

Ciphered Text Hiding in an Image using RSA algorithm

Amer A. Al-Lehiebe

amerallehiebe@yahoo.com

University of Baghdad - College of Education for Women - Computer Science Dept.

Abstract

In this paper, a method for hiding cipher text in an image file is introduced. The proposed method is to hide the cipher text message in the frequency domain of the image. This method contained two phases: the first is embedding phase and the second is extraction phase. In the embedding phase the image is transformed from time domain to frequency domain using discrete wavelet decomposition technique (Haar). The text message encrypted using RSA algorithm; then Least Significant Bit (LSB) algorithm used to hide secret message in high frequency. The proposed method is tested in different images and showed success in hiding information according to the Peak Signal to Noise Ratio (PSNR) measure of the the original image.

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

أخفاء نص مشفر في صورة باستخدام خوارزمية RSA

عامر عبد الهبيبي

جامعة بغداد - كلية التربية للبنات - قسم الحاسبات

الخلاصة

في هذا البحث جرى عرض طريقة لأخفاء بيانات مشفرة في صورة. الطريقة المقترحة هي إخفاء رسالة نصية مشفرة في صورة في المجال الترددي. تضمنت الطريقة المقترحة مرحلتين هما: مرحلة الإخفاء ومرحلة فك الإخفاء أو الاستخلاص. في مرحلة الإخفاء حولت الصورة من المجال الزمني الى المجال الترددي باستخدام تحويل المويجة من النوع البسيط ذو المستوى الواحد. الرسالة النصية شُفرت باستخدام خوارزمية (RSA). من ثم إخفاء الرسالة النصية المشفرة في قيم الترددات العالية للصورة باستخدام خوارزمية (التثنائية الأقل الاهمية). الطريقة المقترحة اختبرت في صور مختلفة واطهرت نجاحها في إخفاء المعلومات وباستخدام مقياس نسبة الضوضاء للصور الاصلية وال (PSNR).

الكلمات المفتاحية: - الإخفاء في الصورة, رسالة مشفرة, خوارزمية RSA, خوارزمية البت الأقل اهمية, التحويل المويجي.

1. Introduction

Steganography is derived from the Greek word Stegano which means Covered or Secret, and Graphy means written or drawn. The objective of steganography is to send a message through some media known as a carrier, to a receiver, while preventing anyone else from knowing that the message exists. The carrier can be one of many different digital media, but the most common is the image. The image should not attract any attention as a carrier of a message and should compare as close as possible to the original image by the human eye. When images are used as the carrier in steganography, they are generally manipulated by altering one or more bits of the byte that make up the pixels of the image. The (Least Significant Bit, LSB) may be used to encode the bits of the message. These LSB's can then be read by the recipient of the stego-image and put together as bytes to reproduce the hidden message, providing they have the stego key – the password for the stego-image. Steganalysis

is the art of discovering a message. Breaking a steganography has been used, reading the embedded to third parties. Steganalysis methods are also used by the steganographer to determine whether the message is secure and whether the process has been successful [1].

Steganography is used for transmitting data in a media such as image. Cryptography and steganography are different in their methods of hiding information. Cryptography scrambles a message and hides it in a carrier, so that if it is intercepted it would be generally impossible to decode. Steganography hides the very existence of the message in the carrier. When the message is hidden in the carrier a stego-carrier is formed e.g. a stego-image. If successful, it would be perceived to be as close to the original carrier or cover image by the human eye. Images are the most widespread carrier medium [2]. They are used for steganography in the following way: The message may firstly be encrypted. The sender embeds the secret message to be sent into a graphic file [3]. This results in production of what is called the stego-image. Additional secret data may be needed in hiding process e.g. a stego key. The stego-image is then transmitted to the recipient. The recipient or extractor extracts the message from the carrier image. The message can only be extracted if there is a shared secret between the sender and the recipient. This could be the algorithm for extraction or a special parameter such as a key (the stego-key) [4].

2. Wavelet Analysis

The wavelet transform (WT) has gained widespread acceptance in signal processing and image compression. Wavelet transform is the breaking up of a signal into shifted and scaled versions of the original (or mother) wavelet. A wavelet is a waveform of effectively limited duration that has an average value of zero. For signals; identity of the signal is given by the low-frequency component. The high-frequency content only imparts save our or nuance. In human voice, if high frequency components are removed, the voice sounds different, but still it can be understood. If low frequency components are removed, signal sounds gabble. On applying wavelet transformations on audio signal, approximation and detail components of audio can be obtained. The approximations are low-frequency components of the signal and details are high-frequency components. The first level detail coefficients have less importance in comparison with detail coefficients of next levels and approximation coefficients because of their low energy level. Figure (1) shows the decomposition of audio signal on wavelet transform [5].

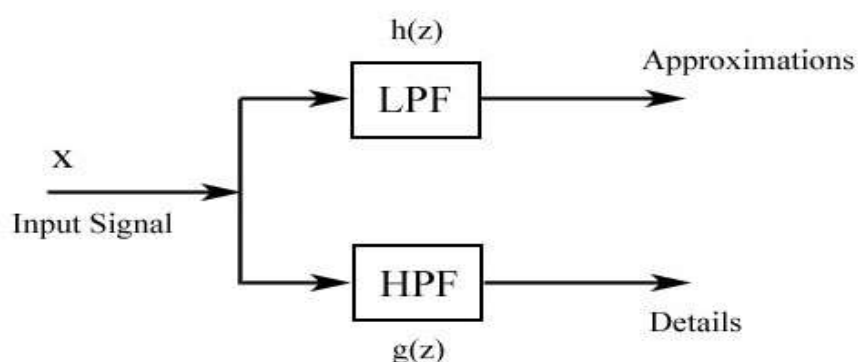


Figure (1) Signal Decomposition

3. RSA Algorithm

RSA is widely used in encrypted connection, digital signatures and digital certificates core algorithms. Public key algorithm invented in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman (RSA)[6]. It is the main operation of RSA to compute modular exponentiation. Since RSA is based on arithmetic modulo large numbers, it can be slow in constraining environments [7].

Especially, when RSA decrypts the cipher text and generates the signatures, more computation capacity and time will be required. Reducing modulus in modular exponentiation is a technique to speed up the RSA decryption. The security of RSA comes from integer factorization problem. RSA algorithm is relatively easy to understand and implement RSA algorithm is based on the theory of a special kind of reversible arithmetic for modular and exponent RSA is used in security protocols such as TLS/SSL and many more applications [8][6].

The public and private keys are functions of a pair of large prime numbers and the necessary activities required to decrypt a message from cipher text to plaintext using a public key is comparable to factoring the product of two prime numbers[8].

3.1. RSA Steps

Key generation:-

- Select random prime numbers p and q , and check $p \neq q$.
- Compute modulus $n=p*q$.
- Compute ϕ , $\phi=(p-1)(q-1)$.
- Select public exponent e , $1 < e < \phi$ such that $\gcd(e, \phi)=1$.
- Compute private exponent, $(d*e) \bmod \phi=1$.
- Public key is $\{n, e\}$, private key $\{d\}$.

Encryption:-

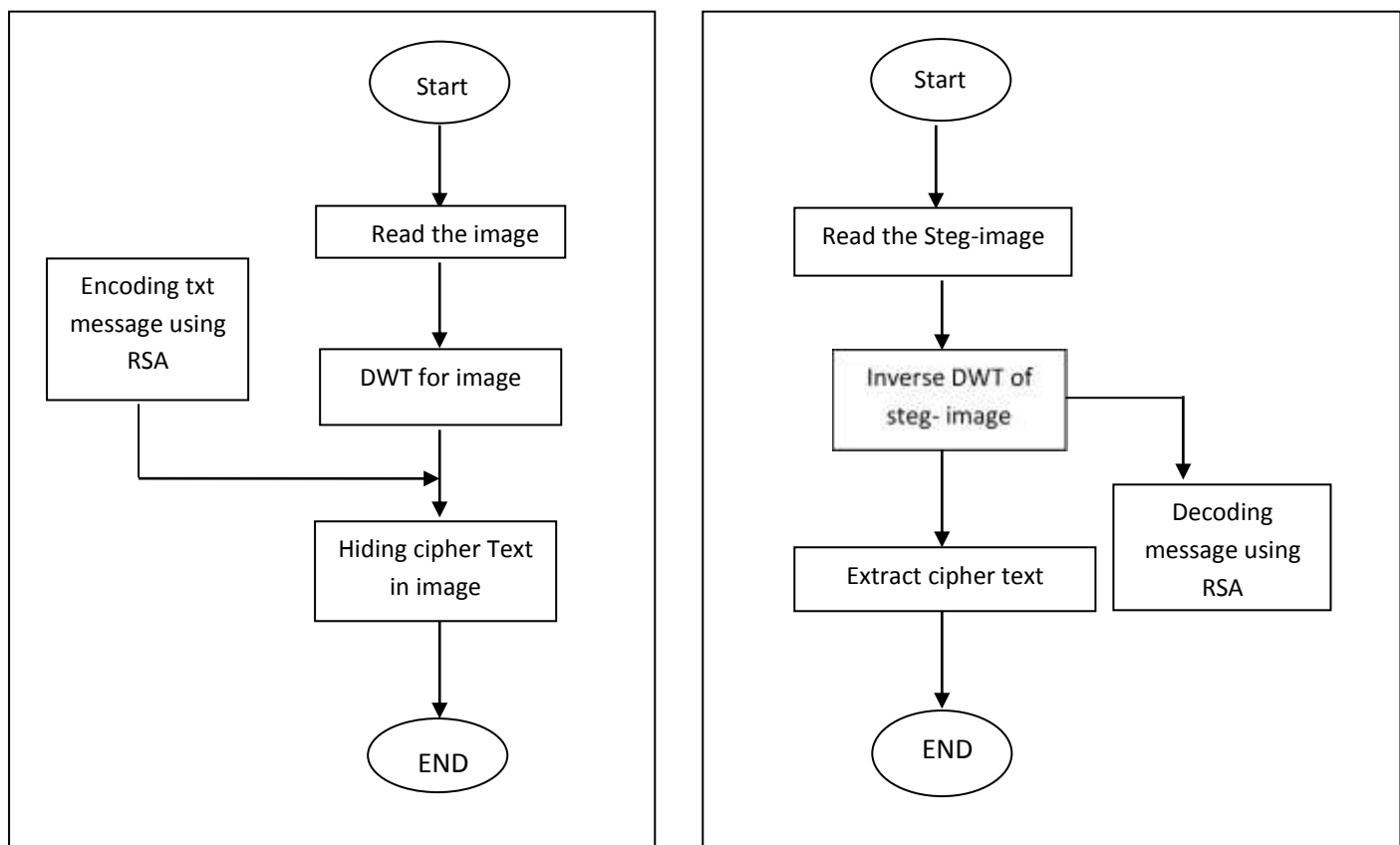
$$c = (m^e) \bmod n.$$

Decryption[9] :-

$$m = (c^d) \bmod n.$$

4. The Proposed System

In the proposed method, the text encrypted by using RSA then embedding it in frequency domain taking discrete wavelet transform (DWT) for color image 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).



(a) Fig (4) the proposed method

(b)

- a- Embedding Phase
- b- Extraction Phase

4-1- Embedding Phase

The embedding phase contains: applied DWT on image to transfer image from spatial domain to frequency domain using Haar transformation, text message will be encrypted by RSA method. 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.

4-2-- Extraction Phase

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

5. 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 equations (1,2 and 3)[10].

For example, the word want to be hidden is "hello" while the key is generated randomly by generate the two primes number randomly; the length of key is 256 bit. The word after encryption became "IYgVivQPTMh6YXDhUYHc7nSWYUD8MxFLUjCiLudGkTyOPNaN0X9qnJLuwMSd7JSxgQHkH U2XXKqJXNW5qzFJ7w==".

The resulting images obtained from the proposed method were compared to 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).

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

Where:







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

And the Mean Square Error (MSE) defined as:

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

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

Table (1) Result of Implementation

Image name	The image	PSNR value	Steg-image
Lana1		74.189	
S1		82.7144	
MM1		73.871	

6. Conclusion

In this paper, we introduced a technique for hiding secret text message in a transform image using discrete wavelet . DWT is applied on color images, We use compound security by using two methods. Results have been tested by PSNR, three achieved values for images (74.189 , 82.7144 and 73.871) are pointed to high similarity between the pair of tested images . Greater resem between the images implies smaller RMSE and, as a result, larger PSNR. Tpical PSNR values over 40 db mean the human eye cannot distinguish the difference between images. Asasuming pixel values in the range[0,255][11].

Reference

- [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 Sight", John W. Wiley, ISBN:0-471-44449-9, 2003.
- [3]- A. Westfield, 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]- R.L. Rivest, A. Shamir and L. Adleman, "A Method of obtaining Digital Signatures and Public Key Cryptosystems", Communication of the ACM, 21: 2, pp. 120-126, 1978.
- [7]- Qing LIU, Yunfei LI, Tong LI, "The Research of the Batch RSA Decryption Performance", Lin HAO, Journal of Computational Information Systems 7:3 (2011) 948-955.
- [8]- Xin Zhou, Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", IEEE, 6th International Forum on Strategic Technology, pp. 1118 – 1121, 2010.
- [9]- Shikha, Kuchhal. Ishank, "Data Security Using RSA Algorithm in Matlab", International Journal of Innovative research and development, 2:7, 2013.
- [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.
- [11] Salomon ,David,"Data compression the complete reference", Fourth Edition,sipringer,2007.