A Proposed Method for Encrypting Data In Image by Using Cryptography Technique and Steganography

(Lecturer) Hasan M. Azzawi*

Abstract

Since the rise of the Internet, one of the most important factors of information technology and communication is the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this is called Steganography. In this paper, a combination of cryptography technique and steganography has been proposed. The proposed algorithm encrypts the information before hiding it in image file to increase the complexity of encryption/decryption process. The peak signal-to-noise ratio (PSNR) is obtained 53.5266. The simulation results show the difference between the original image and the stego image will be hardly noticeable to the human eye. The proposed algorithm is implemented in MATLAB (R2013a) program for computer simulations.

Keywords: Data Security, Cryptography, Steganography, least significant bit (LSB), Encryption, Decryption.

*University of Technology/Electrical Eng.Dept.

1.Introduction

On internet the amount of digital images has increased rapidly but security of images becomes increasingly important for many applications, like, confidential transmission, military and medical applications. The security of the transformation of hidden data can be obtained by two ways: cryptography and steganography. A combination of the two techniques can be used to increase the data security. In encryption, the message is changed in such a way so that no data can be disclosed if it is received by an attacker. In steganography, the secret message is embedded into an image (or any media) called cover image, and then sent to the receiver who extracts the secret message from the cover image. After embedding the secret message, the cover image is called a stego-image. This image should not be distinguishable from the cover image, so that the attacker cannot discover any embedded message. There are many techniques for encrypting data, which vary in their security, robustness, performance and so on. Also, there are many ways for embedding a message into another one {1}.

2. Literature Review

2.1 Cryptography

Cryptography is a technique for keeping message secure and free from attacks. Cryptography provides encryption techniques for a secure communication. In cryptography secret message is scrambled. Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Communication security of data can be accomplished by means of standard symmetric key cryptography. Such important data can be treated as binary sequence and the whole data can be encrypted using a cryptosystem. Secret keys are used to encrypt the data into cipher data. Symmetric or Asymmetric keys are used for apply cryptography in data {2}.

2.2 Steganography

Steganography is the other technique for secured communication. Steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. Steganography is the process of hiding a secret message within cover medium such as image, video, text, audio. Image steganography has many applications, especially in today's modern, high-tech world. Privacy and secrecy is a concern for most people on the internet. Image steganography allows for two parties to communicate secretly and covertly {2}.

3. Data Hiding

Data hiding is a method of hiding secret messages into a cover-media such that an unintended observer will not be aware of the existence of the hidden messages. Cover-images with the secret messages embedded in them are called stego-images. For data hiding methods, the image quality refers to the quality of the stego-images. One of the common techniques is based on manipulating the least-significant-bit (LSB) planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity {3}. The basic structure of Steganography based on LSB is made up of three components, as shown in figure (1):

i. The Carrier image,
ii. The Message,
iii. The Key.

The carrier can be a painting, or a digital image. It is the object that will 'carry' the hidden message. A key is used to decode/decipher/discover the hidden message. This can be anything from a password, a pattern, a black-light. LSB insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M's bit. This technique works well for image steganography. To the human eye the stego- image will look identical to the carrier image. For hiding information inside the images, the LSB method is usually used {4}. When using a 24-bit image, one can store 3 bits in each pixel by changing a bit of each of the red, green and blue color components.

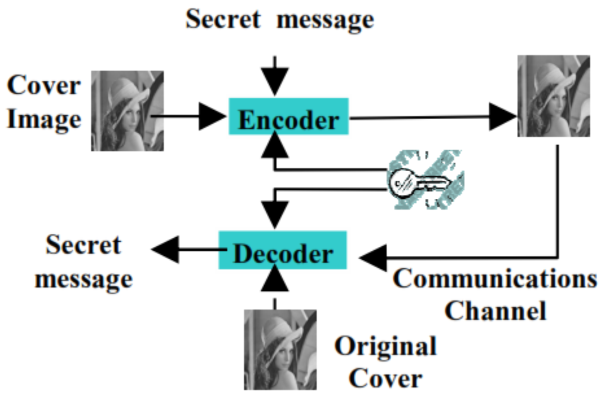


Figure (1): Block diagram of steganography {2}.

The following example shows how the letter Acan be hidden in the first eight bytes of three pixels in a 24-bit image. Consider a 24-bit colour bitmap image where each pixel is stored as a byte representing a RGB value. For example, suppose one can hide a message in three pixels of an image (24-bit colors). Suppose the original 3 pixels, as shown in Table (1):

Table (1): RGB pixel before LSB algorithm

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001

To hide the letter A whose binary value is 01000001, the following new RGB values are shown in table (2). The three underlined bits are the only three bits that were actually altered. LSB insertion requires on average that onlyhalf the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to begin hiding the next character of the hidden message {5}.

Table (2): RGB pixel after LSB algorithm

00100110	**11101001**	**11001000**
00100110	**11001000**	**11101000**
11001000	**00100111**	**11101001**

4. ProposedAlgorithm

4.1 Message Encryption Part

In the first part, encoding hidden messages using encryption algorithm, the following steps are performed, as shown in figure (2):

1- In thispaper, a complex secret key generationalgorithmisproposed. The first two constant keys (X_i and Y_i) are proposed to generate first ciphering key (O_1). These keys are 8-bit secret randomnumbers. The operation of key generationalgorithmisdescribed in Eq. (1 and 2). The third variable key value (Z_i) isused to generatenumber of variable keys. These variable keys are different and it'sfrom (Key_1 to Key_j). Each one of these variable key ismultiplywithciphering key (O_2). The final value (O_3) isthen Exclusive OR (XOR) with the message byte.

$$O_1 = X_i \otimes Y_i \quad (1)$$

$$O_2 = (X_i - O_1) \times (Y_i - O_1) \quad (2)$$

2- The message and dimensions of the message (overalllength for text) form an 8-bit header thatisused to reconstruct the message during the decodingprocess.

3- The header isconcatenated to the beginning of the message and this new combined message isencryptedusing a simple symmetric Exclusive OR (XOR) encryption key (Key).

4.2 Steganography Part

In second part, the procedure of proposed algorithm is shown in figure (3). The least significant bits of some or all of the bytes inside an image are replaced with bits of the secret message. The image is used as a cover to embed the information (Texts or/and Images). This process is done by LSB encoder which replaces the least significant bit of pixel values with the information bits. For each process of steganography part, the following steps are performed:

1- The second part uses the steganographyalgorithmbased on LSB algorithm for embedding the secret message.

2- The LSB algorithm uses anytext documents or images files in which the data iswritten, and the image file as a carrier file in which the secret message or text document or image file to behidden.

3- Eacheight byte of cover or source image isused to beembeddedwith byte of image or text to behidden.

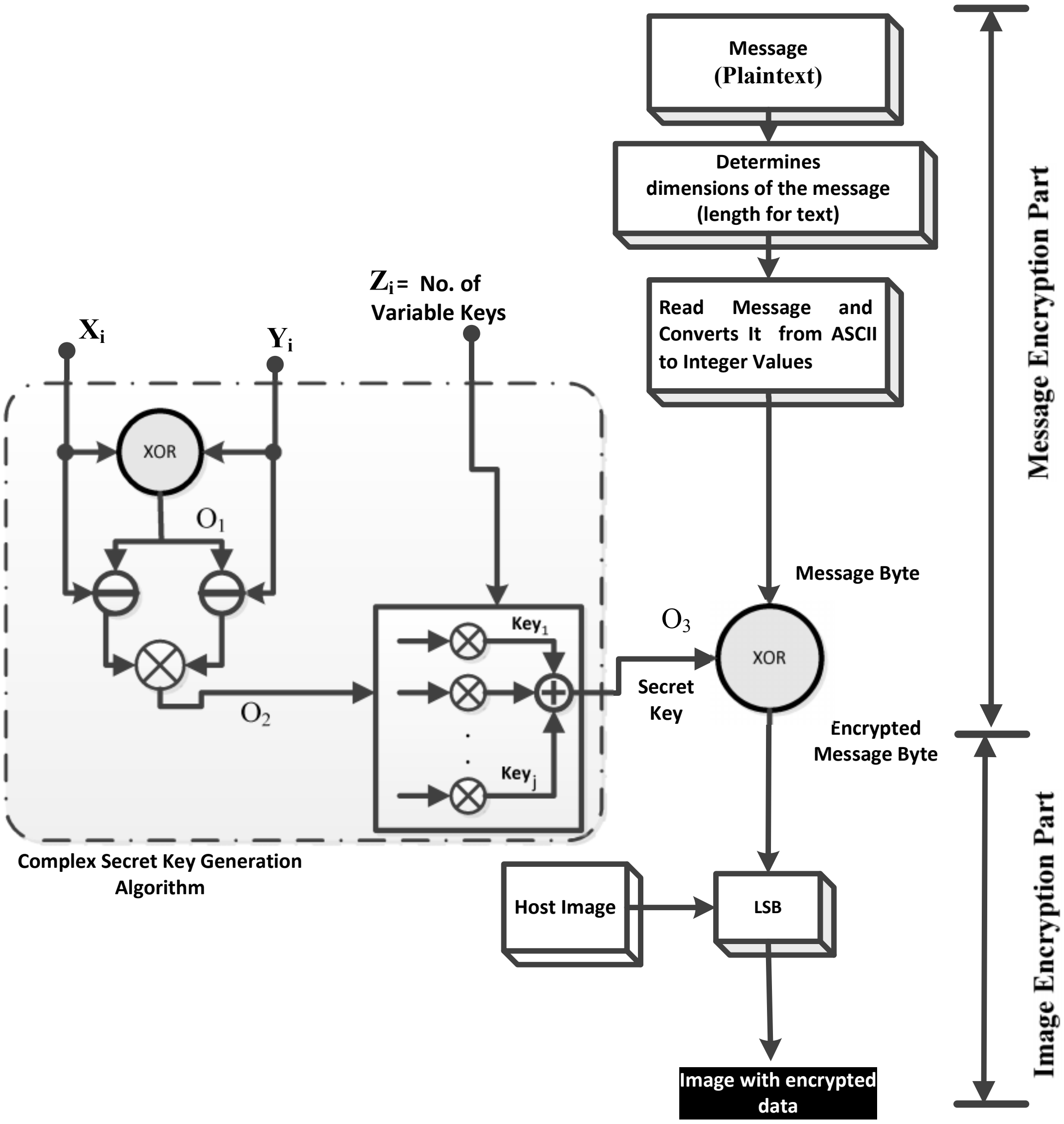

Message
(Plaintext)
Determines dimensions of the message (length for text)
Read Message and Converts It from ASCII to Integer Values
Message Encryption Part
Z_i = No. of Variable Keys
X_i
Y_i
XOR
O_1
O_2
Key_1
Key_j
Secret Key
O_3
XOR
Message Byte
Encrypted Message Byte
Complex Secret Key Generation Algorithm
Host Image
LSB
Image with encrypted data
Image Encryption Part

Figure (2): Proposed algorithm.

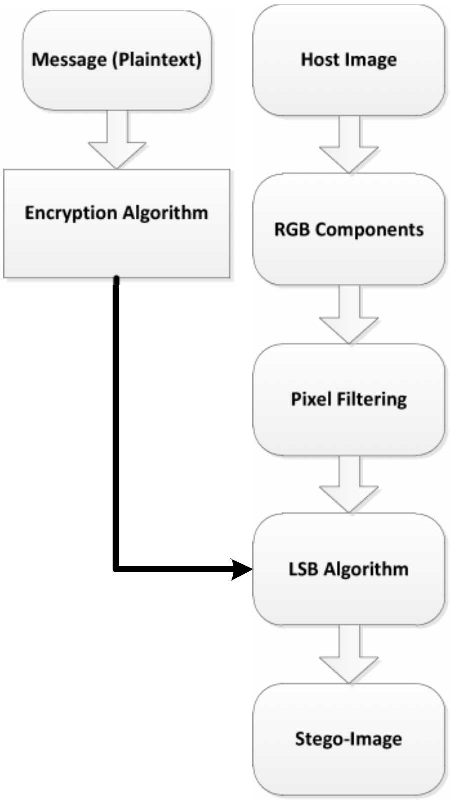


Figure (3):Procedure of Proposed LSB algorithm.

4.3 Decryption Process

The decryption of the encrypted image which was encrypted using the proposed algorithm is done by inverting all the encryption operations with the same keys, the following steps are performed:

1- First, to decrypt a message, use the same of the key bits, and applies the same XOR transformation to the message, bit by bit, as shown in Eq.(3).

$$\text{Plain Image (host image)} = \text{Encrypted Image} \otimes \text{Secret Key} \qquad (3)$$

2- The program recovers the entireencrypted message from the encrypted image by using the header dimensions (length of text message) to determinewhen to stop.
3- The recovered message isdecryptedusing the same XOR encryption key usedduringencoding.
4- Decryptedtext (plaintext) and image (host image) are obtained.

5. Performance Measurements

In steganography, following factor are considered after embedding secret message in the cover medium {6}:

A. Utilization factor

The utilization factor denotes the amount of cover image that has been utilized to embed the secret message into it, and it is given by Eq.(4):

Utilization factor = secret message size (bits)/ host image size (bits) (4)

B. The peak signal-to-noise ratio (PSNR) value

The peak signal-to-noise ratio (PSNR) is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of a logarithmic decibel scale. A higher PSNR value indicates that the reconstruction is of higher quality. PSNR is most commonly used as a measure of quality of reconstruction image. The signal in this case is the original data, and the noise is the error due to hiding. The mean square error (MSE) and PSNR value is calculated by Eq. (5 and 6).

$$MSE = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I(x,y) - I^{t}(x,y)]^{2} \qquad (5)$$

And

PSNR=20*log10(255/sqrt(MSE)) (6)

Where I(x,y) is the original image, I'(x,y) is the approximated version (which is actually the decompressed image) and M,N are the dimensions of the images. MSE and PSNR are the most common methods for measuring the quality of compressed images.

6. Simulation Results

Figure (4) shows general block diagram of the proposed algorithm.For encryption process, the input parameter of the cover image is shown in table (4). The host image (Baboon) is BMP type with 704 kb in size (24bits/pixel), as shown in figure (5a). A BMP is capable of hiding quite a large message. LSB in BMP is most suitable for steganography applications {7}.

Table (4): Input Parameters of the cover image.

Parameter	Input
Image Size	704 KB
Image Type	BMP
D(m*n)	500*500*px*
Text Size	67 KB

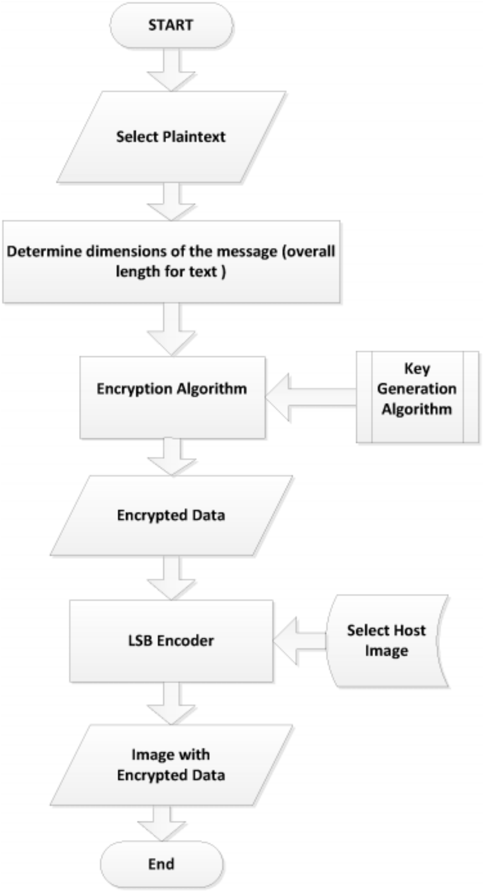
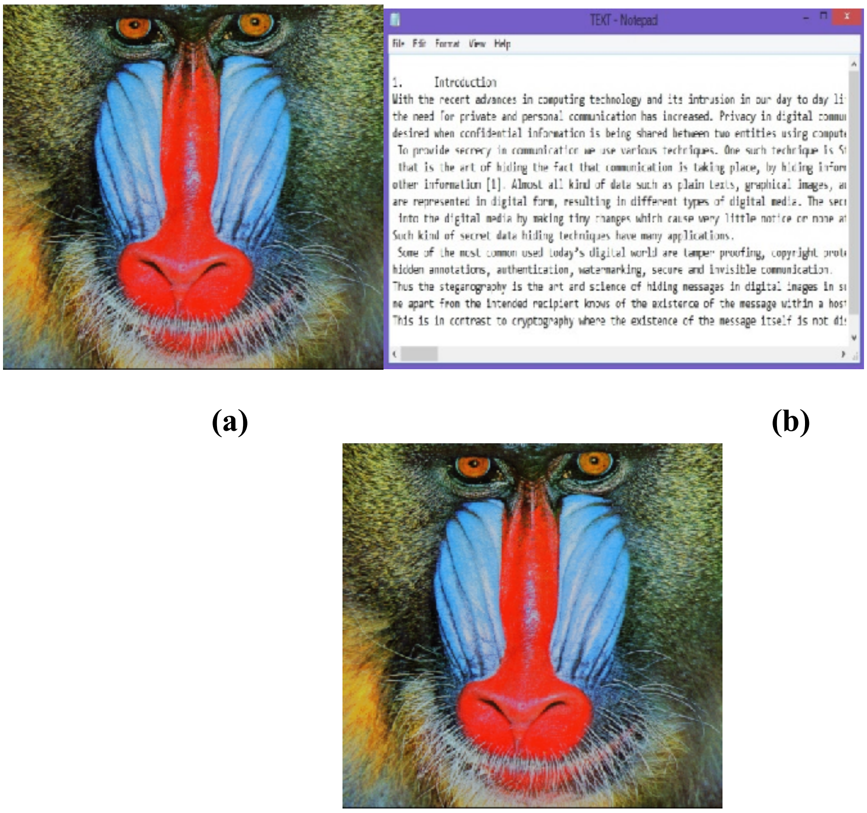


Figure (4): General block diagram of the proposed algorithm.

The text size is 67 kb as shown in figure (5b). The PSNR is obtained 53.5266by using MATLAB program. Figure (5a) and figure (5c) that show a cover image and a stego image (with data is embedded); there is no visible difference between the two images, thereby proving the working of the proposed algorithm at first part. The simulation results show the differencebetweenthe cover (original image) image and the stego image will be hardly noticeable to the human eye. Table (5) shows the results of measurement parameters for encrypted part.



1. Introduction
With the recent advances in computing technology and its intrusion in our day to day li
the need for private and personal communication has increased. Privacy in digital commu
desired when confidential information is being shared between two entities using comput
To provide secrecy in communication we use various techniques. One such technique is St
that is the art of hiding the fact that communication is taking place, by hiding infor
other information [1]. Almost all kind of data such as plain texts, graphical images, a
are represented in digital form, resulting in different types of digital media. The sec
into the digital media by making tiny changes which cause very little notice or none a
Such kind of secret data hiding techniques have many applications.
Some of the most common used today's digital world are tamper proofing, copyright prot
hidden annotations, authentication, watermarking, secure and invisible communication.
Thus the stegarography is the art and science of hiding messages in digital images in s
ne apart from the intended recipient knows of the existence of the message within a hos
This is in contrast to cryptography where the existence of the message itself is not di

(a) (b)

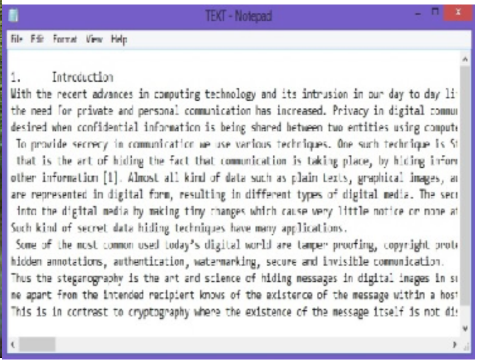
(c)

Figure (5): (a) Baboon host image, (b) Text (6Kb) to behidden, (c) Embedded baboon image withtext.

Table (5): Results of Measurement Parameters

Parameter	Input
PSNR	53.5266 dB
Mean Normalized Cross-Correlation	1.0002
Mean Square Error (MSE)	0.2887
Utilization Factor	0.095

For Decryption process, figure (6a) shows the decrypted image. Figure (6b) shows the decrypted message. The Least significant bit technique by which the encoded bits in the image is decoded and turns to its original state and gives the output as an image. The encryption and decryption is used in order to secure from unauthorized access.



```
1.      Introduction
With the recent advances in computing technology and its intrusion in our day to day li
the need for private and personal communication has increased. Privacy in digital commu
desired when confidential information is being shared between two entities using comput
 To provide secrecy in communication we use various techniques. One such technique is St
 that is the art of hiding the fact that communication is taking place, by hiding infor
other information [1]. Almost all kind of data such as plain texts, graphical images, an
are represented in digital form, resulting in different types of digital media. The sec
 into the digital media by making tiny changes which cause very little notice or none at
Such kind of secret data hiding techniques have many applications.
 Some of the most common used today's digital world are tamper proofing, copyright prot
hidden annotations, authentication, watermarking, secure and invisible communication.
Thus the steganography is the art and science of hiding messages in digital images in s
ne apart from the intended recipient knows of the existence of the message within a host
This is in contrast to cryptography where the existence of the message itself is not di
```

(a) (b)

Figure (6): (a) Decrypted image, (b) Decrypted data.

7. Conclusions

In this paper, a combination of cryptography technique and steganography has been proposed. The proposed algorithm encrypts the information before hiding it in image file to increase the complexity of encryption/decryption process. The algorithm mainly uses 3 keys of size 8-bit to perform encryption and decryption. The achieved result gives more resistance to Brute-force attack and will make it very difficult to decrypt the plaintext without correct values of keys. The proposed algorithm leads to increase the complexity of encryption processand makes the differential and linear cryptanalysis more difficult. The peak signal-to-noise ratio (PSNR) is obtained 53.5266. The simulation results show the difference between the original image and the stego image will be hardly noticeable to the human eye.

References

1. GarimaTomar, “**Effect of Noise on hidden data**”, International Journal of Computer Science & Communication Networks,Vol. 2, No.1, pp. 12-15, 2012.

2. Manoj Kumar Meena, etc. al, “**Image SteganographyToolusing Adaptive EncodingApproach to Maximize Image Hidingcapacity**”, International Journal of Soft Computing and Engineering (IJSCE), Vol.1, No.2, pp.7-11, May 2011.

3. Chi-Kwong Chan, etc. al, “**Hiding Data in Images by Simple LSB Substitution**”, The journal of Pattern Recognition Society, Vol.37, pp.469 – 474, 2004.

4. Shilpa Gupta, etc. al, “**Enhanced Least Significant Bit algorithm For Image Steganography**”,International Journal of Computational Engineering & Management (IJCEM), Vol. 15, No.4, pp.40-42, July 2012.

5. Mamta Juneja, etc. al, “**Application of LSB BasedSteganographic Technique for 8-bit Color Images**”, World Academy of Science, Engineering and Technology, Vol.26, pp.423-425, 2009.

6. Harshitha K M, etc. al, “**Secure Data HidingAlgorithmUsingEncrypted Secret Message** ”, International Journal of Scientific and Research Publications, Vol.2, No.6, pp. 1-4, June 2012.

7. V. LokeswaraReddy ,etc. al, “**Implementation of LSB Steganography and its Evaluation for Various File Formats**”,International Journal of Advanced Networking and Applications, Vol. 2, No. 5, pp. 868-872, 2011.

طريقة مقترحة لتشفيرالبيانات
في صورة باستخدام تقنيةالتشفيرواخفاءالمعلومات

م. حسن محمود عزاوي*

المستخلص

منذ ظهورشبكة الإنترنت ,واحدة من أهم العوامل لتكنولوجيا المعلومات والاتصالات هوأمن المعلومات .تم إنشاءعلم التشفيركتقنية لتأمين سرية الاتصالات والعديد من وسائل مختلفة تم تطويرها لتشفيروفك تشفيرالبيانات من أجل الحفاظ على سرية المعلومات .للأسف أنه في بعض الأحيان لايكفي الحفاظ على محتويات المعلومات سرا , قد يكون من الضروري الحفاظ على وجود المعلومات سرا أيضا.ويطلق على التقنية المستخدمة لتنفيذ هذا بعلم الاخفاء .في هذا البحث ,تم اقتراح دمج تقنية التشفيروإخفاءالمعلومات . الخوارزمية المقترحة تشفرالمعلومات قبل إخفائها في ملف الصورة وذلك يؤدي الى زيادة عملية تعقيد التشفير / فك التشفير .تم الحصول على اعلى نسبة الإشارة إلى الضوضاء بمقدار(53.5266)على التوالي .أظهرت نتائج المحاكاة ان الفرق بين الصورة الأصلية والصورة (stego)ستكون بالكاد ملحوظ اللعين البشرية .تم تنفيذ خوارزمية التشفيرالمقترحة في برنامج (MATLAB (R2013aلمحاكاة الحاسوب.

* الجامعة التكنولوجية/ قسم الهندسة الكهربائية