Lossless Data Hiding Using LSB Method

A. I. Kahdum
Department of Physics, College of Education Ibn Al-Haitham, University of Baghdad.

Abstract

A lossless (reversible) data hiding (embedding) method inside an image (translating medium) presented in the present work using LSB (least significant bit) technique which enables us to translate data using an image (host image), using a secret key, to be undetectable without losing any data or without changing the size and the external scene (visible properties) of the image, the hiding data is then can be extracted (without losing) by reversing the encoding process , knowing and using the same secret key. This method tested by using two images and by using several embedding bit rates , the result is that the host image undistinguishable from the stego images , then we used (PSNR) and (MSE) methods to fined the difference values between the host image and the stego images.

Introduction

Steganography, coming from the Greek words stegos, meaning (roof) or (covered) and graphia which means (writing), is the art and science of hiding the fact that communication is taking place. Using steganography, you can embed a secret message inside a piece of unsuspicious information and send it without anyone knowing of the existence of the secret message (1, 2).

Secrets can be hidden inside all sorts of cover information: text, images, audio, video,... Usually steganographic utilities nowadays, hide information inside images, as this is relatively easy to implement. However, there are tools available to store secrets inside almost any type of cover source. It is also possible to hide information inside texts, sounds and video films for example. The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the cover (1).

The best object considered up to now is probably a digital image. Digital images have the benefit of containing massive amounts of bytes to designate pixel color for the photo (3).

A typical digital steganographic encoder is shown on Figure (1). The message is the data that the sender wishes to remain confidential and it can be as text, images, audio, video, or any other data that can be represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. This is also referred to as the message wrapper (4).

Hiding Information Inside An Image

Hiding information inside images is a popular technique nowadays. An image with a secret message inside can easily be spread over the World Wide Web or in newsgroups.

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 involve the usage of the least-significant bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files(1).

LSB Embedding Technique

A digital image consists of a matrix of color and intensity values. In a typical gray scale image, 8 bits/pixel are used (4). The most important requirement for a steganographic system is the undetectability: stego images should be statistically indistinguishable from cover images. In other words, there should be no artifacts in the stego image that could be detected by an attacker with probability better than random guessing, given the full knowledge of the embedding algorithm, including the statistical properties of the source of cover images, except for the stego key (5).

In the LSB method the least-significant bit of the chosen pixels in the host image replaced with a secret message (hiding data) using a secret key to introduce the sego image (1).

While the two images appear as the same and have the same size the LSBs of each pixel in the host (original) image have been replaced with a hidden message. The human eye cannot distinguish which of the two images is the original image and which of them is the stego (coded) image. While an image with LSB replacement and the original image may be indistinguishable to the human eye, the empirical statistics vary (6).

In the present work we used LSB technique to hide information inside a gray scale image.

Data Hiding Method

There are two important components, cover image and hiding data, in data hiding technique. The cover image *C* is an 8-bit gray scale image. The size of cover image is *m* x *n*. The hiding data *D* embedded in *C* is *g*-bits bitstream. We use the equation below to express image *C*, data *D* and each pixel separately.

$$C = \{c_{ij} \mid 0 \le i < m, 0 \le j < n, c_{ij} \in [0,255]\}$$

$$D = [d_i \mid 0 \le i \le g, g \in [1,2,3,4,5]\}$$

The embedding steps are shown as follows:-

1- Select a number of pixels in the host image depending on a secret key (according to a secret condition).

2- Decide a threshold value t.

3- If the gray level value of a selected pixel satisfy the secret condition and the threshold condition then the step (4) will be executed.

4- According to the value of each data bit d_i in hiding data D, we do the Same change of the selected pixel value in the cover image *C*.

5- Keep all of the pixels values that don't satisfy the secret conditions as the same.

6- The stego image is the image generated by steps *4* and *5*.

To extract the hiding data from the stego image we use the same secret conditions (the essential element of the process) and reverse the process steps.

The Results

After applying the proposed LSB method the results are presented as following:-

1- The amount of the hiding data depending on the size (dimensions) of the host image, where the amount of embedding data equals to (774 ^{bits}) for the rabbit image (its dimensions are 300 x 200) while the amount of embedding data equals to (600 bits) for the air plane image (its dimensions are 200 x 200) when the rate embedding data equals to 1 bit and so on.

2- The stego images have the same size of the host images and the same visible properties then the human eyes cannot distinguish between the two images.

3- The distortion began when the embedding rate equals to (5 bits).

4- The hiding data can be extracted without losing so this method can be used to transmit data.

5- Peak signal to noise ratio (PSNR) and The mean square error (MSE) has been computed for each data hiding rate and the minimum value of (PSNR) was (56 db) for the rabbit image and the minimum value was (55 db) for the airplane image, that means the difference cannot be detected where the human eye cannot detect the difference between two images if the PSNR value is bigger than 30 db.

6- This method cannot be destroyed after compression and decompression process, which means the receiver, can extract the hiding data completely.

Figure (2) shows the host images (original) and the stego images (coded) for each number of embedding bit, and table 1 shows the number of changing pixels, the number of embedding bits and the values of PSNR corresponding to each case.

Conclusion

A lossless (reversible) data embedding technique is presented , this technique depends on least significant bit (LSB) method, by changing the grey scale of chosen pixels in the host image.

The amount of embedding data and changing pixels depend on the capacity (size) of the host image and the number of embedding bits. In spit of changing the statistical properties of the image the human eyes cannot detect the difference between the host and the stego image so this method can be used to translate secret data without detection.

References

1- Curran,K, Bailey, K. (2003), International Journal of Digital Evidence, 2: (2), 1-40.

2- Richer,P. (2003), GIAC Practical Assignment for GSEC, SANS Institute Certification "Steganalysis:detecting hidden information with computer forensic analysis".

3- Dabeer,O.;Sullivan,K;Chandrasekaran, S. and B.S. Manjunath, (2004),IEEE TRANSACTION ON SIGNAL PROCESSING ,52: (10),3046-358

4-Eugene ,T.Lin and Edward, J.Delp.(1999), Video and Image Processing Laboratory , School of Electrical and Computer Engineering, Purdue University, West Lafayette, Indiana "A Review of Data Hiding in Digital Images",.

5- Friddrich ,J. and Goljan,M. (2003). " On Estimation of Secret Message Length in LSB Steganography in Spatial Domain" Department of Electrical and Computer Engineering,SUNY Binghamton, Binghamton.

6-Chuan –Ho Kao and Ren-Junn Hwang, (2005), Tamkang Journal of Science and Engineering. 8:(2), 99-108 .

Table: (1) Number of changing pixels , number of embedding bits and the corresponding (PSNR) and (MSE) values .

Image	Embedding bit rate	Number of changing pixels	Total number of embedding bits	MSE	PSNR(db)
Rabbit	1 bit	774	774	0.0085	68
	2 bits	774	1548	0.0341	62
	3 bits	774	2322	0.0768	59
	4 bits	774	3096	0.1365	56
	5 bits	774	3870	0.2133	54
Airplane	1 bit	600	600	0.0104	67
	2 bits	600	1200	0.0416	61
	3 bits	600	1800	0.0936	58
	4 bits	600	2400	0.1664	55
	5 bits	600	3000	0.2600	53

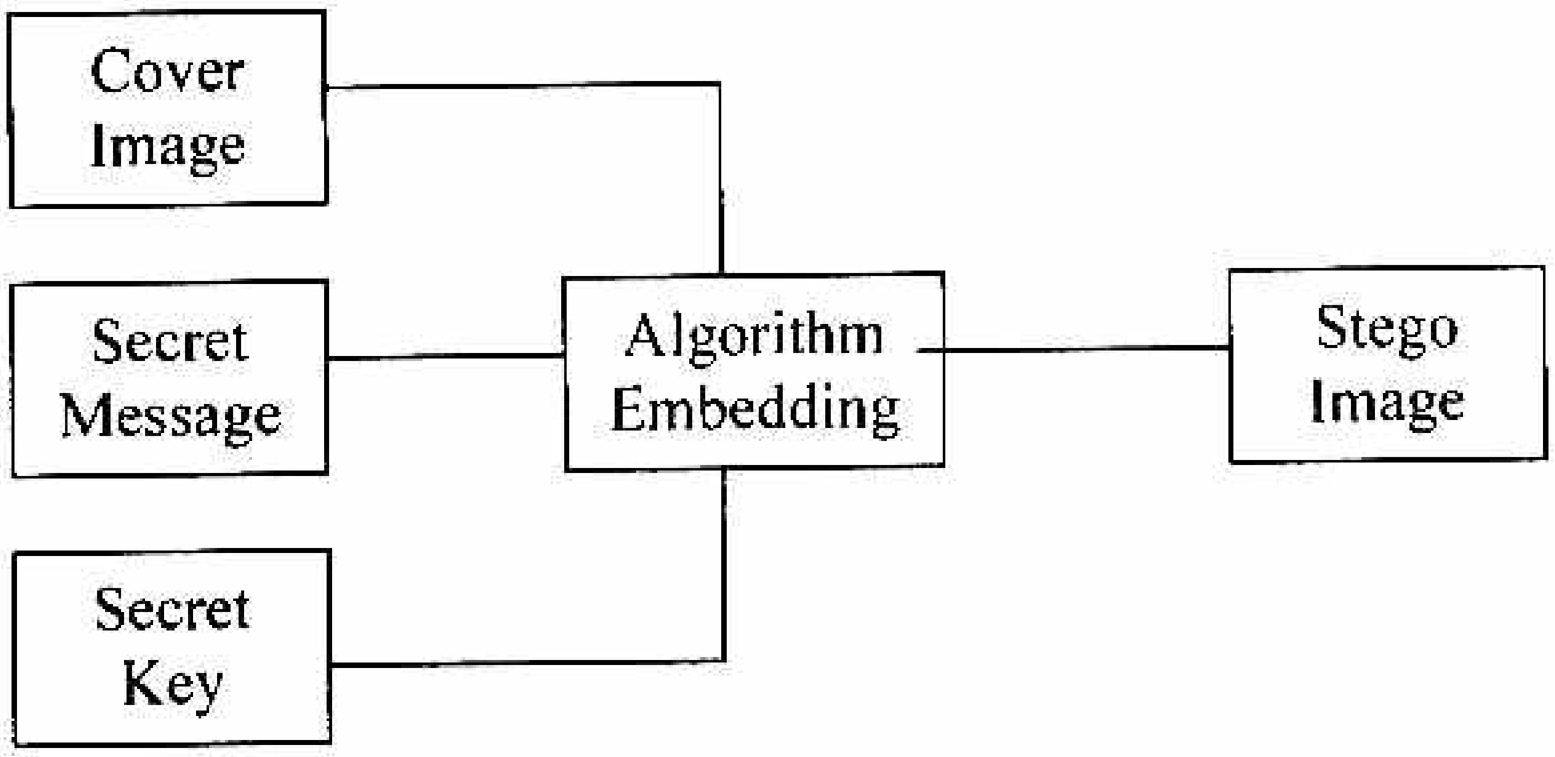

Fig. (1) Steganographic encoding system.

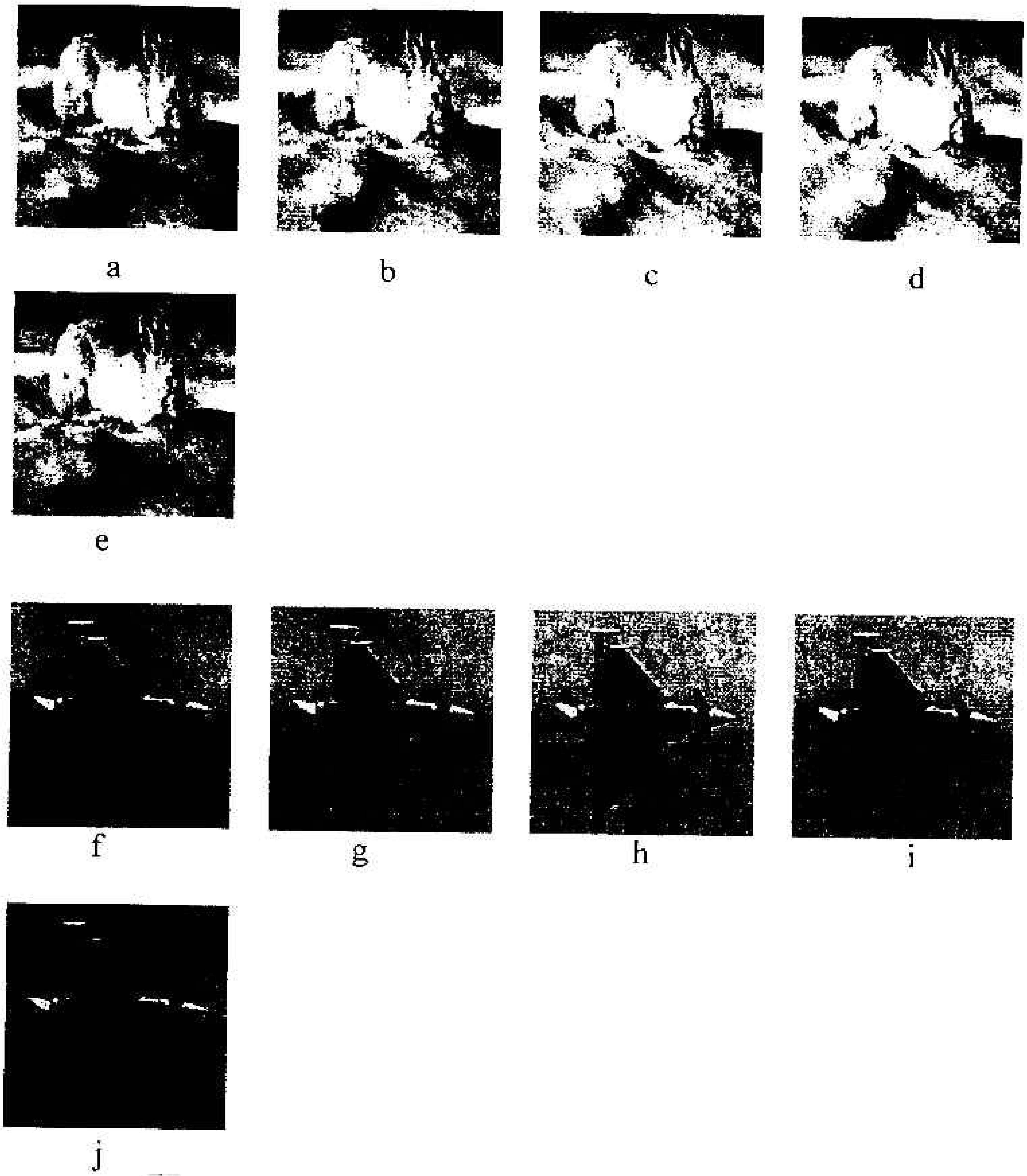

Fig. (2) (a,f) Host images (original). (b,g) Stego images (1 bit embedding),(c,h) Stego images (2 bits embedding),(d,i) stego images (3 bits embedding), (e,j) stego images (4 bits embedding).

إخفاء بيانات من دون فقدان في صورة باستعمال طريقة LSB

عادل اسماعيل كاظم
قسم الفيزياء ، كلية ابن الهيثم ، جامعة بغداد

الخلاصة

قُدِّمت في هذا العمل طريقة إخفاء بيانات داخل صورة كوسط ناقل من بدون فقدان لهذه البيانات (طريقة إنعكاسية) باستعمال تقنية LSB (بت ذات القيمة الاقل) ، التـــي تمكننا من نقل بيانات (نص أو صورة،...) داخل صورة (صورة مضيفة) اعتماداً علـــى مفتاح سري حتى لا يتم كشفها،يتم النقل من بدون خسارة أية بيانات أو تغيير في حجـــم الصورة المضيفة أو منظرها الخارجي (خواصها البصرية) . بعد ذلك تُستخلص البيانات المخفية من الصورة المضيفة باستعمال المفتاح السري نفسه ومن دون فقدان ايضا وذلك بعكس عملية التجفير وباستعمال ومعرفة المفتاح السري نفسه. وقد طُبقت هذه الطريقـــة من صورتين وباستعمال عدة نسب للإخفاء وكانت النتيجة عدم تمييز الصورة الاصـــلية عن الصور المجفرة كما طُبقت طريقة (PSNR) و (MSE) لاستخراج نـــسب الخطـــأ (الاختلاف) بين الصور المجفرة والصورة الاصلية .