Steganography using Energy-LSB Embedded Method

Zainab M. Hussain* (Lecturer) Ph.D

Abstract

In this paper embedding approach based on energy function and a Least Significant Bits (LSB) method was proposed to hide a secret message in a highly color or intensity part of an image that divided into blocks. Even with a different format types and different sizes of the selected images to cover and hide a variable size of a message, the quality results, show that the less distortion of the stego image as compared with the cover image and the proposed algorithm is robust to hide a randomize secret message even with decreasing the sizes of the blocks.

Keywords: *Steganography, Energy, (Least Significant Bits) LSB, MSE, PSNR.*

*Almansour University College

1. Introduction

Steganography is the art and science of writing hidden messages in such that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through Mystery. Steganography is the word of Greek origin which means "concealed writing" from the Greek words *steganos* meaning "covered or protected". In general, messages will appear to be something else such as: images, articles, shopping lists, or some other cover text and classically, the hidden message may be in invisible ink between the visible lines of a private letter [1].

Least Significant Bits (LSB) is a simple approach for embedding information in cover image; this can be done by embedding the bits of the message directly into least significant bit plane of the cover image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the small change in amplitude. To hide a secret message inside an image, a proper cover image is needed such that the data is hidden in the least significant bit of each byte in the image [2].

In this paper a steganography method to hide a secret message in a cover image was proposed. This method is depending on blocking the image and embedding the secret message in the higher energy blocks using the LSB method.

The rest of this paper is organized as: section 2 describes the steganography basics, section 3 focuses on the measurements used to measure the quality of the proposed method. While section 4 describes the proposed method, section 5 illustrates the experimental results. Finally the conclusions are in section 6.

2. Steganography

Coding secret messages in digital images today is the most widely used of all methods in the digital world . This is because it can take advantage of the limited power of the human visual system (HVS). Any plain text, cipher text, image and any other media that can be encoded into a bit stream can be hidden in a digital image. With the continued growth of strong graphics power in computers and the research being put into image based steganography, this field will continue to grow at a very rapid pace [2]. Steganography techniques use different carriers (cover medium in digital format) to hide the data, these carriers may be network

packets, hard drive, amateur radio waves, or generally any computer file types such as: text, image, audio and video. Restrictions and regulations are thought of in using steganography due to the threat from law and rights enforcing agencies and the need of organizations aiming to secure their information. Many easy to use steganography tools are available to hide secret messages on one side of communication and on the other side detect hidden information. Steganography uses cover to embedded secret data, this cover is randomly chooses and for the same secret data everyone can choose different cover without a prior knowledge which one is better, because there are no rules or measurements use for choosing suitable cover [3].

The least significant bit (LSB) technique is used to embed information in a cover image by changing pixels by bits of the secret message. These changes cannot be perceived by the human visibility system. It is works by representing each character (byte) of the secret message as a set of 8-bits (1 byte). Then hide/replace the bits of the characters in the least significant bit of the pixels in the stego-image. If the secret message has n characters, then LSB technique need at least (n*8) pixels in the stego-image to hide the bits of the n characters [4].

Using an energy function allows a stenographic technique to select a set of pixels to embed depending on the image content. This is in contrast to typical techniques that use some a priori fixed scheme such as randomly distributing the message throughout the image [5]. The energy tells us something about how the colors distributed. Assume the *P(g)* to be the *g=0..L-1* color entry distributed in an image then the energy function can be defined by [5]:

$$f = \sum_{g=0}^{L-1}\{P(g)\}^2 \qquad \ldots(1)$$

3. Evaluation Parameters

To measure the image quality, commonly used Mean-Squared Error, Peak Signal-to-Noise Ratio to compare stego-image with cover results [6].

3.1. Mean-Squared Error

The mean-squared error (MSE) between two images I_1 (*m,n*) and $I_2(m,n)$ is [6]:

$$MSE = \frac{\sum_{M,N}[I_1(m,n) - I_2(m,n)]^2}{M*N} \quad ...(2)$$

M and *N* are the number of rows and columns in the input images, respectively. Mean-squared error strongly depends on the image intensity scaling [6].

3.2. Peak Signal-to-Noise Ratio

Peak Signal-to-Noise Ratio (PSNR) is measured in decibels (dB) avoids this problem by scaling the MSE according to the image range [6]:

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \quad \ldots(3)$$

Where R, is the maximum fluctuation in the input image data type.
For example, if the input image has a double-precision floating-point data type, then R is 1. If it has an 8-bit unsigned integer data type, R is 255, etc [6].

4. The Proposed Method

In image steganography there are many methods used to hide information in image. In this paper an algorithm based on blocking a cover image, and finds the maximum energy blocks to embedding a secret message using the LSB method was proposed. Figure (1) list the steps of this algorithm such that the cover image is divided into a number of blocks determined by a predetermining the desired size of the block by the user. The idea of blocking is proposed to be used with the energy function as methods to increase the security of randomly hide the secret message in the cover image and avoiding the traditional sequentially hiding method. The least significant bit (LSB) is used to embed a secret message in cover image by change image pixels by bits of the message. Figure (2) illustrate an example of applying the proposed algorithm.

Input: Cover image, Secret Message to be embedded.
Output: Stego image.
Step1: Read a Cover image and a secret message to be embedded.
Step2: Devide a cover image into a number of blocks depending on the size of each block which was determined by the user.
Step3: Calculate the energy for each block.
Step4: Sort the blocks in descending order.
Step5: Convert the Secret Message into binary.
Step6: Convert all image blocks into binary.
Step7: Embed the secret message in the maximum energy blocks using the LSB method.
Step8: Reconvert and Rearrange the cover image to have the original image.
Step9: Find the PSNR and the MSE measures.
Step10: Retrieving the secret message using the extraction method.

Figure (1) the proposed steganography method

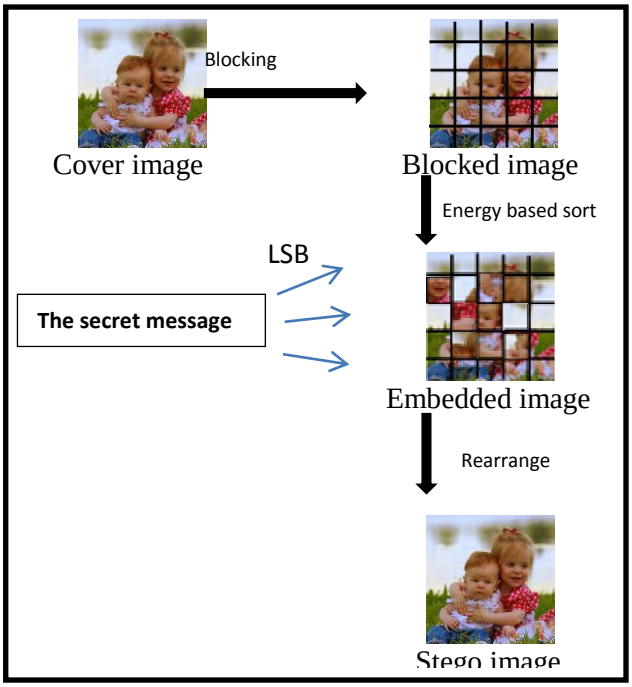

Figure (2) Example of applying the proposed steganography algorithm

5. Experimental Results

Different types and different sizes of a gray scale cover images are used such as (jpg, bmp, tiff, and png). Figure (3) shows the images used in the experiments. The evaluation parameters MSE and PSNR are used to verify the image quality between cover image and stego image in experiments which varied depending on the variation of many factors effects the performance of the proposed algorithm such as the size of the cover image, the size and the number of the blocks of cover image, and the length of the secret message. The sizes of the blocks in experiments are chooses as (8×8, 16×16, 32×32, and 64×64 pixels). The length of the secret message is chooses by two randomization characters lengths 20 and 256.

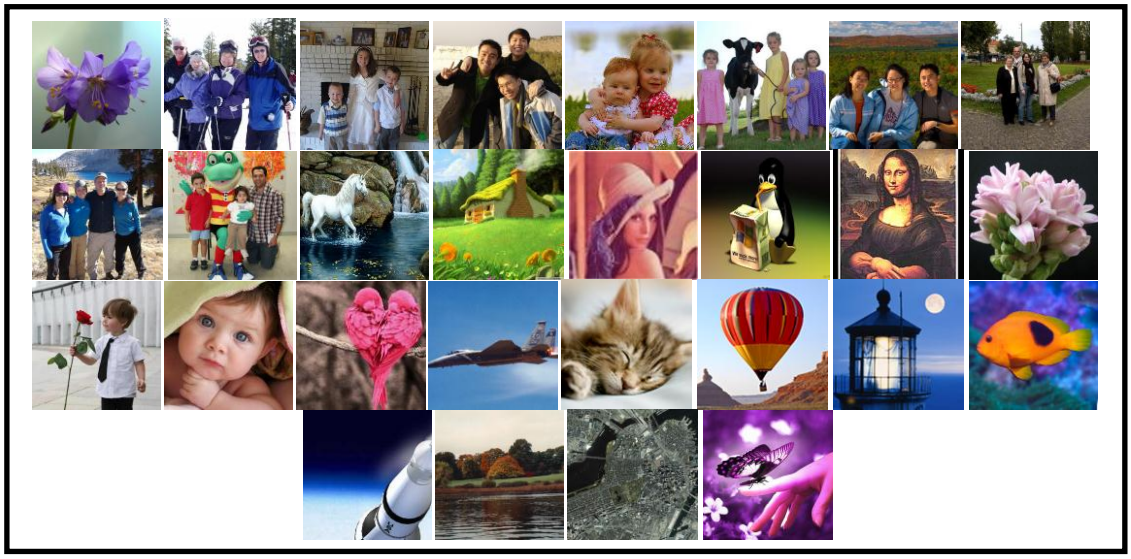

Figure (3) the different types of images used in the experiments

The first experiment focuses on the effect of changing the size and the number of the blocks of the cover image. The number of blocks is varied depending on the size of the images and the size of the block previously determined by the user. Figure (4.a) shows the original "Monaliza.jpg" cover image of size 256×256 pixels with samples of the first maximum energy blocks illustrated in figures (4.b-4.e) for a block size of

(8×8, 16×16, 32×32, and 64×64 pixels) respectively. Figure (4.f) shows the stego image hiding a selected secret message of length 256 characters and blocking size of 64×64 pixels.

The PSNR and MSE between origin cover image and stego image of this experiment are illustrated in figure (5). From this figure it can be seen that the values of PSNR are increases and MSE are decreases while increasing the size of the blocks which implies the variation of the number of blocks of the cover image used to embed the secret image. This experiment is proved and applied using the selected 28 cover images and the average results of PSNR and MSE are illustrated in table (1).

The decreasing of block size means using many blocks to hide the secret message such that increase the pixels that will change such that the PSNR is decrease and the MSE increase. Also it can be seen from this table that the ratio of changing the values of PSNR as an average is 0.3777 which is very low and means that the proposed algorithm is robust while decreasing the sizes of the blocks.

(a) (b) (c) (d

(e) (f)

Figure (4) a) Original 256×256 "Monaliza.jpg" cover image, (b)-(e)first maximum energy blocks for a block size of (8×8, 16×16, 32×32, and 64×64 pixels) respectively, (f) stego-image hides a secret message of length 256 characters.

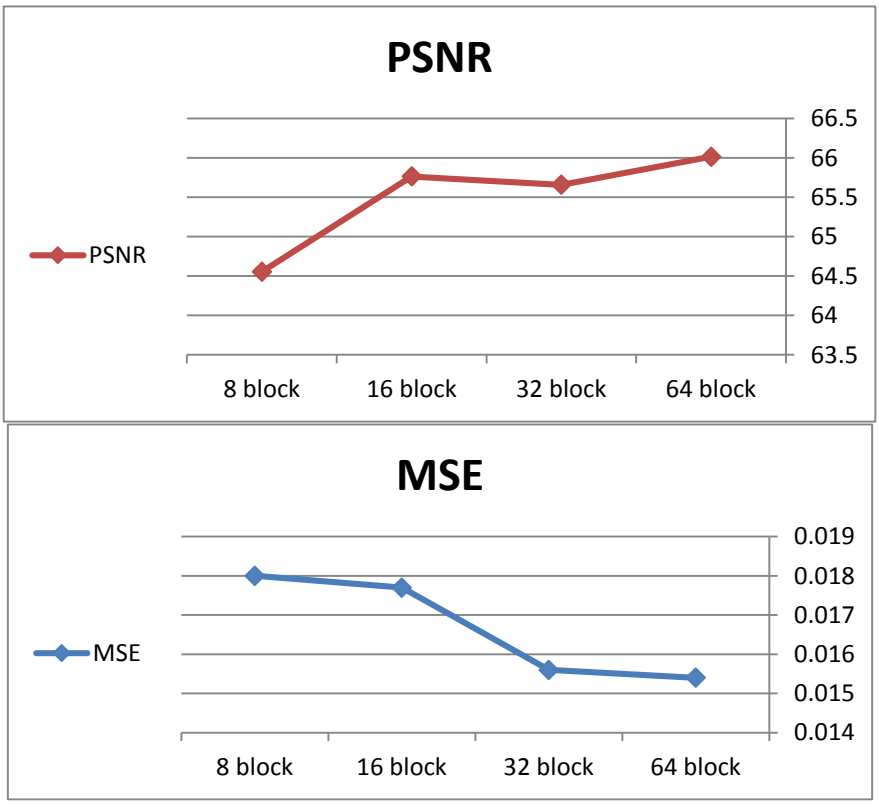

Figure (5) the results of PSNR and MSE measures for experiment in figure (4)

Table (1) average results of MSE and PSNR for 28 images using the proposed steganography algorithm.

Measure	Block size			
	64 × 64	32 × 32	16 × 16	8 × 8
MSE	0.007551	0.00756	0.007586	0.00765
PSNR	72.66718	71.81766	71.8121	71.534

Second experiment focuses on the length of the secret message which is an important factor that affects the quality of the stego image; this can be seen in table (2) which illustrate the results of PSNR and MSE between origin cover image and stego image for 28 selected cover images blocked into 64×64 pixels and used to hide two secret messages of two randomized lengths 20 and 256 characters.

Table (2) PSNR and MSE results between origin cover image and stego image for 28 selected cover images blocked into 64×64 pixels and used to hide two secret messages of two randomized lengths 20 and 256 characters.

image	Image size	MSE (20)	PSNR(20)	MSE(256)	PSNR(256)
flower.jpg	448×448	2.59E-04	83.9775	0.0058	70.4459
f1.jpg	768×768	7.63E-05	89.9274	0.0017	75.6261
f2.jpg	384×384	3.32E-04	82.387	0.0081	68.9796
f3.jpg	704×704	8.68E-05	87.8881	0.002	74.4715
f4.jpg	320×320	5.18E-04	80.6835	0.01	68.0582
f5.jpg	640×640	1.56E-04	86.059	0.0026	74.0425
f6.jpg	832×832	6.79E-05	89.6313	0.0017	76.6299
f7.jpg	832×832	8.52E-05	88.8248	0.0018	76.2232
f8.jpg	768×768	8.99E-05	89.0256	0.0018	75.2122
f9.jpg	640×640	1.12E-04	86.4388	0.0028	74.0541
hors.jpg	384×384	2.98E-04	83.2853	0.0081	69.5562
house.jpg	1024×1024	3.53E-05	90.8304	0.0012	78.018
lena.jpg	512×512	0.0029	84.364	0.0612	70.8769
linux.jpg	1024×1024	5.44E-05	90.7025	0.0011	77.3747
mona.jpg	256×256	8.70E-04	79.4832	0.018	66.014
006.jpg	320×320	4.20E-04	81.4787	0.011	68.0545
baby.jpg	448×448	2.44E-04	84.0807	0.0055	70.7622
baby1.jpg	704×704	9.28E-05	87.3235	0.0023	74.8843
berds.jpg	448×448	2.79E-04	83.6718	0.0053	70.1921
f15.bmp	320×320	4.79E-04	81.2441	0.011	67.642
cat.bmp	512×512	1.75E-04	84.3388	0.0044	71.7861
baloon.bmp	1024×1024	4.86E-05	90.9332	0.001	77.8485
moon.bmp	768×768	7.63E-05	89.5033	0.0019	75.5401
fish.bmp	640×640	1.29E-04	88.3438	0.0027	73.6701
main.bmp	256×256	7.78E-04	79.3936	0.0155	65.7879
a.tif	256×256	7.32E-04	78.49	0.0176	65.7025
bost.tif	2880×2880	5.43E-06	100.5062	1.27E-04	86.6405
beat.png	448×448	2.09E-04	84.2544	0.0052	70.5873

From this table it can be seen that the quality of the cover image affected by increasing the length of the secret message. The PSNR is

decreases (lower quality) by increasing the secret message length and the MSE is increases and vice versa. This is due to the increasing of the number of pixels in cover image that will change such that the distortion is increases and the quality is decreases.

While the size of the cover image is increases the quality of the stego image also increases even with increasing the number of the blocks by decreasing the size of the block, this is because the ratio of the image pixels to the number of character is increases therefore the distortion is decreases. This can be shown in figure (6) and figure (7) which illustrates the results of the PSNR and MSE measures respectively for the tested images embedded with 256 characters of secret message and using different blocking sizes. From these figures it can be seen the robust of the proposed algorithm even with changing the sizes of the images and the sizes of the blocks.

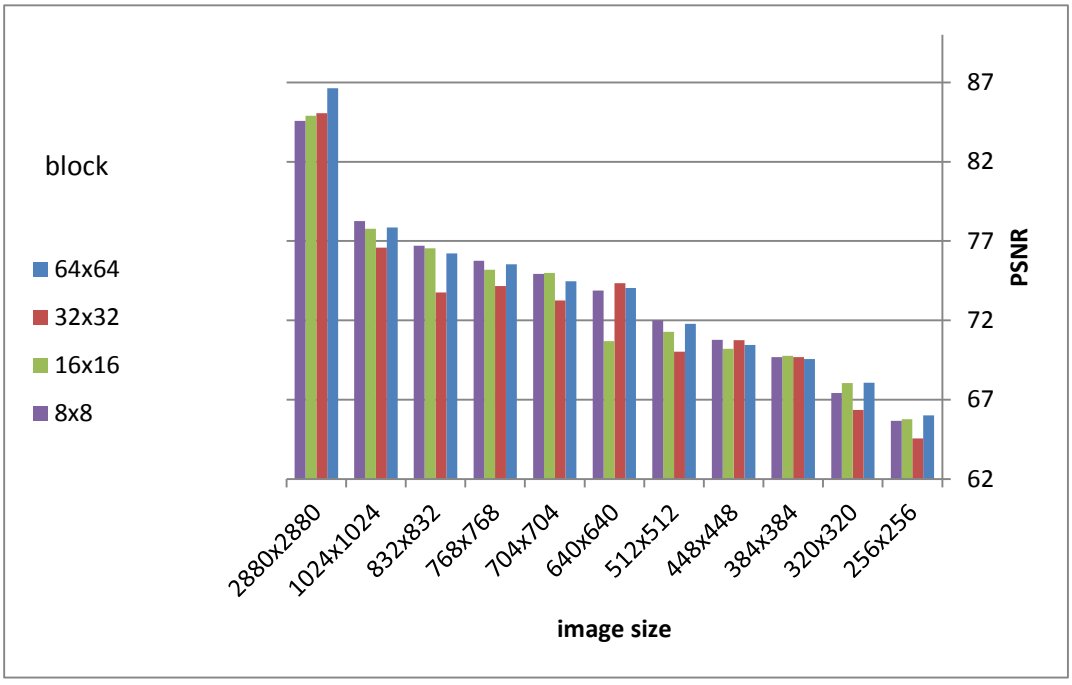

Figure (6) the results of the PSNR measure for the tested images embedded with 256 characters of secret message and using different blocking sizes.

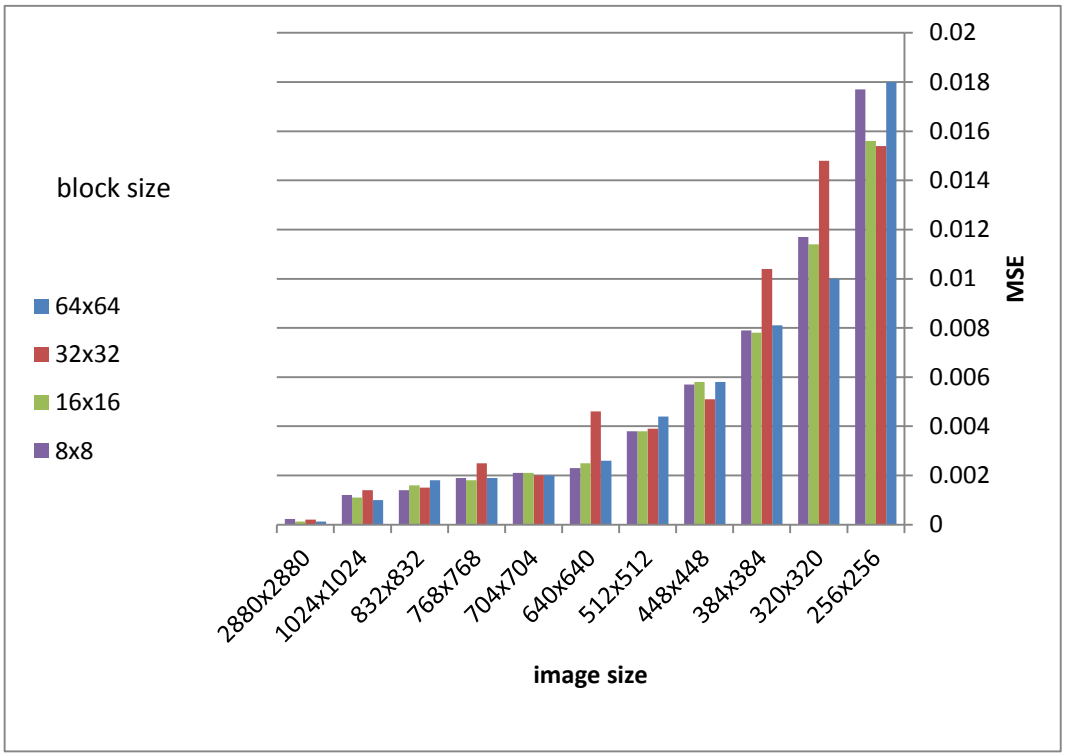

Figure (7) the results of the MSE measure for the tested images embedded with 256 characters of secret message and using different blocking sizes.

6. Conclusions

A steganography algorithm based on a combination of LSB and the maximum energy is proposed in this paper. The quality of the stego image is measured using PSNR and MSE. The idea of using the maximum energy blocks to hide the secret message is that the maximum entropy is mean the most interesting intensity pixels such that the changes in these pixels produce less disturbances and less distortion. The size of the blocks of the cover image is affects the quality of the stego image; therefore the increasing of the block size decreases the changes in stego image such that increase the quality (PSNR) and decrease the MSE. Even with decrease the sizes of the blocks used to hide the secret images but the proposed algorithm is robust.

The length of the secret message is decrease the quality of stego image and increase the error ratio when it increases. This is because the increasing of distortion of pixels. Also by increasing the size of cover image the quality of the stego image will be increases, but the change is very low because the robust of the proposed algorithm.

7. References

1. Eshita Bheda, Chirag Khubdikar, Amol Patwardhan, Mayur Kalebere, and Sowmiya Raksha, "***Multimedia Steganography with Cipher Text and Compression***", International Journal of Emerging Technology and Advanced Engineering, Volume 3, Issue 4, April, **2013.**

2. Dilip Vishwakarma, Prof. Satyam Maheshwari, and Prof. Sunil Joshi," ***Efficient Information Hiding Technique Using Steganography***", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 1, January **2012**.

3. Nidhal K. El Abbadi," ***Cover Optimization for Image in Image Steganography***", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 1, No 3, January **2013**.

4. Dr. Mohammed Abbas and Fadhil Al-Husainy, "***Message Segmentation to Enhance the Security of LSB Image Steganography***", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, **2012**

5. Ian Davidson, Goutam Paul and S. S. Ravi, "**Steganography Using Spatially Interesting Pixels**", ICISS **2012**: 134-148.

6. V. Lokeswara Reddy, Dr. A. Subramanyam, and Dr.P. Chenna Reddy, "***Implementation of LSB Steganography and its Evaluation for Various File Formats",*** Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872, **2011**

إخفاء المعلومات باستخدام التضمين بطريقة الطاقة- البت الأقل أهمية

م.د.زينب محمد حسين*

المستخلص:

في هذه الورقة تم اقتراح طريقة تضمين تعتمد على دالة الطاقة والبت الاقل اهمية (LSB) لإخفاء رسالة سرية في الجزء الاكثر لون أو كثافة من الصورة المقسمة الى كتل. حتى مع استخدام أنواع مختلفة الشكل و مختلفة ألاحجام من الصور المختارة لتغطية وإخفاء رسالة ذات حجم متغير، فان جودة النتائج ، تبين تشويه أقل لصورة الstego بالمقارنة مع صورة الغلاف والخوارزمية المقترحة قوية لاخفاء رسالة سرية بطريقة عشوائية حتى مع تقليل أحجام الكتل.

*كلية المنصور الجامعة