Hiding Secret Text in Image Using RC2 and Serpent Algorithm

Asst. Teach. ISRAA S.AHMED

(Computer Department, Informatics Institute for Postgraduate Studies

(IIPS)/ Iraqi Commission for Computers and Informatics(ICCI),

Baghdad, Iraq, zita_18122003@yahoo.com)

Abstract

In the current work, an effective scheme was adopted for hiding cipher text in image file. The proposed method was to hide the cipher text message in frequency domain of image. The proposed method contained two stages: the first embedding phase and the second extraction phase. In embedding phase the image transformed from time domain to frequency domain using discrete wavelet decomposition technique (Haar). The text message encrypted using RC2 and Serpent algorithm; then used Least Significant Bit (LSB) algorithm used to hide secret message in high frequency. The proposed method tested in different images and showed the success of hiding according to (PSNR) equation.

Keywords: - Steganography in image, Secret message, RC2 algorithm, Serpent algorithm, LSB algorithm, Wavelet transform.

أخفاء نص مشفر في صورة بأستخدام خوارزمية RC2 and Serpent

الخلاصة

في هذا البحث جرى عرض طريقة لأخفاء البيانات السرية في صورة .الطريقة المقترحة هي اخفاء رسالة نصية مشفرة في صورة في المجال الترددي. تضمنت الطريقة المقترحة مرحلتين هما: مرحلة الاخفاء ومرحلة فك الاخفاء او الاستخلاص. في مرحلة الاخفاء تم تحويل الصورة من المجال الزمني الى المجال الترددي باستخدام تحويل الموجة من النوع البسيط ذات المستوى الواحد ثم نختار القيم ذات الترددات العالية لاخفاء الرسالة فيه. الرسالة النصية تم تشفيرها باستخدام خوارزميتين هما .(RC2 and Serpent) من ثم اخفاء الرسالة النصية المشفرة في قيم الترددات العالية للصورة باستخدام خوارزمية (البت الاقل الاهمية). الطريقة المقترحة اختبرت صور مختلفة واظهرت نجاحها في اخفاء واعادة الرسالة النصية وباستخدام معادلة نسبة الضوضاء للصور الاصلية .

الكلمات المفتاحية:- الاخفاء في الصورة، رسالة مشفرة، خوارزمية RC2, خوارزمية Serpent, خوارزمية البت الاقل اهمية، التحويل المويجي.

1. Introduction

Steganography; means unseen writing, is used for transmitting a message by a carrier signal, to a receiver but without allowing intruders to know its presence or uncover its content. The carrier is often a digital image that usually doesn't bring any notice and ought to be very close to the genuine image by naked eyes. In steganography, one ore many bits of

the bytes of pixels; making up the image (carrier) are altered. Least Significant Bit, LSB, can be employed to cipher message bits and revealed by the receiver and saved as bytes to reconstruct the embedded message. This can be materialized when the password of the stego-image is known. Steganalysis is a technique of revealing a message and uncover its embedded contents by a third party. It is utilized to investigate the security and success of transmitted messages [1].

Steganography and Cryptography differ in the way they hide information. Cryptography jumbles the message contents. When intercepted, the message cannot be decoded. Steganography un-noticeably employs the carrier to embed the message and form a stego-image. Successful stego-image cannot be distinguished and seen from the novel carrier.

In steganography, images are used as carrier media [2]: firstly, the message is coded, and then hid for sending to a graphic file and producing a stego-image [3]. Stego-key is also required to hide the process of sending the stego-image to the receiver, who takes out the content of the message from the carrier image. The extraction of the message can only be made possible if both the sender and the receiver share the same secret key; an algorithm or stego-key [4].

2. Wavelet Analysis

Wavelet transforms (WT) implies segmenting a signal into many versions of scaled and shifted wavelets. Each wavelet is a limited time-length waveform of zero average value. The identity of the signal is expressed by a low-frequency signal.

The removal of high frequency component from human voice will yield different but understandable voice. Contrarily, the removal of low frequency component will give unclear signal that sounds like gibberish talking.

The application of wavelet transformations on the audio signal will give detailed audio signal. Approximating the solution will represent the low-frequency signal of and the details will be the high-frequency signal. Due to their low energy level, the detail coefficients of the first level are not very important when compared with next level detail coefficients.

Figure (1) illustrates the disintegration of audio signal on wavelet transform [5].

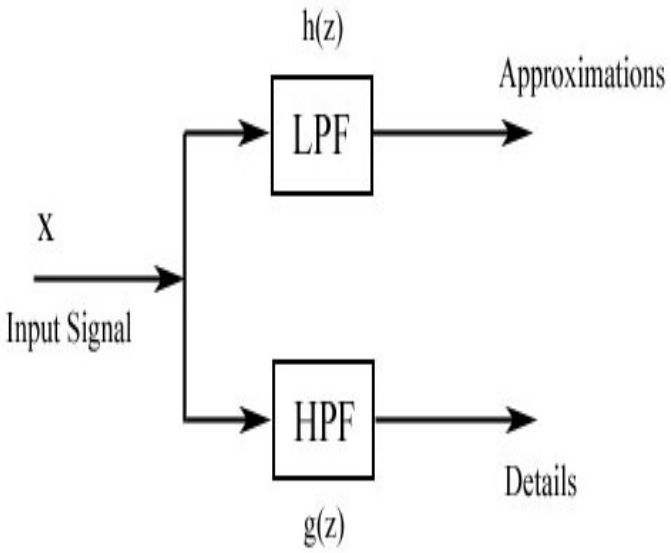
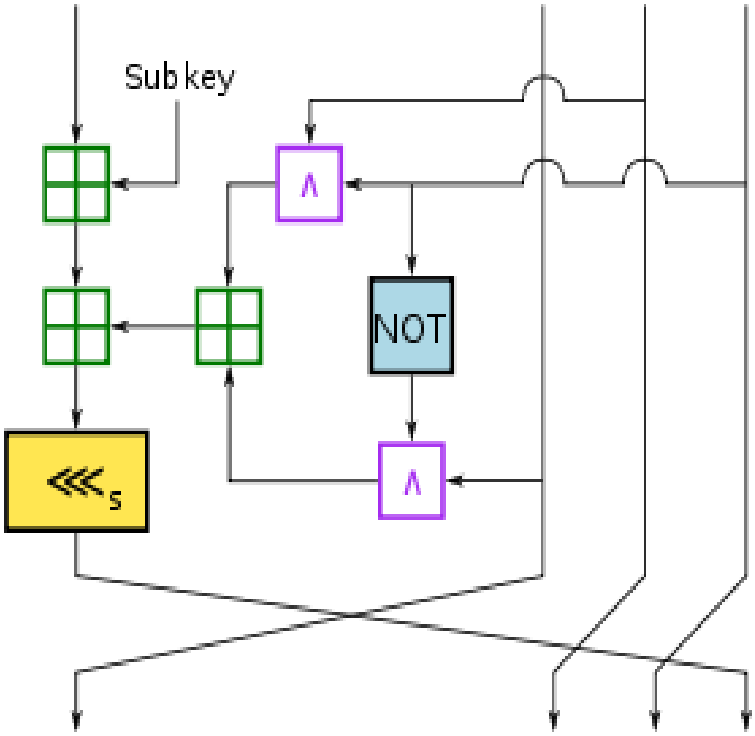


Figure (1) Signal Decomposition

3. RC2 Algorithm

RC2 is a block cipher designed as a simple and fast algorithm. The algorithm's most significant characteristic is its small key length: 40 bits. RC2 could support key sizes from 8 to 128 bits [6]. It functions on 64-bit blocks which split into 4 words of each 16 bits. This is frequently repeated block code in which the cipher text is worked out; a number of times, with respect to the original text and the secret key. RC2 contains 16 mixing and 2 mashing rounds. As a function of other words, there is an updated intermediate cipher text in each round of the four 16-bit words. Each mixing round has sixteen-bit sub key. These sixty four sub keys are selected from 1-128 bytes keys by the user [7].



4. Serpent Algorithm

Serpent is a symmetric 128 bits key block cipher; suggested by Ross Anderson et al in order to execute all operations in parallel, using 32 1-bit slices [8]. It operates with many key size combinations; such as 128, 192 or 256 bits.

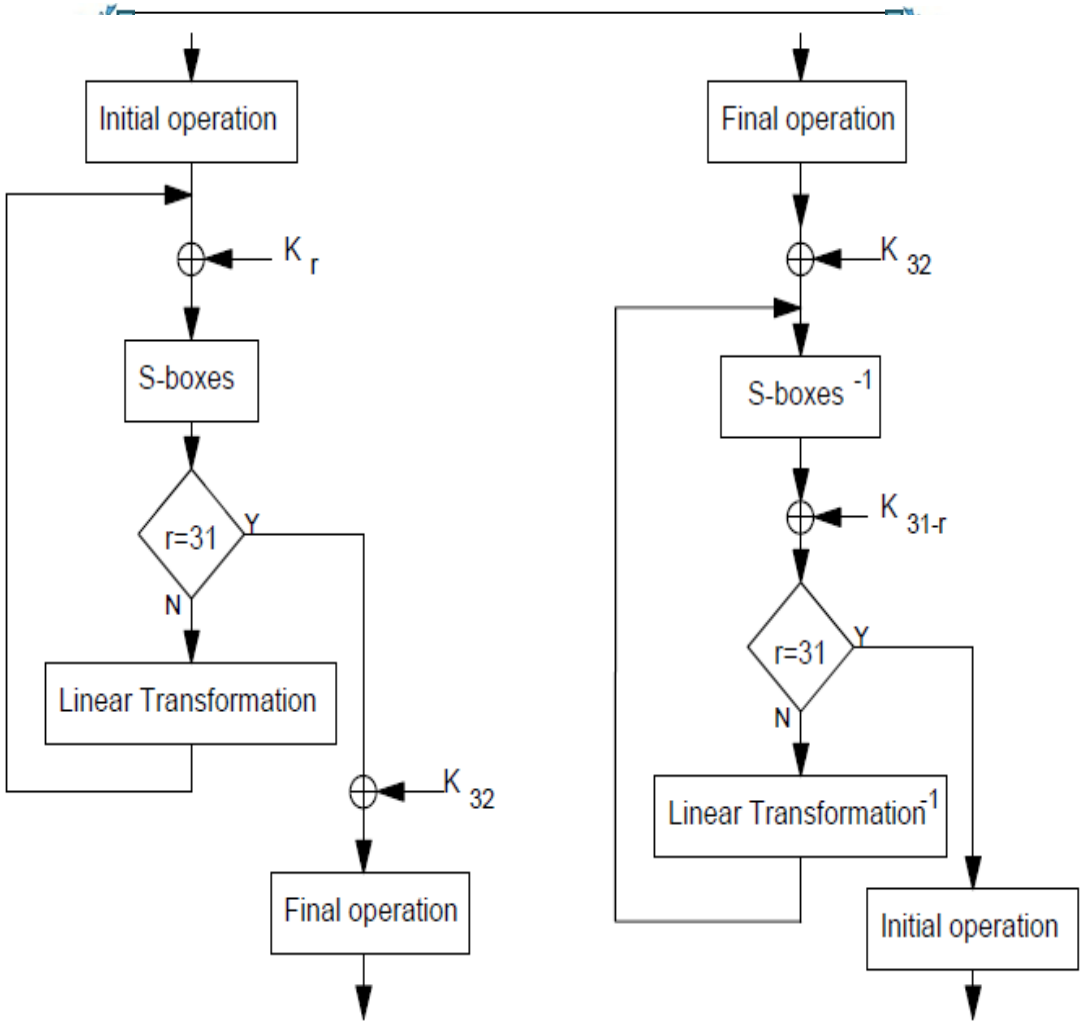


Figure (3) Encryption and Decryption of Serpent Algorithm

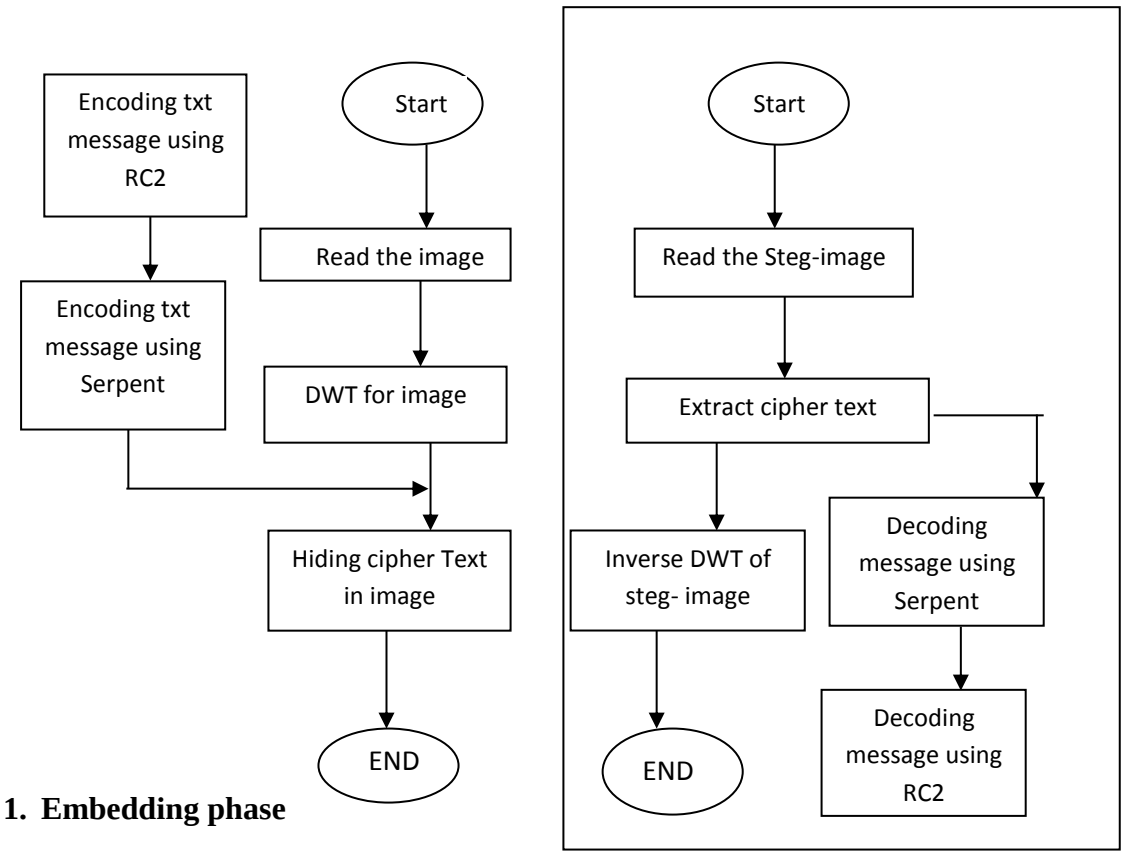
of ciphered text and 128 bit coding key. Each of the 32 Serpent rounds requires one 128 bit sub key to the EXOR with the text block. The 32 sub keys are created by a key generation algorithm [9].

5. The Proposed System

In this paper, propose a method for hiding secret text message in image. The text encrypted by using RC2 algorithm and cipher text also encrypted in Serpent algorithm, then embedding it in frequency domain by taking DWT for color image by using Haar transform for DWT. The cover image

(color image) is decomposed into four sub-band (LL, LH, HL, HH) using DWT. Then hiding the secret message in image using Least Significant Bit (LSB).

This method contains two phases, the embedding and extraction, as shown in figure (4).



1. Embedding phase

Figure (4) the proposed method

1-Embedding Phase

The embedding phase contains: applied DWT on image to transform image from spatial domain to frequency domain using Haar transformation, encrypt text message will be hidden in image by RC2 and

Serpent methods. The secret message converted into ASCII code for hiding secret message in the high frequency coefficient of image by using the LSB (Least Significant Bit) algorithm.

2- Extraction Phase

The Extraction Phase contains: Extract the cipher text form stego-image, decrypt the hidden message by decryption of Serpent algorithm then decryption of RC2 algorithm. Then take the inverse of wavelet transform for stego-image to return to the original image.

6. Implementation and Results

The proposed method was used different images. Peak Signal to noise ratio (PSNR) of the stego cover images objects was used for calculating the noise, as shown in equation (1,2,3)[10].

The word want be hidden is "hello world" while the key is "computer". The word after encrypted by RC2 algorithm becomes:-

"ej1FmolceCMuEUcmQFax4g==".

While in hexadecimal:- "7a3d459a895c78232e1147264056b1e2".

Then encrypted this cipher text using Serpent algorithm then become: -

"YyqiSgniR1ljD7ZYolsoIguOhKCyWbir8GR0Kb346rA=".

While in hexadecimal :-
"632aa24a09e24759630fb658a25b28220b8e84a0b259b8abf0647429bdf8eab0"

The resulted images; obtained from the present work was compared with the original images by using PSNR, it can be seen that the steganographed image is not distinguishable from the original. As shown in Table (1).

PSNR = $10 \log_{10}(s^2/MSE)$ …… (1)
Where:

$$s^2=\frac{1}{m*n}\sum_{i=1}^{m}\sum_{i=1}^{n}J^2(i,j) \quad \ldots\ldots\ldots (2)$$

And the Mean Square Error (MSE) defined as:

$$MSE=\frac{1}{m*n}\sum_{i=1}^{m}\sum_{i=1}^{n}[J(i,j)-j^1(i,j)]^2 \quad \ldots\ldots\ldots (3)$$

Where j^1 represents the pixel in the stego image (the result of the steganography system).

Table (1) the result of implementation

Image name	The image	PSNR value	Steg-image
A1		71.4893	
A2		74.7388	

A3		72.8481	

7. Conclusion

In this paper, we introduce technique for hiding secret text message in image using discrete wavelet transform. DWT is applied on color images. We use multilayer security by using two encryption methods. The Encryption and Decryption techniques for two encryption algorithms are RC2 and Serpent algorithms. The evaluation of the proposed method shows good performance that cannot distinguish between the stego-image and original image.

REFERENCES

[1]- K. Curran, L. Xuelong, R. Clarke, 2005, "An Investigation into the use of the least Significant Bit Substitution Technique in digital Watermarking", International Technologies Research Group, University of Ulster, magee Campus, Northland Road, Northern Ireland, UK, American Journal of Applied Science 2(3), pp: 648-654.

[2]- E. Cole, "Hiding in Plain Sigt", John W. Wiley, ISBN:0-471-44449-9, 2003.

[3]- A. Wstfield, and Pfitzmann, "Attacks on Steganographic System", Third International Workshop, IH'99 Dresden Germany, October Proceedings, Computer Science, 1768:61-76, 1999.

[4]- J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, Wicke and G. Wolf, "Modeling the Security of Steganographic System", Information Hiding, 2nd International

Workshop, IH'98 Portland, Oregon, USA, Computer Science,1525: 344-254,1998.

[5]- Michael Weeks, "Digital Signal Processing Using MATLAB and Wavelets", Pearson publications, ISBN – 81-297-0272-X 2(13) :15-16, 2011.

[6]- Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, "Security in Computing", ISBN 978-0-13-408504-3, fifth edition, 2016.

[7]- National Institute of Standards and Technology. Advanced encryption algorithm (AES) development effort. http://www.nist.gov/aes.

[8]- Murat Çakiro_lu, "Software implementation and performance comparison of popular block ciphers on 8-bit low-cost microcontroller", International Journal of the Physical Sciences Vol. 5(9), pp. 1338-1343, 18 August, 2010.

[9]- R. Anderson, E. Biham, L. Knudsen , "SEPRENT A Proposal for the Advanced EncryptionStandard", http://csrc.nist.gov/encryption/aes/round2/AESAlgs/Serpent/Serpent.pdf.

[10]- Lee K. and Chen H., "A High Capacity Image Steganographic Model", in IEEE Proceedings on Vision Image and Signal Processing, China, pp.288-294,2000