  Enc_SImg according to equation (2.1)
 Step 4: return encryption image Enc_SImg.
End
```

3.2.2 Least Significant Bits (LSB) insertion

Today, when converting an analog image to digital format, we usually choose between three different ways of representing colors:

24-bit color: every pixel can have one in 2^24 colors, and these are represented as different quantities of three basic colors: red (R), green (G), blue (B), given by 8 bits (256 values) each.

8-bit color: every pixel can have one in 256 (2^8) colors, chosen from a palette, or a table of colors.

8-bit gray-scale: every pixel can have one in 256 (2^8) shades of gray.

LSB insertion modifies the LSBs of each color in 24-bit images, or the LSBs of the 8-bit value for 8-bit images.

Example : The letter 'A' has an ASCII code of 65(decimal), which is 1000001 in binary. It will need three consecutive pixels for a 24-bit image to store an 'A':

Let's say that the pixels before the insertion are:

10000000.10100100.10110101, 10110101.11110011.10110111, 11100111.10110011.00110011

Then their values after the insertion of an 'A' will be:

10000001.10100100.10110100, 10110100.11110010.10110110, 11100110.10110011.00110011

(The values in bold are the ones that were modified by the transformation) The same example for an 8-bit image would have needed 8 pixels:

10000000, 10100100, 10110101, 10110101, 11110011, 10110111, 11100111, 10110011

Then their values after the insertion of an 'A' would have been:

10000001, 10100100, 10110100, 10110100, 11110010, 10110110, 11100110, 10110011

From these examples we can infer that 1-LSB insertion usually has a 50% chance to change a LSB every 8 bits, thus adding very little noise to the original picture.

3.2.3 Embedding Based on Hash Function

In order to increase security, the encrypted secret image is embedding in random locations in least significant bits of the pixels in the cover image according to the following equation.

$$\text{Newloc}=\text{mod}\ (\text{loc}(\text{SCB}),\text{LSBno}) \quad ,\ldots\ldots\ldots\ldots \quad (3.1)$$

Where *Newloc* is the new location for the embedding, *SCB* is the current bit of the secret message and *LSBno* is the number of the least significant bits that are selected for the embedding process.

For example assume that the input secret message is (0001010101111111000), the number of the least significant bits that are selected for the embedding process (*LSBno=4)* and (SCB=5). According to the equation (3.1) the current bit of the secret message will be embedded in the first least significant bits of the cover pixel.

Cover image pixels number	S=0001010101111l1000, *LSBno=4,Bno=2*
Pix1	The first current bit SCB=0 will embedding in the *LSBno=1* The second current bit SCB=0 will embedding in the *LSBno=2*
Pix2	The third current bit SCB=0 will embedding in the *LSBno=3* The fourth current bit SCB=1 will embedding in the *LSBno=1*
Pix3	The fifth current bit SCB=0 will embedding in the *LSBno=1* The sixth current bit SCB=1 will embedding in the *LSBno=2*
. . .	. . .

As shown from above example the embedding process is done in random locations in least significant bits of the cover image pixels and this will increase the method security.

Algorithm (3.2): ***The embedding process***

```
Input: Cover Image (CI), Secret Image (S), number of embedding bits (Bno)
    Output: Stego_ Image (SI) Begin
 Step1: read cover image and save in (CI), read Secret Image and save (S)
Step2: Encrypt Secret Image (S) using algorithm (3.1)
Step 3: Repeat
 Step 4: Embed (Bno) secret bits in each pixel of cove image by applying
                equation (3.1)
 Step 5: do until embed all secret image bits.
Step 6: save the result in the Stego_ Image (SI) End.
```

3.2.4 Extraction Procedure

At the receiver side, the extraction process is done in reverse order. At first, the encrypted image is extracted based on hash function. Secondly, the process of decryption is applied on the received image as depicted in Algorithm (3.3).

Algorithm (3.3): ***The extracting procedure***

```
   Input: Stego_ Image (SI)
Output: Reconstruction Secret Image (RS)
Begin
   Step1: read Stego_ Image and save in (SI)
   Step 2: Repeat
         Step 2.1: Extract (Bno) secret bits in each pixel of stego image by
   applying  equation (3.1)
       Step 2.2: do until extract all secret image bits.
   Step 23 Dencrypt Secret Bits (Bno) using equation(2.2) and save the
   result in Reconstruction Secret Image (RS)
End.
```

Chapter Four

Experiential Results and Discussions

Chapter Four

Experiential Results and Discussions

4.1. Introduction

This work proposes a Steganography technique for the gray image. In the first stage, secret image is encrypted. Then secret image is hidden by Least Significant Bits technique of the original cover image. During embedding, secret image is dispersed within the original image depending upon the hash function. The developed system was established using Matlab (version 12) programming language. The programs work under windows XP service pack2 operating system, laptop computer with processor: Intel core2 CPU.

4-2 Test Material

All test images that implemented in our experiments are 256 gray levels. Figure (4-1) shows examples of these images.

(a)Original image (Lenna.bmp)

(b) Original image (House.bmp)

(c) Original image (Barbara.bmp)

(c) Original image (Girl.bmp)

Figure (4-1) Examples of tests cover images

Figure (4.2) shows examples of secret images.

Figure (4-2) Examples of tests secret images

4.3 Experiential Results:

In this section different results will be reviewed for different test images. At first, the secret image is encrypted using Arnold algorithm. Figure (4.3) shows example of original and encrypted images with dimensions (32*32).

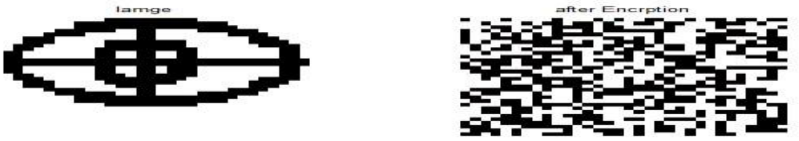


Figure (4-3) Examples of original and encrypted secret images

Secondly, the encrypted image is embedded in the cover image based on hash function. Figure (4.4) shows the stego image of (Lena.bmp) with (PeakSNR = 55.4087) and (Mean2err= 0.1886).

Figure (4-4) Stego image

At receiver side, the encrypted secret image is extracted as shown in Figure (4.5) based on Hash function.

Figure (4-5) Encrypted secret image

Secondly, the extracted secret image is decrypted using RSA to obtain original image as shown in Figure (4.6).

Figure (4-6) Decrypted secret image

Another example applied on the cover image (lenna.bmp) with dimensions (256*256) and secret image with dimensions (32*32). The PeakSNR = 55.9355 and Mean2err = 0.1671. Figure (4.7) shows the results.

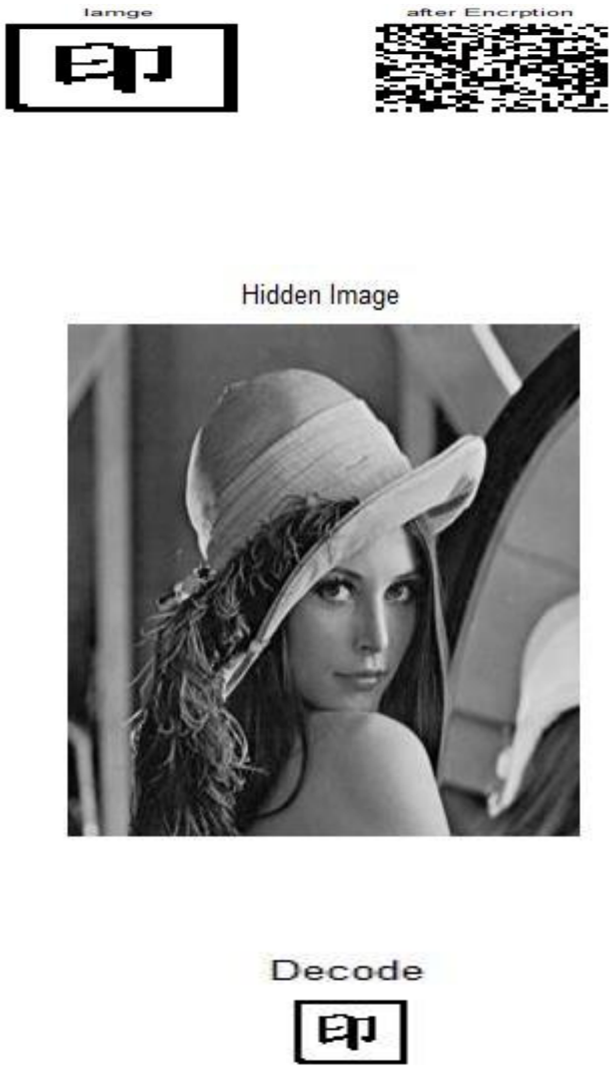


Figure (4-7) Decrypted secret image

4.3 Conclusions

In the applied method the secret image is hidden in the cover image. So there is a small visual change in between cover image and stego image. Due to strong security aspects this small amount of imperceptibility is acceptable. encryption before hiding step is more appropriate in invisibility of the steganography. Furthermore it increases the image secyrity. Moreover, adding a step of embedding based on hash function allows for multiple separate phases of information security.

4.3 Future Works

In the following some suggested ideas are given below:

- In future work, examining how other image processing techniques such as brightness and contrast adjustment can be taken advantage of in steganography with the purpose of giving the communicating parties more preferences to manipulate their secret communication .
- This approach can be applied for image steganography in transform domain such Discreet Wavelet Transform (DWT) and Discreet Cosine Transform (DCT).

الخلاصة:

إن علم إخفاء المعلومات هو فرع من فروع العلم يخفي المعلومات ويهدف إلى الوصول إلى مستوى مرغوب فيه من الأمن في تبادل البيانات العسكرية والتجارية الخاصة غير الواضحة.
في هذا المشروع تم إجراء دراسة لإخفاء صور ثنائية في صورة اخرى تسمى صوره الغطاء.
لدى النظام مشاركين اثنين هما المرسل والمستلم. سيقوم المرسل بتطبيق طريقة الاخفاء، تتكون هذه الطريقة من عدة مراحل. يتم تطبيق أسلوب التشفير Arnold لزيادة الامنية.
للحصول على صوره الاخفاء يتم تضمنين الرسالة المشفره بالاعتماد على مبدا HASH. في جانب المستلم ، سيتم تطبيق طريقة الاستخراج لاستخراج الرسالة السرية) الصوره المضمنه(. تتكون هذه الطريقة من نفس المراحل في طريقة التضمين ولكنها تطبق في هذ ا الجانب بشكل معكوس.

References

1. S. Gupta, G. Gujral and N. Aggarwal, "Enhanced least significant bit algorithm for image steganography", *Int. J. Comput. Eng. Manage.*, vol. 15, no. 4, pp. 40-42, 2012.
2. R. Das and T. Tuithung, "A novel steganography method for image based on Huffman encoding", *Proc. 3rd Nat. Conf. Emerg. Trends Appl. Comput. Sci.*, pp. 14-18, Mar. 2012.
3. A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images", *Proc. IEEE Int. Conf. Electr. Comput. Commun. Technol. (ICECCT)*, pp. 1-4, Mar. 2015.
4. N. Patel and S. Meena, "LSB based image steganography using dynamic key cryptography", *Proc. Int. Conf. Emerg. Trends Commun. Technol. (ETCT)*, pp. 1-5, Nov. 2016.
5. Wang, Y., Tang, M., & Wang, Z.," High-capacity adaptive steganography based on LSB and Hamming code". Optik, vol. 213,2020, https://doi.org/10.1016/j.ijleo.2020.164685.
6. Delmi, A., Suryadi, S., & Satria, Y., "Digital image steganography by using edge adaptive based chaos cryptography". In Journal of Physics: Conference Series,Vol. 1442, No. 1, pp. 1-7, IOP Publishing, January 2020, DOI: 10.1088/1742-6596/1442/1/012041
7. R.Anderson and F. Petitcolas, "On the limits of steganography", IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
8. K. Jenita Devi,"A Sesure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique" , B.SC thesis, Department of Computer Science and Engineering National Institute of Technology, May 2013.

9. S. Majumder, K. J. Devi, and S. K. Sarkar, “Singular value decomposition and wavelet-based iris biometric watermarking”, IET Biometrics, vol. 2, no. 1, 2013.

10. Fabien A. P. Petitcolas, Ross J. Anderson, "Information Hiding" " Proceedings of the IEEE, special issue on protection of multimedia content" , 87(7), July 1999.

11. Md. Rafiqul Islam, A.W. Naji, A.A.Zaidan, B.B.Zaidan “ New System for Secure Cover File of Hidden Data in the Image Page within Executable File Using Statistical Steganography Techniques”, International Journal of Computer Science and Information Security (IJCSIS), ISSN: 1947-5500, P.P 273-279, Vol.7 , NO.1, January 2010,USA..

12. Hamdan. Alanazi, Hamid.A.Jalab, A.A.Zaidan, B.B.Zaidan, “New Frame Work of Hidden Data with in Non Multimedia File”, International Journal of Computer and Network Security, 2010, Vol.2, No.1, ISSN: 1985-1553, P.P 46-54,30 January, Vienna, Austria.

13. M. K. I. Rahmani and N. P. KamiyaArora, “A crypto-steganography: A survey,” International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.

14. M. Li, T. Liang and Y. He, "Arnold Transform Based Image Scrambling Method",3rd International Conference on Multimedia Technology (ICMT13), Atlantis Press, 2013.

15. S. Roy and A.K. Pal, "A robust blind hybrid image watermarking scheme in RDWT-DCT domain using Arnold scrambling", Multimedia Tools and Applications, 76(3), 3577-3616, 2017.

16. X. Yu, C. Wang, and X. Zhou, “A survey on robust video watermarking algorithms for copyright protection," Appl. Sci., vol. 8, no. 10, Oct,2018.