Three Levels of Protection by using Cryptography and Steganography

Firas Sabah Salih Al-Turaihi
College of Information Technology, Babylon University
firassabahalturaihi@yahoo.in

Abstract

The proposed research provide a new idea to protect the data as the data protection currently is necessary in all fields that use the world wide web as knownforLife is in need to use networks, internet and especially password to enter the private sites social media sites and transactions electronic banking. The idea of research, is based on three levels of protection, first is to encrypt the text and then convert the text to binary system and choose the image for of hiding the text within images, this represents the second level of protection. It is assumes that the image containing the text image of secrecy and selecting second image represents the cover and then using LSB method for the purpose of hiding the image which containing in the ciphertext and this is the third level of protection.
Keywords: Hide text, text encryption, data protection, electronic banking transactions

الخلاصة

يقدم البحث المقترح فكرة جديدة لحماية البيانات حيث ان حماية البيانات في الوقت الحالي تعتبر من الاشياء الضرورية في كل المجالات التي تستخدم الشبكة العالمية وكما نعرف ففي الوقت الحاضر لا يوجد اي تعامل في الحياة لايستخدم شبكات الانترنت وخصوصا كلمة السر الخاصة بالدخول للمواقع الخاصة ومواقع التواصل الاجتماعي والمعاملات المصرفية الالكترونية. فكرة البحث تعتمد ثلاث مستويات من الحماية الاول هو تشفير النص ومن ثم تحويل النص الى النظام الثائي واختيار صورة لغرض اخفاء النص داخل الصور وهذا يمثل المستوى الثاني من الحماية، يتم افتراض الصورة الحاوية على النص صورة السرية ويتم اختيار صورة ثانية تمثل الغطاء ومن ثم يتم استخدام طريقة LSB لغرض اخفاء الصورة الحاوية على النص المشفر وهذا هو المستوى الثالث للحماية.
الكلمات المفتاحية: إخفاء النص، تشفير النص، حماية البيانات، معاملات مصرفية الكترونية، LSB

Introduction

The security of information has become a fundamental issue,besides cryptography, and steganography, it can be employed to secure information. Steganography is a technique of hiding information in digital media. In contrast to cryptography, the message or encrypted message is embedded in a digital host before passing it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach of information hiding can be extended to copyright protection for digital media: audio, video, and images. The growing possibilities of modern communications need the special means of security especially on computer network. The network security has become more important as the number of data being exchanged via the Internet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorized access and use. This has resulted in an explosive growth of the field of information hiding. In addition, the rapid growth of publishing and broadcasting technology also require an alternative solution in hiding information. The copyright such as audio, video and other source available in digital form may lead to large-scale unauthorized copying. This is because the digital formats make possible to provide high image quality even under multi-copying. Therefore, the special part of invisible information is fixed in every image that could not be easily extracted without specialized technique saving image quality simultaneously [Provos, 2001].It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting *stego-image* can be transmitted without revealing

that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique and detect the message from the *stego-object*, he would still require the cryptographic decoding key to decipher the encrypted message [Cachin,1998].

Overview Steganography

The word steganography comes from the Greek *Steganos*, which mean covered or secret and *–graphy*mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected and a communication is happening [Johnson, Jajodia, 1998; Popa, 1998]. A secret information is encoding in a manner such that the very existence of the information is concealed. Paired with existing communication methods, steganography can be used to carry out hidden exchanges. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [Johnson and Jajodia, 1998]. It is not to keep others from knowing the hidden information only, but also to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed [Provos and Honeyman, 2001]. The basic model of steganography consists of *carrier*, *message* and *password*. Carrier is also known as *cover-object*, which the message is embedded and served to hide the presence of the message. Basically, the model for steganography is the message is the data that the sender wishes to remain it confidential. It can be plain text, ciphertext, other image, or anything that can be embedded in a bit stream such as a copyright mark, a covert communication, or a serial number. Password is known as *stego-key*, which ensures that only recipient who know the corresponding decoding key will be able to extract the message from a *cover-object*. The *cover-object* with the secretly embedded message is then called the *stego-object*.steganography techniques that embed hidden messages in multimedia objects have been proposed [Johnson & Jajodia, 1998]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are included as below [Johnson and Jajodia,1998]:

(i) Least significant bit insertion (LSB)
(ii) Masking and filtering
(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Overview Cryptography

Basically, the purpose of cryptography is to provide secret communication. Cryptography hides the contents of a secret message from a malicious people. In cryptography, the structure of a message is scrambled to make it meaningless and unintelligible unless the decryption key is available. It makes no attempt to disguise or hide the encoded message. Basically, cryptography offers the ability of transmitting information between persons in a way that prevents a third party from reading it.

Cryptography can also provide authentication for verifying the identity of someone or something.In cryptography, the system is broken when the attacker can read the secret message.

PSNR (Peak Signal-to-Noise Ratio)

The quality of the stego images have been measured using PSNR (Peak Signal-to-Noise Ratio). PSNR is a standard measurement used in steganography technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have. If the cover image is C of size M × M and the stego image is S of size N × N, then each cover image C and stego image S will have pixel value (x, y) from 0 to M-1 and 0 to N-1 respectively. The PSNR is then calculated as follows:

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right) \qquad (1)$$

wher

$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - S(x,y))^2$$

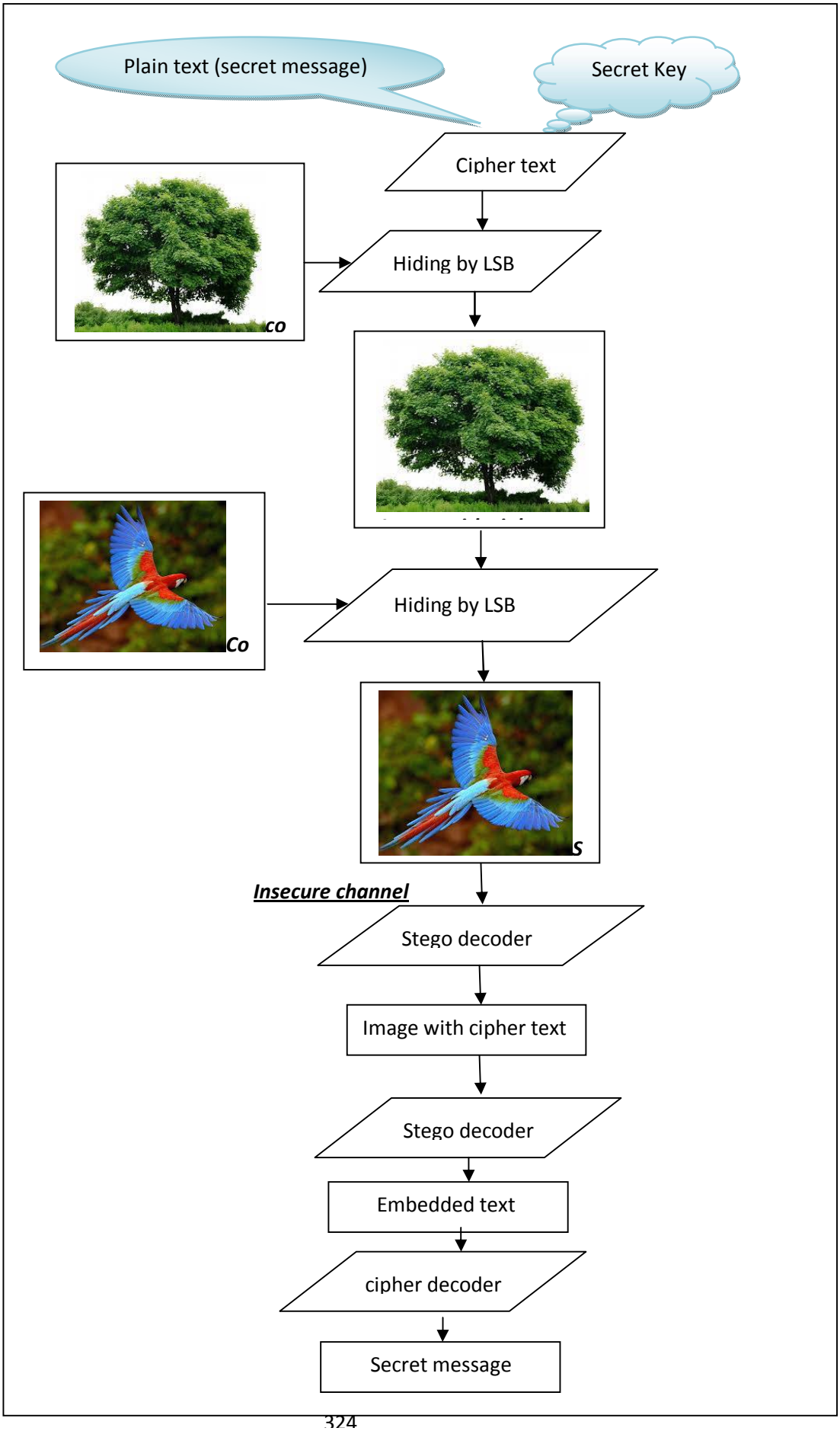

Figure (1) proposed algorithm

Encryption Process:

- In this step we save the entered plain text in a text file (using files instead of arrays to save space) .
- Encrypting the plaintext by using substitution cipher with this equation : cipher = (k1+(index of letter *k2)) mod 26 , where k1,k2 are keys with values k1 =5, k2 =3.
- Saving the cipher text in a text file and convert it to stream of bits.
- Creating text file with random stream bits for using it to another encrypt (by using**xor** between this random file and the cipher text file).

Decryption Process:

In this process we decrypt the cipher text to get the plain text , get the letters from the last text file and making xor operation with the random stream and then use the following equation to obtain the original text:
plain = (k2 inv * (letter index - k1)) Mod 26,where k2 inv=9,k1 =5.

Hiding Process:

Hiding the encrypted text in cover image is below

- Taking one byte from cipher text and cover it into binary system.
- Taking one pixel from image file (RGB).
- Hiding the first two bits in the R band of image file by using the (AND gate and OR gate).
- Hiding the second three bits in the G band of image file by using the (AND gate and OR gate).
- Hiding the last three bits in the G band of image file by using the (AND gate and OR gate).

Experimental Results

In this section the experimental results of the proposal research, it is contain two steps.
Step 1:showing the hiding cipher text size in several images and the PSNR,
table (1) shows the experimental result of hid cipher text in cover image

Image Name	Plan Text Size	PSNR
I1	11 KB	72.5598
I2	16KB	65.7825
I3	3KB	95.1758
I4	20KB	52.6333
I4	30KB	50.9897

Step2: hiding image that contain the cipher text in cover image, the histogram of original image and stego image and the PSNR are showing below:

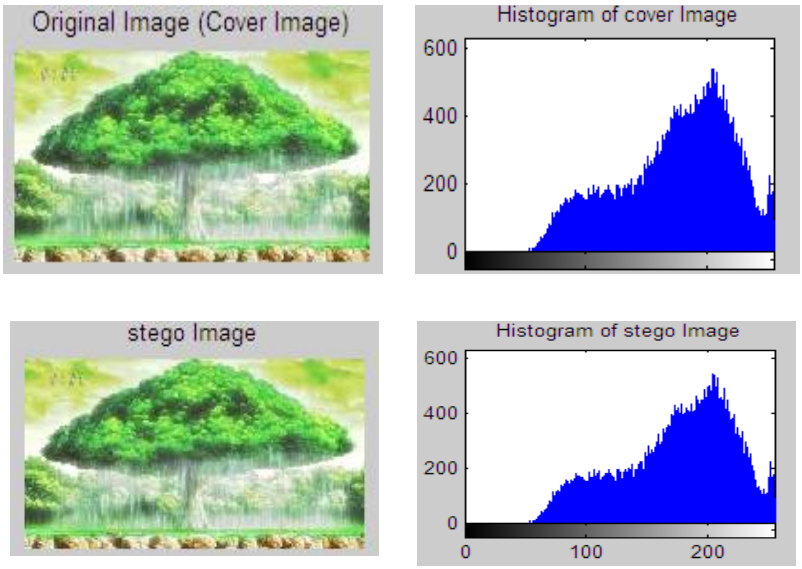

Figure (2) shows the original image and it histogram, stego image and its histogram , PNSR=43.7969

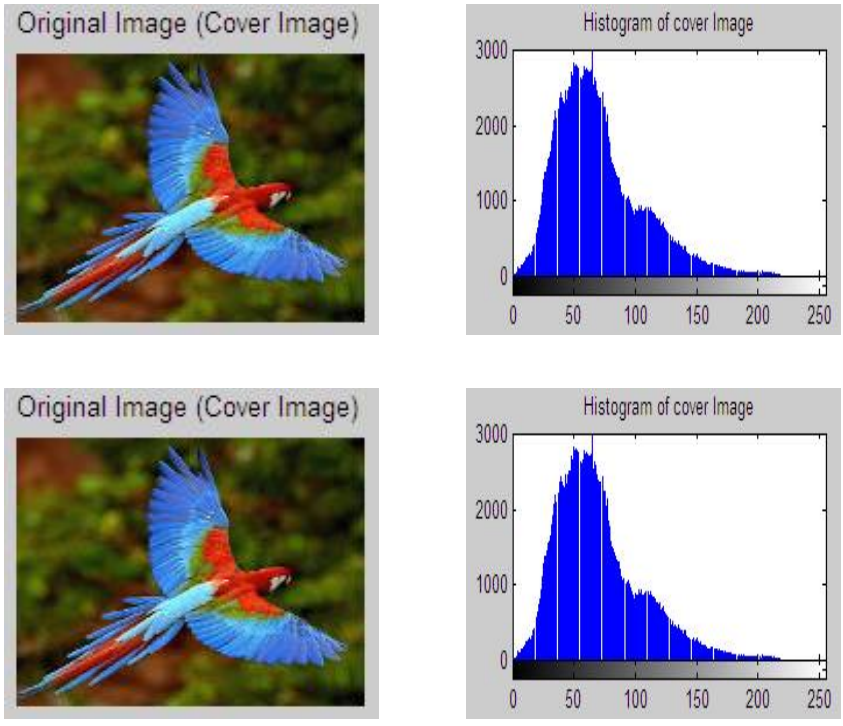

Figure (3) show the original image and it histogram, stego image and its histogram , PNSR= 44.2707

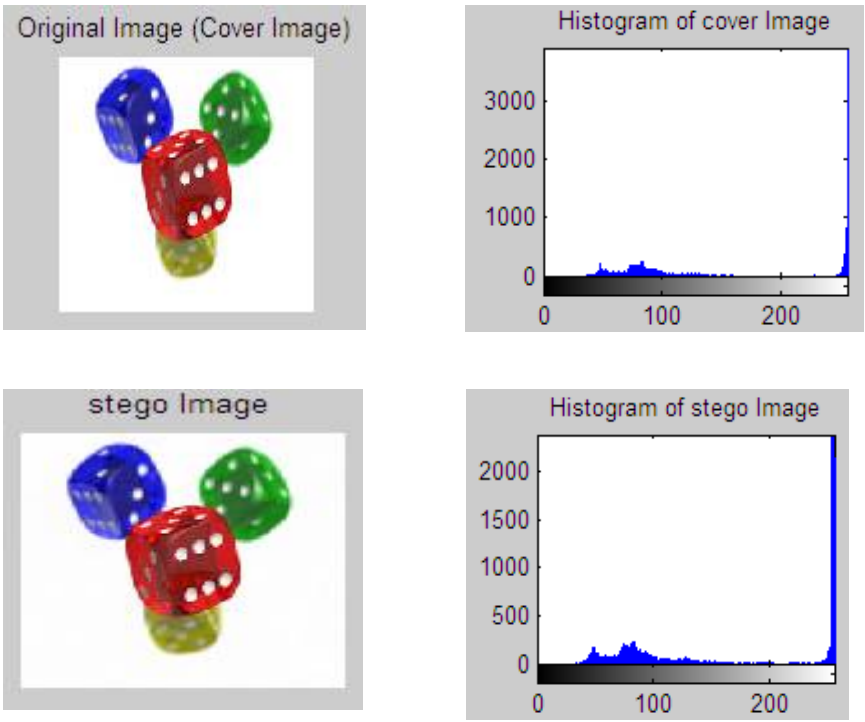

Figure (4) show the original image and it histogram, stego image and its histogram , PNSR= 44.2461

Conclusion

The proposal research provide three levels of safety for the secret message which protect the secret information and data that have been sent from sender to receiver, also this research show the using of steganography techniques based on security algorithm by using techniques for encrypting and hiding data.

The measurements used in this research such as histogram and PSNR show the efficiency of the proposed system.

References

Amin, M.M.; M. Salleh, S. Ibrahim, *et al.,* "Information Hiding Using Steganography", *4th National Conference On Telecommunication Technology Proceedings (NCTT2003),* Shah Alam, Malaysia, pp. 21-25, January 14-15, 2003.

Anderson, R.J. ; F.A.P. Petitcolas, "On The Limits of Steganography", *IEEE Journal of Selected Area in Communications*, pp. 474-481, May 1998.

Cachin, C. "An Information-Theoretic Model for Steganography", in *proceeding 2nd Information Hiding Workshop*, vol. 1525, pp. 306-318, 1998.

Isbell, R A "Steganography: Hidden Menace or Hidden Saviour", *Steganography White Paper*, 10 May 2002.

Johnson N.F. & S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", in *Proceeding for the Second Information Hiding Workshop*, Portland Oregon, USA, April 1998, pp. 273-289.

Johnson N.F. and S. Jajodia, "Exploring Steganography: Seeing the Unseen", *IEEE*, pp. 26-34, 1998.

Johnson, N.F. ; S. Jajodia, "Staganalysis: The Investigation of Hiding Information", *IEEE*, pp. 113-116, 1998.

Peticolas, F.A.P ; R.J. Anderson and M.G. Kuhn, "Information Hiding – A Survey", in *proceeding of IEEE*, pp. 1062-1078, July 1999.

Popa, R."An Analysis of Steganographic

Provos, N. "Probabilistic Methods for Improving Information Hiding", *CITI Technical Report 01-1*, January 31, 2001.

Provos, N. ; P. Honeyman, "Detecting Steganography Content on the Internet". CITI Technical Report 01-11, 2001.

Ramkumar M. & A.N. Akansu. "Some Design Issues For Robust Data hiding Systems", *http://citeseer.nj.nec.com/404009.html*

Siridevi,R. Damodaram, A. &Narasingham, S.,2009. Efficient Method of AudioSteganography by Modified Lsb Algorithm and Strong Encryption Key with EnhancedSecurity.Journal of theoretical and applied information technology,5(2), pp.25-31

System", The "Politehnica" University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering, May 25, 1998.