Image in Image Steganography based on modified Advanced Encryption Standard and Lest Significant Bit Algorithms

Aymen Mudheher Badr[a] Mohamed layth talal[b] Ghassan Sabeh[c]

[a]*Law and Political College, University of Diyala,Diyala, Iraq*

[b]*Administration and Economic College, University of Diyala, Diyala, Iraq*

[c]*College of Sciences, University of Diyala, Diyala, Iraq*

Aemn_1978@yahoo.com mohammed.l.talal@gmail.com ghassan.programer@gmail.com

Submission date:- 1/4/2018 Acceptance date:- 7/5/2018 Publication date:- 9/9/2018

Keywords: *Encryption, AES, LSB, Steganography, Decryption, watermark, PSNR, MSE.*

Abstract

Because the big grown of digital market and the growing demand for protection to data and information which transmitted through the Internet. Steganography it is art of embedding, hiding information into different digital media, it was the main reason to increase its importance in exponential development of the secret communication of computer and digital cloud users over the internet. There are a lot of techniques and different ways to achieve hiding data. Usually, the data embedding is obtained in communication such as image, text, voice or any multimedia content for copyright and also in military communication for authentication and many other different purposes. In this paper we protected the information in two ways: Encryption and Steganography. The basic idea is to present a method that encrypted the message firstly by using The AES (Advanced Encryption Standard) it is a symmetric-key encryption each of these ciphers it has 128-bit the size to block, and size keys of 128, 192 and 256 bits. Secondly, hide that encrypted message in color cover image in the Least Significant Bit (LSB) to image's frame with (.bmp, .jpg) extensions. Our scheme is to enhance the ability of LSB algorithm to include the storage of information and images encoded and intangible sense of human vision. That two methods to increased together the security attend any attack.

1. Introduction

The steganography is type of arts to hiding information or any data in different ways to prevent its detection. It was usually given as a substitute for cryptography but it is not usually used in that way. Steganography is not intended to replace cryptography but supplement it.

The issue of security of data has increased unique importance. One of the most important in the area of Information security is the concept of hidden exchange of data or information via internet. Hiding information or image inside image is named steganography, the main purpose of steganography is to put and hide a message in some media to obtain new data (with the secret message) practically indistinguishable from the original media [1]. The steganography word was derived from the two Greek's words: stegano and graphic, its mean "the covered writing". Steganography is the direct derivation of the watermarking methods used for the hiding the information [2].

In the system of image hiding, the images that was used to embed the secret data is called (host image) or (cover image). Stego-image it is the resulting image from the embedded original image with secret data [1]. The host media like a digital video, images, audio or any other type of media [3].

Known as cryptography or blind since ancient times, it was used in the military and military field. It was stated that the first the process of encryption for messaging between the army sectors were the (Pharaohs) and also reported that the Arabs them obsolete in the area of encryption attempts. And Chinese used many ways in cryptography to transmit messages during wars. It was their intent from the use of encryption is to hide the shape of the real messages even if they fell into the hands of the enemy, it is difficult to understand it.

1.1. The Advanced Encryption Standard Algorithm AES

It is one of a block cipher algorithm which is intended to replace DES algorithm as a standard recognized for some applications [4]. AES is a standard algorithm for encryption and decryption data (Advanced Encryption Standard). In our paper the AES was used because due to its advantages to secure documents and is proven to be safe based on NIST Standard [5]. The AES algorithm shown in fig.1.

AES have three types of encryption models (128, 192, and 256) bits. Each cipher mode has agreement in a number of rounds (Nr), it based on key length of (Nk) words. The state block size (Nb) is constant for all encryption modes. The128-bit block is referring to the state. Each one of state is included 4 words. Each one of word is thereafter defined as 4 bytes. Both encryption and decryption begin with the round key expansion created by the key schedule function [6]. Table.1 we show the possible key, state block and round combinations [7].

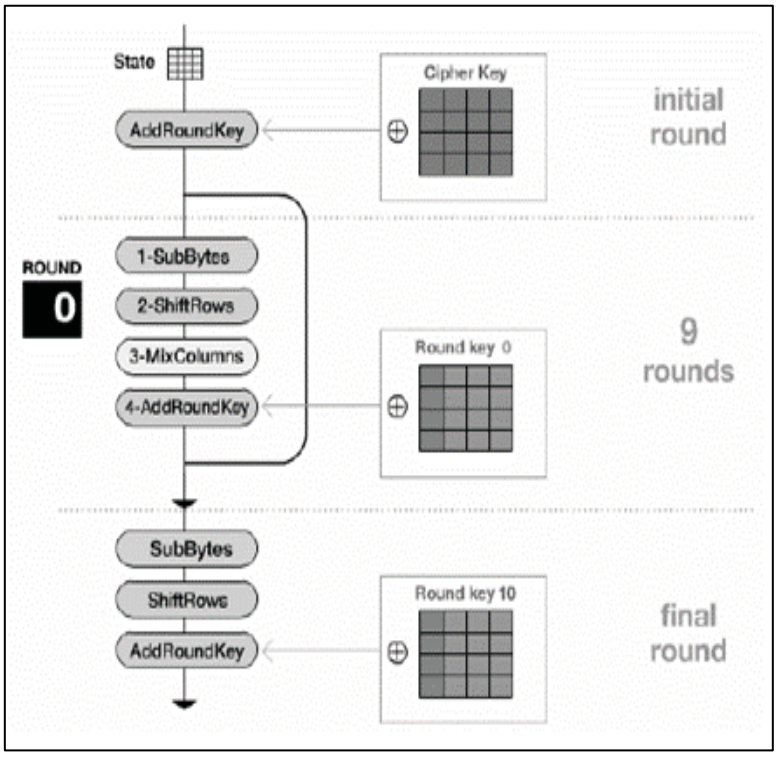

Fig. 1. Encryption Process Diagram

Table1. ASE Categorization

KeySize (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Number of Rounds	10	12	14
Expanded key size (words/byte)	44/176	52/208	60/240

1.2 LSB *(Lest Significant Bit)* Algorithm

It is classified as one of the commonly used digital steganography and embedding techniques [8]. It called like that because the way to embedded message within a cover image. In computer science, the term Least Significant Bit (LSB) refers to the smallest (right-most) bit of a binary order.

When we applied LSB techniques to every byte of 24-bit to image, each pixel can be encoded it to three bits, as each pixel was represented by three bytes. For example, the letter (a) we can be embedding it in three pixels. We can represent original three pixels as three 24-bits:

(00100101 10101001 11101000)
(10100111 10001000 11011001)
(01101000 10100111 10101001)

The binary value for letter (a): 01100001, we inserting the binary value of letter (a) into the three pixels, start from the left byte, the result is:

(00100100 10101001 11101001)
(10100110 10001000 11011000)
(01101000 10100111 10101001)

To hide information like (decimal numbers) or (characters) after convert them to binary and convert each value of color in colored cover image from decimal to binary and since each value of color is made up of three colors value Red, Green and Blue (RGB), the embedding was being easily and without any changes in the pixel bits will be unfeeling to human eyes.

2.Related works

In Al-Husainy [9] paper, proposed enhance the performance of the Classic-LSB image steganography technique. The segmentation message LSB image steganography technique was suggested by splitting the long secret message to number of short segments and hide these short segments in different parts of the best matched LSB in the pixels of the stego-image.

The researcher Subarna Shakya [10] proposed a method, encrypted the message in the first by using algorithm based on Fibonacci series or the Rijndael cryptographic algorithm, and then embedded this encrypted message inside color image using improved Least Significant Bit (LSB) substitution method where the secret information is stored into a specific position of Least Significant Bit of an image based on the security key entered. This combinational methodology will satisfy the requirements such as capacity, security and robustness for the secure data transmission over an open channel.

LSB based image steganography using secret key which provides good security issue than general LSB based image steganography methods. That method is an effective way to integrate hidden information reporting and it is very difficult for the unauthorized users to identify the changes in stego image, them used a secret key to hide hidden information into cover image the LSB of RGB bits. This process provides a new dimension for image steganography. It is very difficult to recover the hidden information for third party without knowing the secret key.

Z. Ni, Y.-Q. Shi [11] was proposed an image reversible data hiding algorithm which can recover the cover image without any distortion from the stego image after the hidden data have been extracted. Histogram shifting is the better technique between the existing approaches of reversible image data hiding because it can control the modification to pixels, thus limiting the embedding distortion, and it only requires a small size location map, thereby reducing the overhead encountered. The current state-of-the-art for reversible image data hiding is the general framework presented by those researchers.

Ahmed Laskar & Hemachandran [12] employed a method for applications that require high-volume embedding with robustness against certain statistical attacks. This scheme is an attempt to identify the requirements of a good data hiding algorithm and it is not intended to replace steganography or cryptography but rather to supplement it. If a message is encrypted and hidden with a LSB steganographic method the embedding capacity increases and thus it is possible to hide large volume of data and the method satisfies the requirements such as capacity, security and robustness which are intended for data hiding. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. If an attacker was to defeat the steganographic technique to detect the message inside the stego-object, the attacker would still require the cryptographic decoding key to decipher the encrypted message. The main aim is to develop a system with extra security features where a meaningful piece of text message can be hidden by combining two basic data hiding techniques.

3. Proposed method

In his section we present our scheme, it used color image (Cover) with extended (.bmp or .jpg). The basic idea that used round of image (frame) because all times didn't have any important information and the human ayes always see the object of image more than round of image, as show in Fig.2.

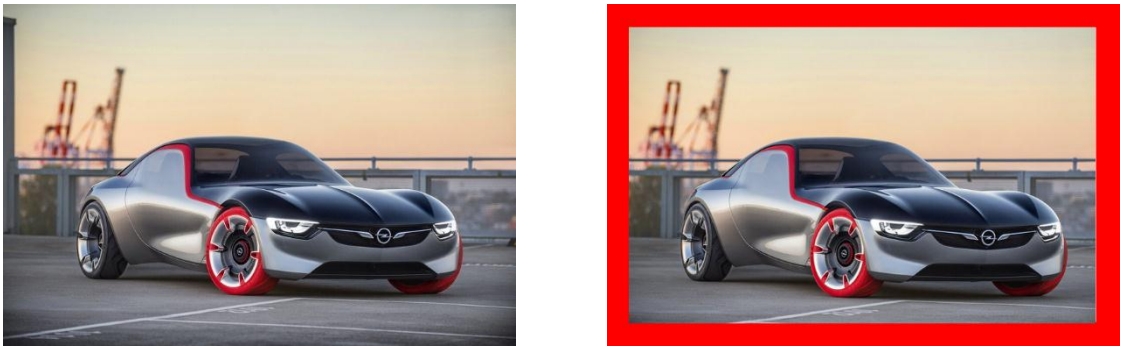

Fig. 2. The image round

2.1 Encryption:

First algorithm: Message Encryption (W):

Input data: Watermark (message (W)) as gray level with size (100*100) or (200*200).

The result: (W') Encrypted watermark.

1- Let (W) be original message (gray image) with size (100*100) or (200*200).
2- Split (W) image to four parts {P1, P2, P3, and P4} as show in Fig.3.
3- Swapping between those four parts as:

TA= P1; P1= P4; P4= TA;
TA= P2; P2= P3; P3= TA; Where TA: temporary array

4- By AES Algorithm to Encrypted that parts to generate new encrypted parts.
W {P1, P2, P3, P4} ➔ AES ➔ W' {P1', P2', P3', P4'}

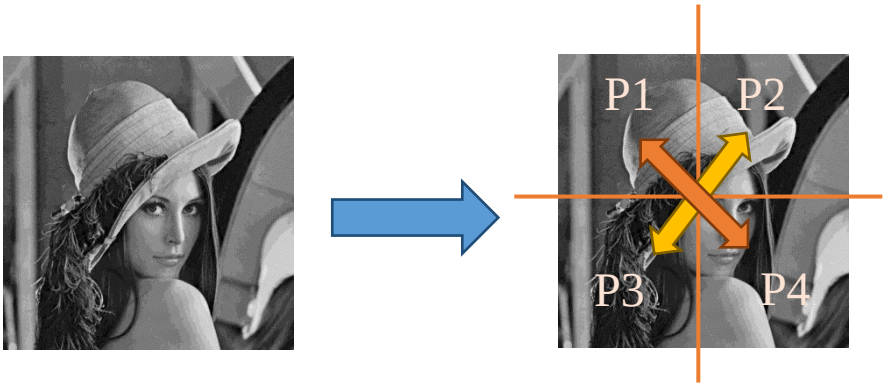

Fig.3. Splitting and Swapping between parts

2.2 Information Hiding:

By LSB algorithm to hide the encrypted watermark (W') by embed it in the color image data (C).

To obtain a large space to hide the information inside any image without and change to host cover information, our scheme used 3-bit for one pixel to RGB as show following:

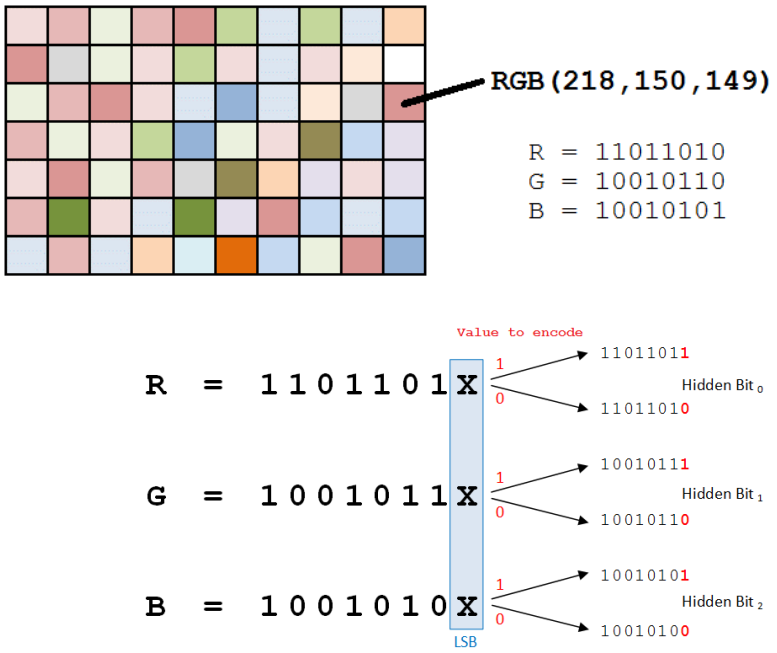

Fig.4. Pixel diagram and LSB to one pixel. [9]

Second algorithm: The Embedding:

Input data: Encrypted Watermark (W'), Color image (C)

The result: final image (C')

1- Reading color image as a cover (C).
2- By using LSB Algorithm to hide the encrypted watermark (W') inside the round of color cover (C) to generate (C').

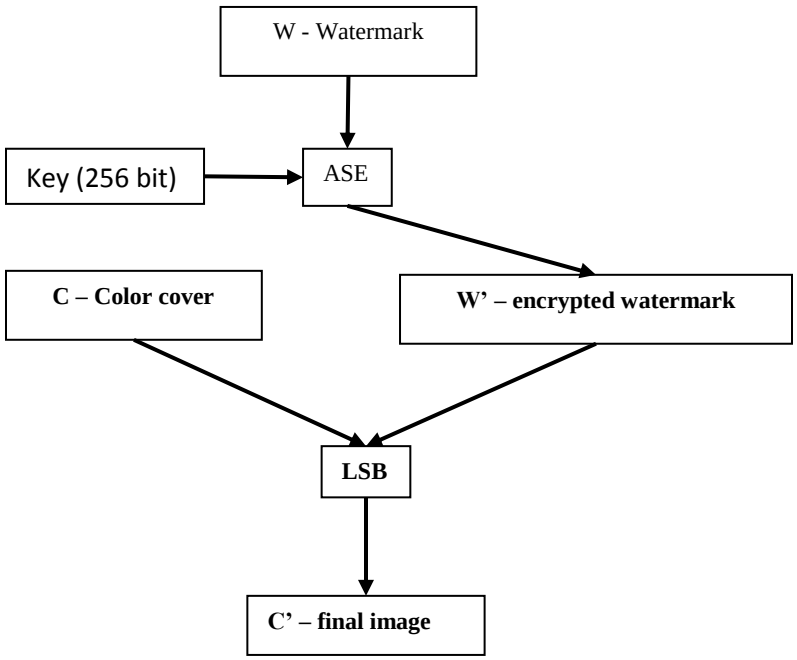

Fig.5. Encrypted watermark and embedding scheme

3.2.Extracting Watermark:

When revised the image from the sender after send it via internet or another, must chick is it original one or not? Because maybe happen some change on it after attend it to many type of attacking.

Extraction algorithm it is to extract the secure message from a round of color image. The first step, extract the watermark from the LSB to round of color cover and secondly make de-encrypted to watermark by using AES Algorithm to get the original message.

Third algorithm: Extraction:

1- Let be the color image (that received it stego-image) as (CR).
2- By LSB algorithm to round of color cover (CR), extract the watermark and let it be (WR').
3- Split the watermark (WR') to four parts {P1', P2', P3' and P4'}.
4- Using ASE (*Advanced Encryption Standard*) to decrypt each part of the watermark (WR') to get the original parts {P1, P2, P3 and P4}.
5- Swap the parts between them to get the right order to message to get an original message (WR).
6- Calculate NC.

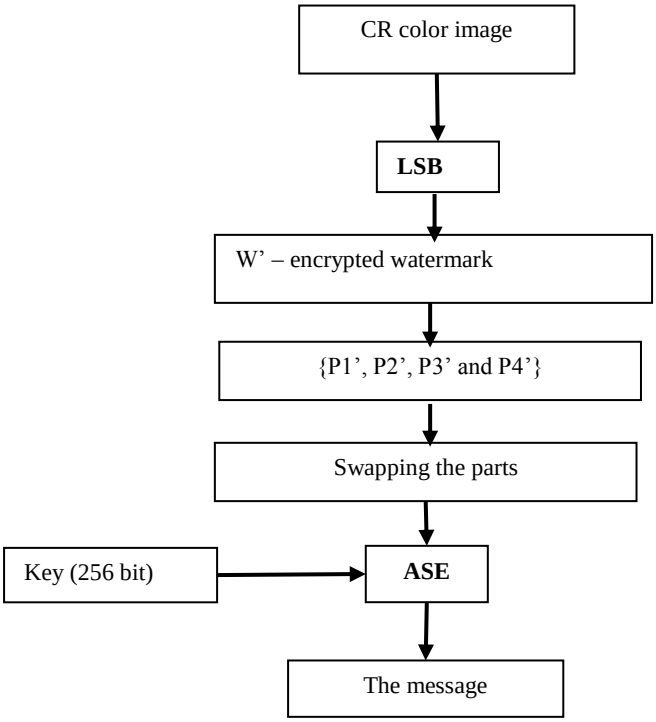

Fig.6. Extraction scheme

4. Results and Analysis

To evaluate the performance of the steganography by following parameters [8]:

1) The Capacity: It is the maximum amount of data was embedded into the image.
2) The Robustness: It is the message arrive to receiver without any change because the attacking like rotation, cropping, filtering and compression etc.
3) The stego-image quality that measured by using MSE, PSNR and NC.

- ***Normalization Correlation (NC):***

$$NC = \Sigma i\ sw\ (i) * s\ (i) / \Sigma i\ (s\ (i))^2 \qquad (1)$$

- ***Mean Squared Error (MSE):***

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N} \qquad (2)$$

- ***Peak Signal to Noise Ratio (PSNR):***

$$PSNR = 10\log\left(\frac{C_{max}^2}{MSE}\right) \qquad (3)$$

As a performance measurement for embedding capacity, the average number of bits embedded into each pixel is calculated as:

- Capacity = (Total Number of bits embedded into image/ Total Number of Pixels in image) (bits/pixel) (4)

The larger PSNR shows well quality of the image or in other terms lesser distortion. The bigger the PSNR esteem the littler the likelihood of visual assault by human eye [13][14].

Our scheme, applied on more types of image like (JPEG and BMP), the target of measuring is the good quality of the image that containing the resulting encrypted watermark.

The results of schema are shown in Table.1 with the values of (MSE, PSNR) and the Normalization Correlation to all the image is (NC = 1) to that size.

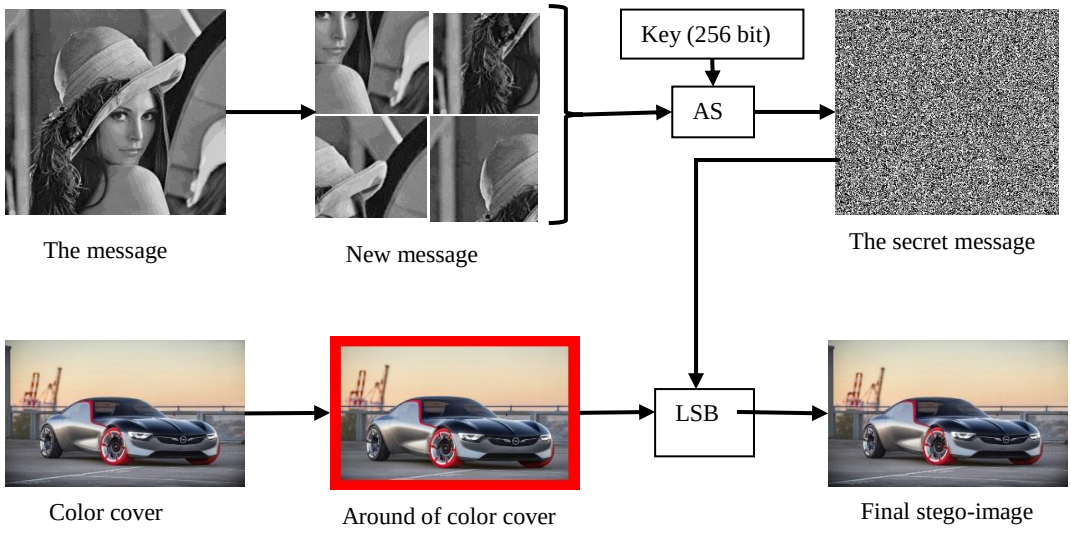

Fig.7. Encrypted and Embedding watermark

Table2. The PSNR and MSE values to stego-image

Image size	Image type		CAP		PSNR		MSE		NC	
	.Bmp	***.Jpeg***	***.Bmp***	***.Jpeg***	***.Bmp***	***.Jpeg***	***.Bmp***	***.Jpeg***	***.Bmp***	***.Jpeg***
100*100	Lena	Lena	4.1131	4.2360	71.546	72.275	0.64	0.65	1	1
	Baboon	Baboon	4.1568	4.1371	84.546	84.685	0.60	0.59	1	1
	car	car	4.1988	4.1831	68.023	69.001	0.62	0.61	1	1
200*200	Lena	Lena	4.7538	4.7362	74.465	74.756	0.62	0.64	1	1
	Baboon	Baboon	4.6908	4.7441	86.736	85.534	0.61	0.60	1	1
	car	car	4.7353	4.6322	70.664	70.645	0.63	0.64	1	1

5.Conclusions

Steganography and cryptography, will play to increasing role of secure in the future on the communication in the "digital world". The art of Steganography to hide a digital image or another media in another digital image (video, text and audio).

Our scheme in this research based on merge between encryption and hiding to gives high performance explained by the statistical estimators (objectively) and subjectively and the stego-image remains as the original one in size and quality.

The results shown the efficiency of our scheme, was the embedded and hidden information in the around of color image not made any distortion or lost in the cover data used. The division message and the swapping between 4 parts has led to increase the strength of the algorithm. The Hidden text after encrypted with modified AES algorithm led to increasing to secure of hidden information and it's gives better results than the existing methods.

CONFLICT OF INTERESTS

There are no conflicts of interest.

6.References

[1] C. Chan. L. M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition* Vol.37, pp. 469-474, 2004.

[2] D. Artz, "Digital steganographic: hiding data within data", *IEEE Int. Comput*, 5(3), pp. 75–80, 2001.

[3] Aakaash J ois, Tejaswini L, "Survey on LSB Data Hiding Techniques", *IEEE conference, 978-1-4673-9338-6*, 2016.

[4] Stalling, William, "Cryptography and Network Security 4th Edition", *Prentice Hall*, 2005.

[5] Annabelle Lee, "Guideline for Implementing Cryptography in the Federal Government", *NIST Special Publication*, 800-21A., 2005.

[6] Orlando J. Hernandez, etc. al, "A Low Cost Advanced Encryption Standard (AES) Co- Processor Implementation", *Journal of Computer Science & Technology (JCS&T)*, Vol.8, No.1, pp. 8-14, 2008.

[7] Rashi Kohli etc.,"S-Box Design Analysis and Parameter Variation in AES Algorithm", *International Journal of Computer Applications*, Vol.60, No.2, 2012.

[8] Ahmad M. Odat, Mohammed A. Otair, "Image Steganography using Modified Least Significant Bit", *Indian Journal of Science and Technology*, Vol 9(39), DOI: 10.17485/ijst/2016/v9i39/86878, 2016.

[9] Al-Husainy, M. A. F., "Message Segmentation to Enhance the Security of LSB Image Steganography". *Transit*, 3(3), 2012.

[10] Subarna Shakya, Sanjita Lamichhane," Secured Crypto stegano data hiding using Least Significant Bit Substitution and Encryption", *Journal of Advanced College of Engineering and Management*, Vol. 2, 2016.

[11] Z. Ni, Y.-Q. Shi, etc. al, "Reversible data hiding" *IEEE Trans. Circuits Syst*. Video Technol., vol. 16, no. 3, pp. 354–362, Mar. 2006.

[12] Ahmed Laskar, S., & Hemachandran, K, "High Capacity data hiding using LSB Steganography and Encryption", *International Journal of Database Management Systems*, 4(6), (pp.57-68), 2012.

[13] M. Hossain, S.A. Haque, F. Sharmin,"Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Iriformation", *Proceedings of 12th International Conference on Computer and Information Technology (ICCIT 2009), Dhaka, Bangladesh*, 2009.

[14] X. Li, B. Li, etc. al, "General framework to histogramshifting-based reversible data hiding" *IEEE Trans. Image Process., vol. 22, no. 6, pp. 2181–2191, Jun.* 2013.

إخفاء صورة داخل صورة باستخدام خوارزميات (AES، LSB) المحسنة

الخلاصة

الستيكانوغرافي هو فن لإخفاء المعلومات او البيانات أو تضمينها في وسائط رقمية مختلفة مثل الصور، الفيديو، الصوت والنصوص. وان هناك الكثير من التقنيات لتحقيق عملية الإخفاء. في هذا البحث قمنا بحماية البيانات أو أي معلومات بطريقتين: التشفير والإخفاء. الغرض الأساسي من البحث هي تقديم طريقة تشفير مطورة للرسالة أولا باستخدام خوارزمية (التشفير القياسي المتقدم) AES هو تشفير مفتاح متماثل حيث ان لكل شفرة من الشفرات بحجم كتلة ١٢٨ بت، حيث ان الأحجام الرئيسية هي من ١٢٨، ١٩٢، ٢٥٦ بت. ثانيا نقوم بإخفاء تلك الرسالة المشفرة في الحدود الخارجية للصورة الملونة (الإطار الخارجي للصورة الغلاف) باستخدام دالة LSB (البت الأقل اهمية) في ملفات الصورة الغلاف التي تكون بامتداد (bmp) أو(Jpeg) علما ان الخوارزمية الأخيرة تتسم بالضعف تجاه الهجمات لذلك تم تطويرها وتدعيمها بخوارزمية AES لزيادة الأمن ضد اي هجوم محتمل اثناء ارسالها عبر شبكة الانترنيت من المرسل الى المستلم.

الكلمات الدالة: التشفير، AES، LSB ، إخفاء المعلومات، فك التشفير، العلامة المائية، PSNR، MSE.