Steganography Image in Image using Modified method in Least Significant Bit (LSB) substitution

Suhad A.H.Al-Ani *

Date of acceptance 15/1/2007

Abstract:

Steganography is the art of hiding and transmitting message through unsuspecting cover in an effort to conceal the existence of message. The aim of this paper is to design and implementation image in image steganography that hide the gray scale into color image, using embedding message in LSB of cover image. In Least Significant Bit (LSB) technique two methods (Spin method and Look-up Table Method)have been suggested and compared with classical method. The imperceptibility of the stego image is assessed by using the mean square error (MSE) Root Mean Square Error (RMSE) (closeness measure), and peak signal-to-noise ratio (PSNR) measures used, the stego image, under different methods, have excellent quality (PSNR above 60 dB).

1-Introduction

1-1 Information Hiding

Information hiding techniques have been 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 . Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the content of a message using encryption, seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. Criminals try to use whatever traffic security properties are provided intentionally or otherwise in the available communications systems, and police forces try to restrict their use [1] . There are three different to information hiding system that content with one another : capacity, security and robustness. Capacity refers to the amount of information that can be hidden, security to the inability of an eavesdropper to detect hidden information, and robustness to the amount of modification the cover medium can withstand before the hidden information is destroyed [2].

1-2 Steganography

Steganography refers to the science of "invisible" communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, Steganographic techniques strive to hide the very presence of the message itself from an observer. Although Steganography is an ancient subject, the modern formulation of it is often given in terms of the prisoner's problem where Alice and Bob are two inmates who wish to communicate in order to hatch an escape plan. However, all communication between them is examed by the warden, Wendy, who will put them in solitary confinement at the slightest suspicion of covert communication. Specifically, in the general model for Steganography, we

*Physics department, College of Science University of Baghdad .

have Alice wishing to send a secret message m to Bob. In order to do so, she embeds m into a cover-object c, to obtain the stego-object s. The stego-object s is then sent through the public channel. The warden, Wendy, who is free to examine all message exchanged between Alice and Bob, can be passive or active. A passive warden simply examines the message and tries to determine if it potentially contains a hidden message. If it appears that it does, she then takes appropriate action, else, she lets the message through without any action. An active warden, on the other hand, can alter messages deliberately, even though she may not see any trace of a hidden message in order to foil any secret communication that can nevertheless be occurring between Alice and Bob. The amount of change the warden is allowed to make depends on the model being used and the cover make sense that the warden is allowed to make changes as long as she does not alter significantly the subjective visual quality of a suspected stego- image. It should be noted that the main goal of steganography is to communicate securely in a completely undetectable manner [3].

1-3 Steganography Advantage and Disadvantage

The advantage of Steganography is that it can be used to secretly transmit messages without the fact of the transmission being discovered. Often, using encryption might identify the sender or receiver as somebody with something to hide . For example, the picture of your cat could conceal the plans for your company's latest technical innovation. Steganography has a number of disadvantages as well. Unlike encryption, it generally requires a lot of overhead to hide a relatively few bits of information. However, there are ways around this. Also, once a Steganographic system is discovered, it is rendered useless. This problem. Too, can be overcome if the hidden data depends on some sort of key for its insertion and extraction [4].

1-4 Types of Steganography systems

One could categorize the stego-systems according to their stego-key used in the embedding process to three types: Pure Steganography, Secret Key Steganography and Public Key Steganography.

1-4-1 Pure Steganography

A steganographic system which does not require the prior exchange of some secret information (like a stego key) called pure steganography. Formally, the embedding process can be described as a mapping $E: C \times M \rightarrow C$, where C is the set of all possible covers and M is the set of all possible messages. The extraction process consists of a mapping $D: C \rightarrow M$. Clearly it is necessary that $|C| \geq |M|$. Both the sender and receiver must have access to the embedding and extracting algorithm, but the algorithm should not be public. In practice, the pure steganographic system is not secure enough because the security of the system depends on stego object imperceptibility and the algorithm secrecy so that violates Kerckhoffs principle, so the stego-systems based on key give a better performance from the security viewpoint but of course not from complexity one.

1-4-2 Secret Key Steganography

A secret key steganography system is similar to a symmetric cipher. The sender chooses a cover and embeds the secret message using a secret key. If the key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message. Anyone who does not know the secret key, depending on the security of the key, should not be able to obtain evidence of the encoded information. Formally, the embedding process is a

mapping E_K: C × M × K→ C and the extracting process is a mapping D_K : C × K → M, where K is the set of all possible secret keys the same secret key is available to both the transmitter and receiver. So to overcome these problems, a public key steganography is used.

1-4-3 Public Key Steganography

As in public key cryptography, public key steganography does not rely on the exchange of a secret key. Public key steganography systems require the use of two keys, one private and one public; the public key is used in the embedding process, the secret key is used to reconstruct the secret message. One way to build a public key steganography system is the use of a public key cryptosystem. Public key steganography utilized the fact that decoding function in a steganography system can be applied to any cover, whether or not it already contains a secret message. In the later case, a random element will be the result, so called "natural randomness" of the cover.

1-5 Steganographic Technique

Many different steganographic methods have been proposed during the last few years; most of them can be seen as substitution systems. Such methods try to substitute redundant part of the signal with a secret message; their main disadvantage is the relative weakness against cover modification. There are several approaches in the classifying steganographic techniques. One of these approaches is to categorize them according to the cover modifications applied in the embedding process. Mainly, steganographic techniques may be grouped into five categories as follows:

- ***Substitution Techniques***: Substitute redundant parts of a cover with a secret message.
- ***Transform Domain Techniques***: Embed secret information in a transform space of the signal.
- ***Spread Spectrum Techniques***: Adopt ideas from spread spectrum communication.
- ***Statistical Techniques***: Encode information by changing several statistical properties of cover image.
- ***Distortion Techniques***: Store information by signal distortion and measure the deviation from the original cover in the decoding step.

In this paper focused on Substitution Techniques

1-5-1 Substitution Techniques

Basic substitution systems try to encode secret information by substituting insignificant parts of the cover by secret message bits; the receiver can extract the information if he has knowledge of the positions where secret information has been embedded. Since only minor modifications are made in the embedding process, the sender assumes that they will not be noticed by an attacker [5].

- Least Significant Bit Encoding

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used. In a typical full-color image, there are 24 bits/pixel, 8 bits assigned to each color components. The simplest Steganography techniques embed the bits of the message directly into the least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in a human-perceptible difference because the amplitude of the change is small other techniques "process" the message with a pseudo-random noise sequence before or during insertion into the cover image. The advantage of LSB embedding is its simplicity and many techniques use these methods. LSB embedding also allows high perceptual transparency. However, there are many weaknesses when robustness, tamper resistance, and other security issues are

considered. LSB encoding is extremely sensitive to any kind of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is very likely to destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image [6] .

1-6 The Quantization process

Due to the modification that is applied to the cover image in the previous processes, the pixel of the image that obtained after the inverse wavelet packets are not quantized as a gray scale. So that, they must be quantized to preserve the initial dynamic range of the cover image. Depending on the mapping equation, quantization may be classified into two types: uniform quantization where all subdivisions in which the dynamic range is divided are of equal width , and nonuniform quantization where these subdivisions are of non-equal width. Of course, in the proposed stegosystem the first type is used. For 256 subdivisions, uniform quantization can be done as follows [5]:

$$f_q(r,c) = (f(r,c) - f_{\min}).\frac{255}{(f_{\max} - f_{\min})} \ldots(1)$$

Where $f(r,c)$ is the image before the quantization and $f_q(r,c)$ is the quantized version of it, $f_{\max}$ and $f_{\min}$ is the maximum and minimum values in the original image respectively. As mention before, this process affects the embedded image because many grey levels of the attenuated version of this image will be merged in one level depending on the attenuation factor[5].

2-Objective Measure of an Image Quality

An objective quality measure should well reflects the distortion on the image due to many reasons (e.g., blurring, noise, compression or, turbulence effects). Such measures include the mathematical terms using to compute the similarity degree between images. A good example is the mean-square- error(MSE) over the image array is [7] :

$$MSE = \frac{1}{N^2}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} e^2(x,y) \quad ...(2)$$

$$MSE = \frac{1}{N^2}\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}[g(x,y) - f(x,y)]^2 \quad ...(3)$$

and the Root Mean Square Error(RMSE) is define as **[7]**:

$$RMSE = \left[\frac{1}{NM}\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}(g(x,y) - f(x,y))^2\right]^{1/2} \quad ...(4)$$

The values of error measures normalized RMSE (NRMSE) lie between zero (good closeness) and one(different images) [7]. Commonly used objective measures are the root-mean-square error (E_{RMS}), the root-mean-square signal-to-noise ratio (SNR_{RMS}) and the peak signal-to-noise ratio (PSNR). Because related works have used the PSNR, it will be used here for comparison purposes. The PSNR is usually measured in dB and can be defined as [5] :

$$PSNR = 10\log_{10}\frac{(L-1)^2}{\frac{1}{N^2}\sum_{r=0}^{N-1}\sum_{c=0}^{N-1}[\hat{f}(r,c) - f(r,c)]^2} \quad ...(5)$$

where L is the number of the grey levels, f(r, c) is the original image and $\hat{f}(r,c)$ is the reconstructed image[5].

When PSNR maximum, then the quality of the reconstructed image is good.

3- Experimental Work and Results

In this section represent the experimental work and results of applying three different methods in distribute the bits of secret image in cover image using Least Significant Bit Substitution (LSBS), two cover images and two secret images using to evaluate the performance the methods. In this paper suggested two methods and compare with classical method using (MSE), (RMSE), (PSNR), and histogram to check distortion in stego-image. Several true color image (2^{24} color) with size (240 x 320) pixels are used as cover and them histogram are shown in figure (1), and several gray image (2^{8} color) with size (125 x 125) pixels are used as secret and shown in figure (2), the dimension of cover image must be >=((dimension of secret image * 8(bit))/3(color)).In order to be able to decode the secret message, the receiver must have access to the sequence of element indices used in the embedding process. The process of this is operation is done as following:

1- read cover image (2^{24} color, RGB mean: R:0-255,G:0-255,B:0-255) and quantize uniform it to 128 level of every color according to equation (1). The quantize make all the LSB of all bytes of cover is zero, these bits are used to embed the bits of secret image.

2- read secret image, which can be ciphered, and then discreet the bytes of secret image to bits and embed it in different method as following :

3-1 Classical Method

In this method the process consists of choosing a subset $\{C_1,\dots ,C_{l(n)}\}$ from the cover image, where l(n) is the length of the message, the performing the substitution operation $C_i \leftrightarrow m_i$ on them, which exchanges the LSB of the C_j by m_i ($C_{j=1---8m/3}$ where C_j is a pixel (24 bit color RGB) of cover image ; $m_{i=1\ ---\ 8n}$ where m_i is a bit series of message (secret image) can be either be 1 or 0). The distribute of m_i as line by line and mi in Red, m_{i+1} in Green and m_{i+2} in Blue, and so on, as shown in figure (3), and the results of applying this method as in figure (4) and table (1).

3-2 Spin Method

In this method modify classical method by distribute the bits of secret image around and toward the center of cover image as illustrated in figure (5), and the results of applying this method as in figure (6) and table (2).

3-3 look-up table Method

In this method also, modify classical method by distribute the bits of secret image after change lines with respect to look-up table as in figure (7), and the results of applying this method as in figure(8) and table (3), in this case receiver must know the look-up table as below:

code ↓ / decode ↑

1	2	3	4	5	6
5	4	1	3	6	2

Conclusions

When compare the classical method with the modified methods (spin and look-up table) and depending on the previous results can conclude the quality hiding in modified methods is converge to the quality hiding in classical method.

References:

1– Fabien, A.P.Petitcolas, Ross J. Anderson and Markus G. Kuhn, July 1999, "Information Hiding –A Survey", Proceedings of the IEEE, Secial issue on protection of multimedia content,87(7):1062-1078.

2- Brian, Chen and Gregory W. Wornell., May 2001, "Quantization Index Modulation :A Class of Provably Good Methods for Digital Watermarking

and Information Embedding ". IEEE Transactions on Information Theory,47(4);1423-1443.

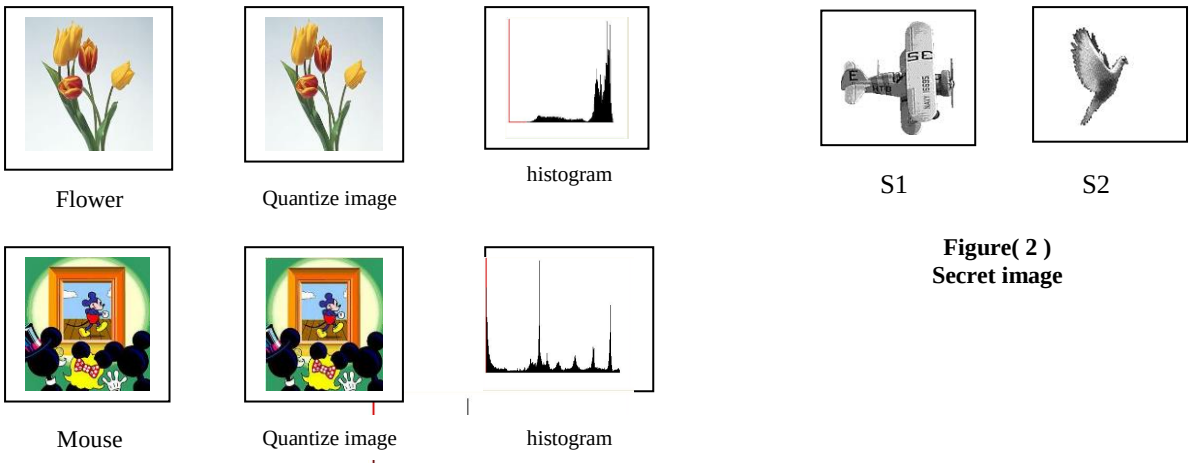
3- Ismail Avcibas, Nasir Memon, and Bulent Sankur, February 2003, " Steganalysis Using Image Quality Metrics",IEEE Transaction on Image Processing , 12(2).

4- Ahmed H. A., 2002, "Image in Image Steganography using PIFS", M. Sc. thesis submitted in computer Dept. College of Science, Baghdad University.

5- Al-jashammi, A. M. H., 2002, " Image Steganography Using Wavelet Transform Techniques ",M.Sc.thesis submitted in Electronics and Communication Engineering Dept. College of Engineering, University of Baghdad .

6- N.Johnson and S.Jajodia, 1998, " Steganalysis of images created using current steganography software", Lecture Notes in Computer Science, vol.1525, pp.273-289.

7- Gonzalaz, R.C. & Woods , R.E., 2000, (Digital Image Processing), Pearson Eduction Asia Pte Ltd.



Figure(2)
Secret image

Figure (1)
Cover Image, Quantize image and it's histogram

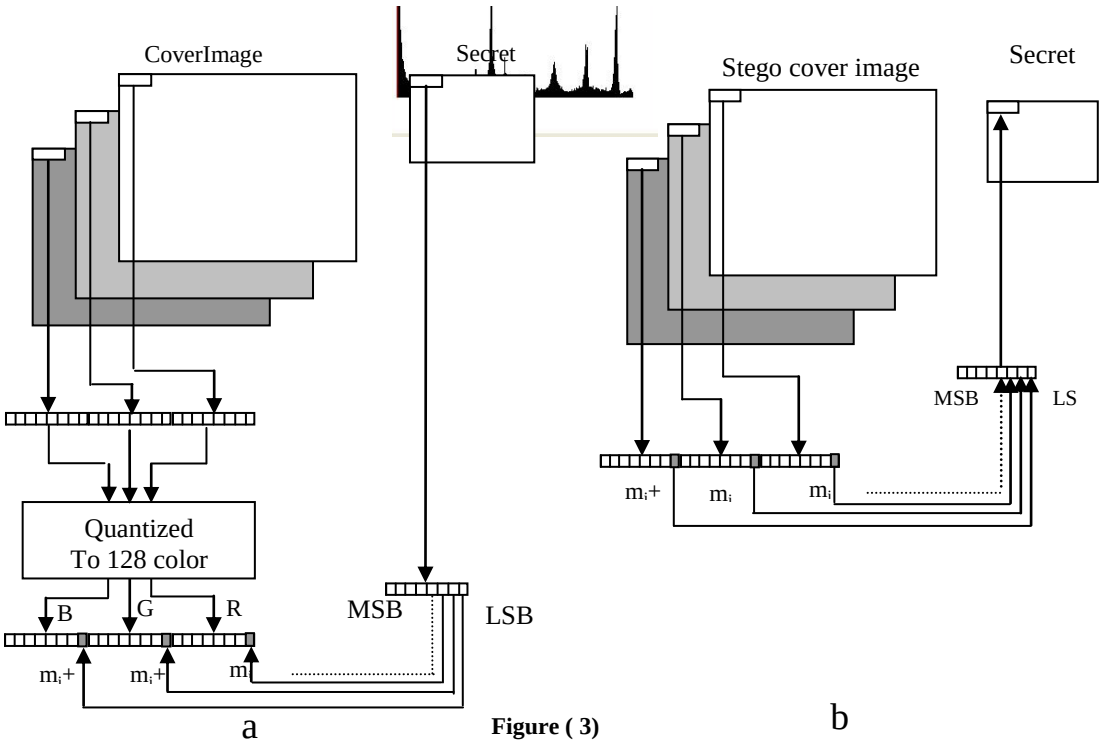


Figure (3)
a-The diagram of the embedding algorithm
b- The diagram of the extracting algorithm

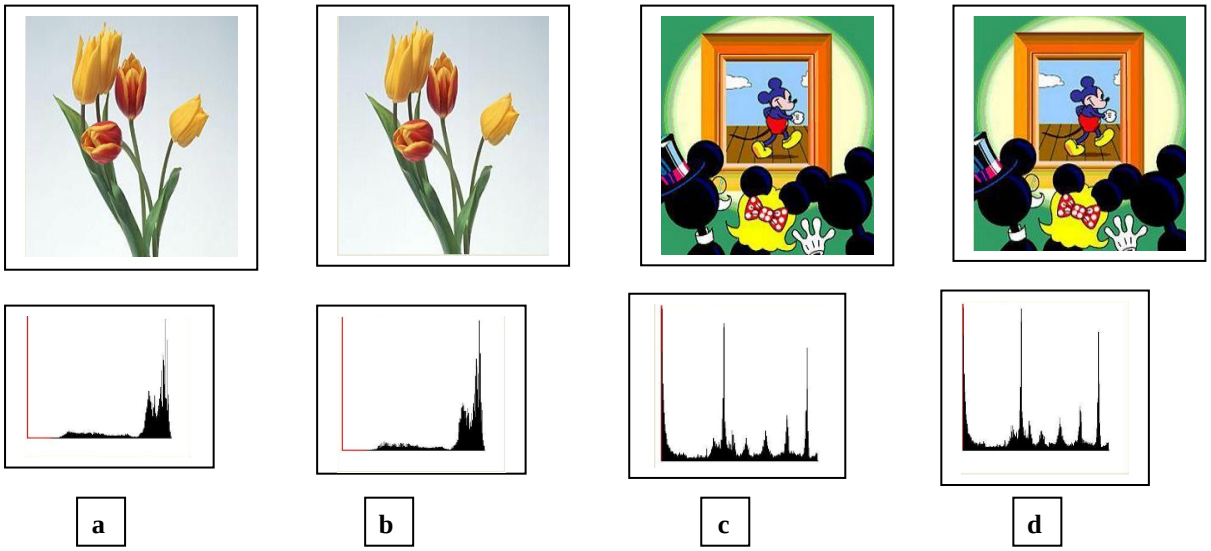
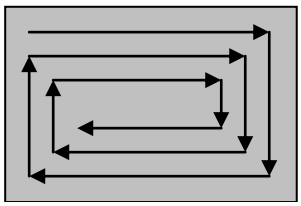


Figure (4) Stegoanography using Classical Method
a-Stego cover image (flower cover image and s1 secret image) and it's histogram
b-Stego cover image (flower cover image and s2 secret image) and it's histogram
c-Stego cover image (Mouse cover image and s1 secret image) and it's histogram
d-Stego cover image (Mouse cover image and s2secret image) and it's histogram



Figure(5)
The manner to distribute secret image
incode and decode using Spin Method

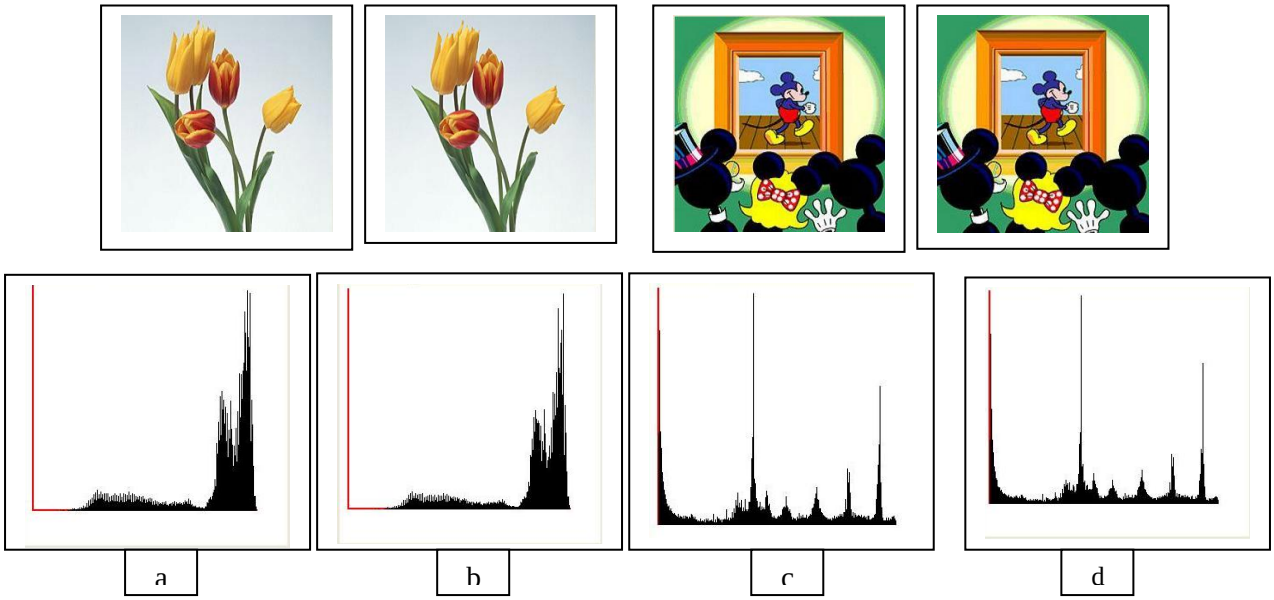
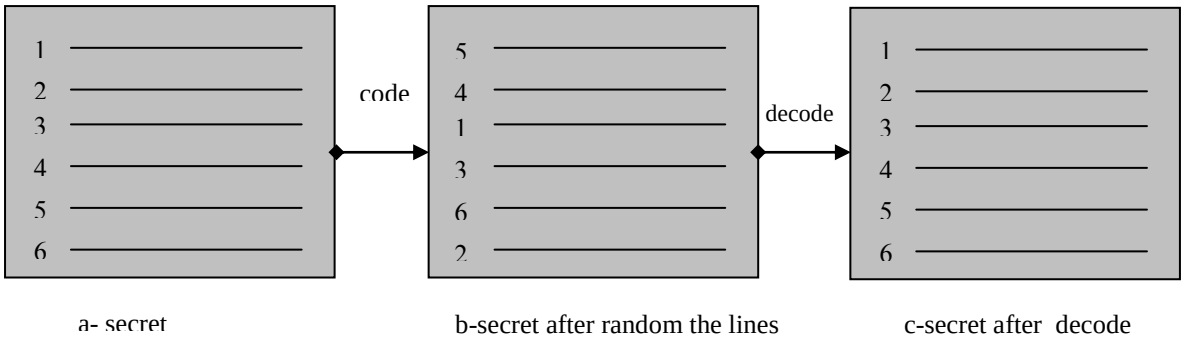


Figure (6) Stegoanography using Spin Method
a-Stego cover image (flower cover image and s1 secret image) and it's histogram
b-Stego cover image (flower cover image and s2 secret image) and it's histogram
c-Stego cover image (Mouse cover image and s1 secret image) and it's histogram
d-Stego cover image (Mouse cover image and s2secret image) and it's histogram



Figure(7)
The manner to distribute secret image in code and decode using Look—up table Method

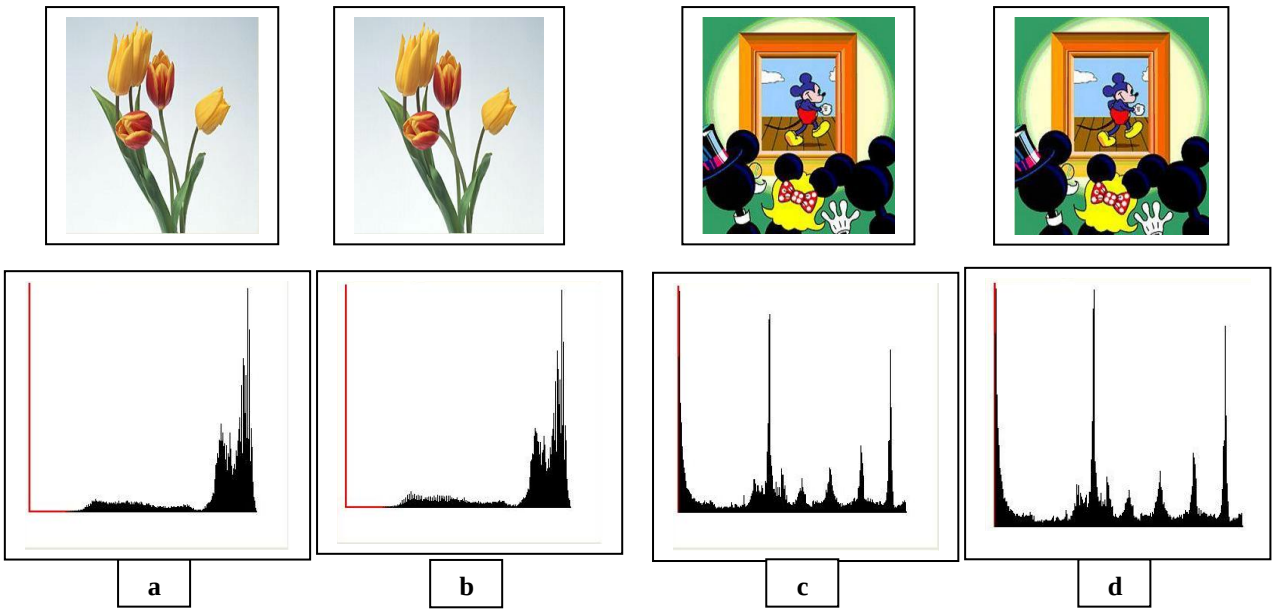


Figure (8) Stegoanography using 3 Look-up table Method
a-Stego cover image (flower cover image and s1 secret image) and it's histogram
b-Stego cover image (flower cover image and s2 secret image) and it's histogram
c-Stego cover image (Mouse cover image and s1 secret image) and it's histogram
d-Stego cover image (Mouse cover image and s2secret image) and it's histogram

Table (1) The MES, RMSE, and PSNR for Classical Method

Cover image	Secret image	Stego cover image	MSE	RMSE	PSNR
Flower	S1	Fl-s1	2.457429*10^-3	4.957246*10^-2	68.171263
Flower	S2	Fl-s2	2.463419*10^-3	4.963284*10^-2	68.160691
Mouse	S1	Mo-s1	4.607573*10^-3	6.7879105*10^-2	65.441352
Mouse	S2	Mo-s2	4.605136*10^-3	6.786115*10^-2	65.443649

Table (2) The MES, RMSE, and for PSNR Look-up table Method

Cover image	Secret image	Stego cover image	MSE	RMSE	PSNR
Flower	S1	Fl-s1	2.457174*10^-3	4.956989*10^-2	68.171715
Flower	S2	Fl-s2	2.463311*10^-3	4.963176*10^-2	68.160880
Mouse	S1	Mo-s1	4.607735*10^-3	6.7880306*10^-2	65.441198
Mouse	S2	Mo-s2	4.604815*10^-3	6.785879*10^-2	65.443951

Table (3) The MES, RMSE, and PSNR for Spin Method

Cover image	Secret image	Stego cover image	MSE	RMSE	PSNR
Flower	S1	Fl-s1	6.398224*10^-3	7.998889*10^-2	64.015479
Flower	S2	Fl-s2	6.412100648*10^-3	8.007559*10^-2	64.0060709
Mouse	S1	Mo-s1	1.450869*10^-3	0.12045204*10^-2	60.459791
Mouse	S2	Mo-s2	1.449824*10^-2	0.120408	60.462919

اختزالِ صورة في صورة بإستعمال طريقةً الحشر في البت الاقل اهمية المحورة

سهاد عبد الكريم حمدان*

*مدرس مساعد/جامعة بغداد /كلية العلوم /قسم الفيزياء

الخلاصـة:

فن الاختزال هو فَنُّ اختفاء وإرْسال رسالةِ خلال غطاءِ بعيد عنِ الشكَّ في محاولة لا َخفاء وجودَ الرسالةِ. في هذا البحثِ تم تبني إخفاء صورة في صورة حيث تم تطبيق إخفاء صورة ذات تدرج رمادي في صورة ملونة (224 لون)،واستعملت تقنية تضمين الرسالة السرية بتقنية الحشر في (Least Significant Bit (LSB)) في الصورةِالغطاءِ وتم اقتراح طريقتان في هذه التقنية Spin method and Look-up Table Method (ومقارنتهماً بالطريقةِ التقليديةِ.ولصعوبة تمييز الاختلاف بين الصورة الغطاء والصورة الحاملة للرسالة، استخدمنا معيار معدل مربع الخطأ وجذر معدل مربع الخطأ، كذلك معيار قمة نسبة الإشارة إلى الخطأ، وتم الحصول على نتائج ممتازة (فوق 60 ديسبيل).