Improvement Data Security Using LSB, DCT and RSA Based on Image Steganography

Noora H.Sherif
AL-Turath University Collage

Abstract

Speedy development of telecommunication makes transactions message even easier and faster. The main problem in the transmitting and receiving message is security, especially if the message is private and secret. Steganography is designed to conceal the appearance message by hiding the secret message inside an innocent folder. For efficient security, steganography is mixed with cryptography. In this paper, steganography and cryptography are mixed to supply a strong system capable of enciphering a secret image using LSB, DCT and RSA algorithm. This method consists of two parts: firstly, embedding stage and secondly is extraction stage. The enciphering picture can be concealing in some another image using LSB, DCT so that the secret's message occurs using RSA algorithm. Conceal encrypted image in the cover image by DCT is called embedding stage. Extract encrypted image from cover image by DCT and decrypt text by RSA is called extraction stage**.** The quality of image has been calculated like PSNR (Peak Signal to Noise Ratio), and MSE (mean square error) using MATLAB R2015a. In this method obtains higher values of PSNR and lower values of MSE for images.

Keyword: LSB (Least Significant Bit), RSA algorithm, DCT (Discrete Cosine Transform), steganography, cryptography PSNR, MSE.

الخلاصة

لقد جعل التطور السريع للاتصالات إرسال الرسائل أسهل وأسرع. إن المشكلة الأساسية في إرسال الرسائل واستلامها هي الأمان، خصوصا إذا كانت الرسالة خاصة وسرية. علم الاخفاء هو إخفاء رسائل المعلومات عن طريق إخفاء الرسائل السرية في المجلدات من أجل الحصول على أمان فعال.

في هذا البحث، يتم الجمع بين تقنية إخفاء المعلومات والتشفير لتكوين نظامًا قويًا حيث يستخدم خوارزمياتLSB و DCTو RSAلتشفير الصور المصنفة. تتكون الطريقة من جزأين: الجزء الأول هو مرحلة التضمين، والجزء الثاني هو مرحلة الاستخراج. نستخدم LSB و DCTلإخفاء صورة المشفرة في صورة أخرى ولتشفير الرسالة السرية باستخدام خوارزمية.RSA

إن إخفاء الصورة المشفرة في صورة الغلاف بواسطة DCT يسمى مرحلة التضمين. اما استخراج الصورة المشفرة من صورة الغلاف بواسطة DCTوفك تشفير النص بواسطة RSA بمرحلة الاستخراج. في هذا البحث تم حساب جودة الصورة مثل اعلى مقدار للإشارة إلى نسبة الضوضاء ومتوسط الخطأ التربيعي باستخدام برنامج الماتلاب و تم الحصول على قيم أعلى لأعلى مقدار للإشارة إلى نسبة الضوضاء وقيم أقل لـمتوسط الخطأ التربيعي للصور.

1-Introduction

Since the growth of the internet one of the most important elements of information technology and communication has been the security of information. Cryptography was made as a technique for securing the privacy of communication and many different ways have been developed to encrypt and decrypt data in order to maintain the message secret. Alas it is sometimes not enough to maintain the contents of a message secret, it may also be

requirement to maintain the existence of the message secret. The mechanism used to implement this, is called steganography [1].

Steganography is the fine art and science of invisible communication. This is done through hiding information in other information, hence hiding the existence of the communicated information [2].

In this paper new mechanisms have been introduced recently for data encryption using RSA algorithm. The idea is to implement RSA public key cryptography- steganography on image encryption/ decryption [3].

2- Least Significant Bit (LSB)

The Least Significant Bit (LSB) is one of the important methods in spatial domain image steganography. LSB is the base huge piece inside the byte estimation of an image pixel. The LSB based image steganography installs the transformation name in minimum great predictable bits of pixels' parataxis of the blanket image [4]. It trades on the truth that the level of accuracy in a lot of image formats is a prolonged way greater than that perceivable through average human inspired and prescient. So, an altered image with moderate formats in hints may be cloudy from the interesting through an individual, just by taking a looking at it. LSB approach only four bytes of pixels are sufficient to hold one message byte. staying bits in the pixel left over's the equal [5].

3- RSA Algorithm

The RSA algorithm is a public key cryptosystem that offering both encryption and authentication. Its denotation stands for the 1st letters of its creators' names Rivest, Shamir and Adleman [6].

The suggested approach is using to create two prime to create public and private key. Both keys are applied for encryption and decryption objective [7].

There are three stages are as follows-

1- Key generation, 2- Encryption, 3- Decryption

•Key generation:

- Choose two different prime numbers T and U
- Determine n=T*U
  - Determine ph=(T-1) (U-1)
  - Choose an integer e such that 1<e<ph and GCD (e, ph) =1; e and ph are co- prime.
  - Select a number relatively prime to ph and call it F.
  - Find F such that e*F=1mod ph
  - Public key is (n, e)
  - Private key is (n, F)

•Encryption

Cipher text(C), $C= M^e \bmod n$

• Decryption

Plain text (M), $M= C^F \bmod n$

3-Discrete Cosine Transform (DCT)

DCT in digital image processing is commonly done by splitting the images into small pieces or sub-block with standard size 8x8 pixels .The results of transformation of 8x8 pixel sub-blocks will create 64 coefficients which comprised of a DC coefficient and 63 AC coefficients. Equation 1 is indicated to DCT where input images, A, DCT coefficients for image output, B. In these equations, the input image having I * J pixels, C (i, j) is the

intensity of the pixel in rows m and columns n of the image, and T (p, q) is the DCT coefficient in row u and column v of the DCT array [8].

$$T_{pq} = \alpha_p \alpha_q \sum_{i=0}^{I-1} \sum_{j=0}^{J-1} C \cos\frac{\pi(2i+1)p}{2I} \cos\frac{\pi(2j+1)q}{2J} \quad \text{.....1}$$

To rebuild the image after DCT process according to Eq.2

$$C_{ij} = \sum_{i=0}^{I-1} \sum_{j=0}^{J-1} \alpha_p \alpha_q T_{pq} \cos\frac{\pi(2i+1)p}{2I} \cos\frac{\pi(2j+1)q}{2J} \quad \text{.....2}$$

4- Suggested Work

The aim of suggested scheme is to get more secure and robust method of information exchange so that confidential and private data must be saved against attacks and illegal access. To attain the required robustness and security, cryptography and steganography is mixed as shown in figure1. Image is taken as a cover medium for steganography and RSA algorithm is applied for encryption.

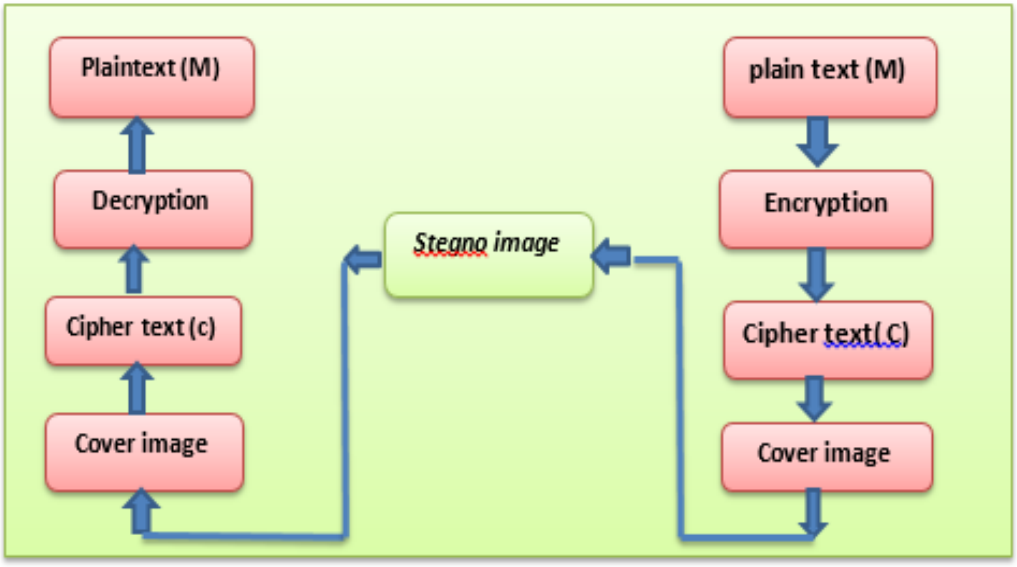

Fig.1: Mixed of Steganography and Cryptography

4.1: Suggested Methodology

The suggested scheme has been implemented in the MATLAB R2015a for the utilize of steganography set of preferred cryptography. The Figure.2 is the suggested system architecture of this work. There are many steps are followed, so that the whole algorithm is subdivided into subsections.

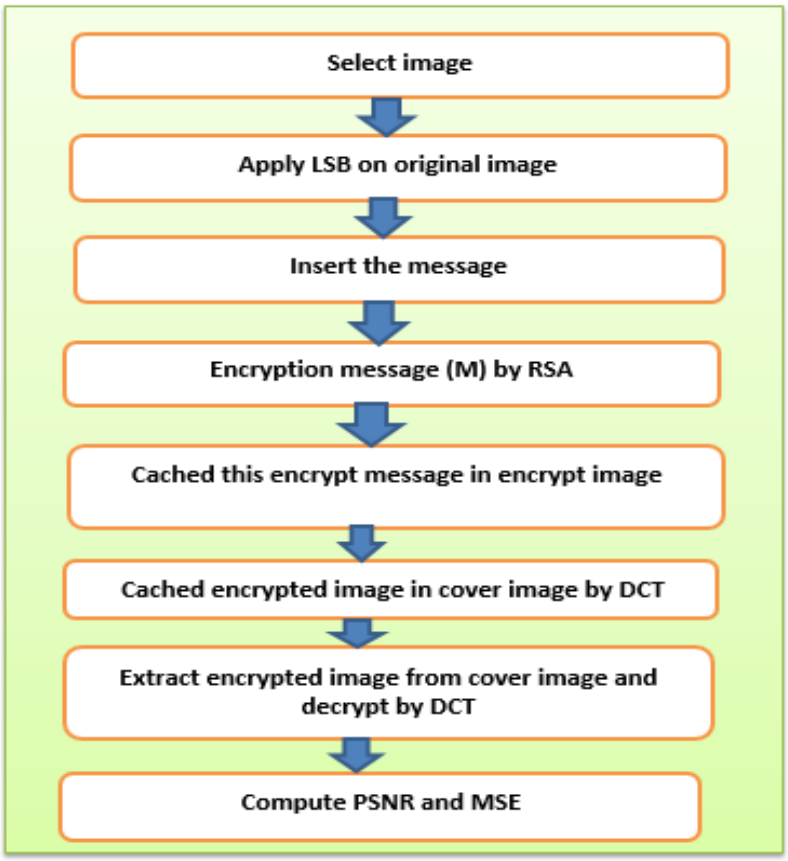

Fig.2: Flow chart of the work.

At the first, choose the cover image from database in the computer then converted to grayscale image (512*512 pixels the size of images). each pixel of image is converted to the binary value and the data is caching in the least significant position of the binary value of pixel of the image using LSB.

In the encryption operation, encrypted text using RSA algorithm. This algorithm used two different keys. One is public key which everyone knowing it used in encryption operation. Second is private key which kept private from everyone used for decryption operation.

At the receiver employed private key to perform RSA algorithm which is the secret text recipient is encrypted by public key. Private key used to convert the cipher text into original text. In decryption operation used hash function to discover the position of LSB and DCT where the data bits had been hidden. the position of the bits had been indicated, the bits are extracted from the position in the same series as they were hidden. Cached the encrypted image in the image transformed by DCT. extracted the encrypted image from cover image and decrypt the text by DCT.

MSE (mean square error) is used to estimate the error between the cover image and stegno-image. PSNR (peak signal to noise ratio) is used to estimate the highest noise which the signal affords.

Compute MSE and PSNR value by the following equations

$$\mathbf{MSE}=\frac{1}{MN}\sum_{I=0}^{M-1}\sum_{J=0}^{N-1}[I(i,j)-K(i,j)]^2 \quad \text{..... 3}$$

$$\mathbf{PSNR=20.log_{10}}\left[\frac{MAX_I}{\sqrt{MSE}}\right] \quad \text{..... 4}$$

5-Result

The result analysis and simulations using Matlab R 2015a.In the beginning browse the image from database. The selected image is transformed into the grayscale image is shown in Figure 3. the cover image for the steganography operation.

Fig.3: The cover image for the steganography operation.

After choosing the cover image, the LSB is applied on the cover image. This is the original image which is embedded later to the stegno.image with DCT mechanism.
The plain text (M) inserted by user, the plain text (M) transformed to the cipher text(C) using RSA algorithm is shown in figure 4.

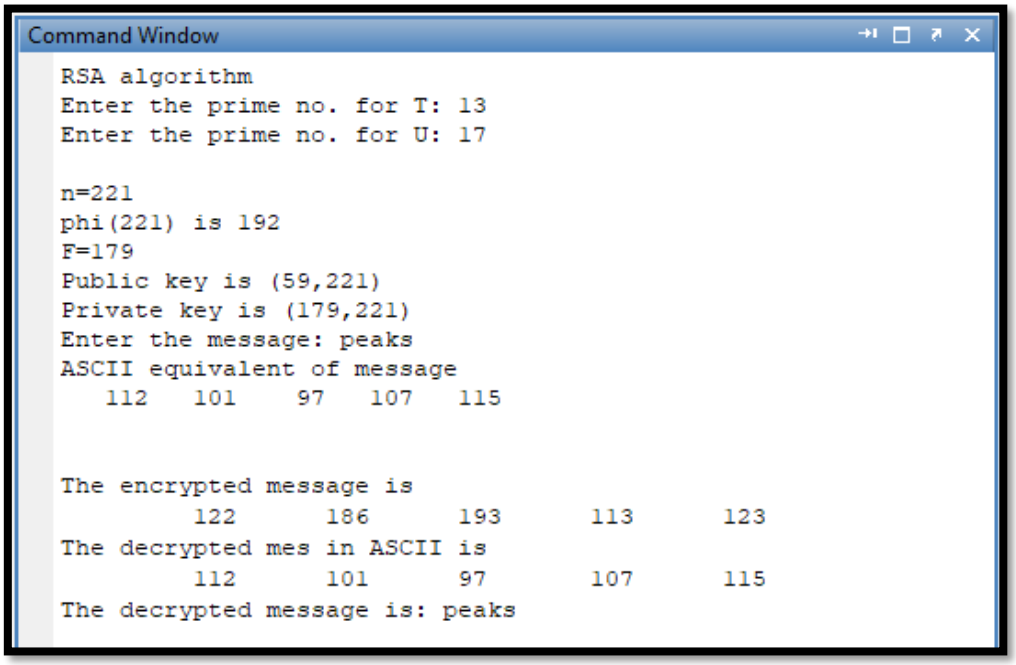

Fig. 4: RSA algorithm.

The cipher text is hidden behind the encrypted image. Applying RSA algorithm has made our mechanism more secure for unlock channel. Figure (5) shows the stegno.image .

Fig.5: the stegno.image.

The stegno.image embedded into the original image. This image is transported into the communication channel from transmitter to receiver which conceals the encrypted image in which the message is hidden. In the decoding, the LSB extraction operation is applied to get the message bits. When the orientation of the bits had been specified, the bits are extracted from the orientation in the same order as they were embedded. Extract encipher image from cover image by DCT and decrypt text by RSA algorithm with receiver's private key. Figure (6) shows the extracted image.

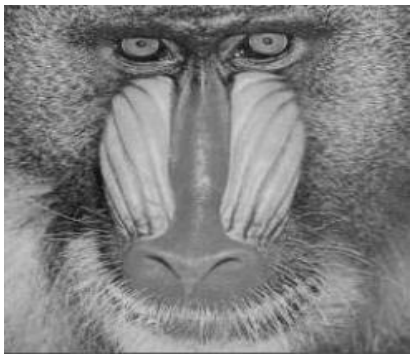

Fig.6: the extracted image.

Compute MSE and PSNR the cover image and stegno.image. The better results, high value of PSNR and low value of MSE. These values are computed for some related images and shown below in table 1.

Table (1): suggested and Existing Technique for MSE and PSNR

Name of image	MSE Before suggested Technique	MSE After Suggested Technique	PSNR(dB) Before suggested Technique	PSNR(dB) After Suggested Technique
Babbon.BMP	**1.7160**	**1.2051**	**66.86**	**73.2243**
LENA.JPG	**1.7150**	**1.2042**	**66.90**	**73.2146**
PEARS.PNG	**1.6933**	**1.1990**	**66.95**	**73.8332**
PEPPERS.BMP	**1.7186**	**1.2051**	**66.84**	**73.1132**

6- Conclusion

In this paper suggest a LSB and DCT-steganography based on encryption. To give higher security steganography and cryptography are mixed together.

The power of LSB-RSA and DCT hybrid increased the range of security in the suggested approach where the symmetric key cryptography algorithm is applied for encryption in the existing technique. It can be very hard to use the attack of brute force in this technique because RSA can be used for LSB and DCT, as the improvement in existing technique, the suggested method gets higher values of PSNR and lower values of MSE for images to achieve the better result and the stegno.images of our suggested algorithm are almost identical to the cover images.

7-References

[1]-T. Morkel, J.H.P. Eloff, M.S. Olivier**,"** An overview of Image Steganography" proceedings of the fifth annual information security south Africa conference, June/July 2005.

[2]- Pooja Rani, Mrs. Preeti Sharma," Cryptography Using Image Steganography", IJCSMC, Vol. 5, , July 2016, p.451 – 456.

[3]- Sura F. Yousif," Encryption and Decryption of Audio Signal Based on RSA Algorithn", International Journal of Engineering Technologies and Management Research, Vol.5, Issue. 7,July 2018.

[4]- Shahana T, "A Secure DCT Image Steganography based on Public-Key Cryptography", International Journal of Computer Trends and Technology– vol.4 , Issue 7–July 2013.

[5]- Swati Bhargava and Manish Mukhija," Hide Image and Text Using LSB, DWT and RSA Based on Image Steganography", ictact journal on image and video processing, , volume: 09, issue: 03, february 2019.

[6]- Abari Ovye John, P.B.Shola, Simon Philip," Comparative Analysis of Discrete Logarithm and RSA algorithm in Data Cryptography", International Journal of Computer Science and Information Security, Vol. 13, No. 2, 2015.

[7]- Dharitri Talukdar, Lakshmi Prasad Saikia," Simulation and Analysis of Modified RSA Cryptographic Algorithm using Five Prime Numbers", International Journal on Recent and Innovation Trends in Computing and Communication, Volume: 5 Issue: 6, June 2017.

[8]- De Rosal Ignatius Moses Setiadi , Eko Hari Rachmawanto, Christy Atika Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption", Journal of Applied Intelligent System, Vol. 2 No. 1, April 2017, pp. 1-11.