Research Article Impact Factor: 0.621 ISSN: 2319-507X
Snehal Mankar, IJPRET, 2014; Volume 2 (9): 83-88 IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

CRYPTOGRAPHY, STEGANOGRAPHY AND NETWORK SECURITY

MISS. SNEHAL R. MANKAR

Computer Science and Information Technology, H.V.P.M COET Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Most of the data travel over the internet and it becomes difficult to make data secure. So Cryptography was introduced for making data secure. There arises a need of data hiding. So here we are using a combination of steganography and cryptography for improving the security**.** Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. We then illustrate two different approaches that help us achieve a higher level of secrecy and security, together with their limitations. The first method is about combining steganography and cryptography in such a way to make it harder for a steganalyst to retrieve the plaintext of a secret message from a stego object if cryptanalysis were not used. The second method does not use any cryptographic techniques at all and relies solelyon steganographic ones.

Keywords: Cryptography, Stegnography, PKS, SKC, AES, DCT.

Corresponding Author: MISS. SNEHAL R. MANKAR

Access Online On:

www.ijpret.com

How to Cite This Article:

Snehal Mankar, IJPRET, 2014; Volume 2 (9): 83-88

PAPER-QR CODE

INTRODUCTION

Cryptography and steganography :

Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence. These techniques have many applications in computer science and other related fields: they are used to protect e-mail messages, credit card information, corporate data, etc. steganography1 is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. In this paper we will focus to develop one system, which uses both cryptography and Steganography for better confidentiality and security. Presently we have very secure methods for both cryptography and Steganography – AES algorithm is a very secure technique for cryptography and the Steganography methods, which use frequency domain, are highly secured. This paper mainly focuses on to develop a new system with extra security features where a meaningful piece of text message can be hidden by combining security techniques like Cryptography and Steganography. There are many aspects to security and many applications. One essential aspect for secure communications is that of cryptography. But it is important to note that while cryptography is necessary for secure communications, it is not by itself sufficient. There are some specific security requirements [3] for cryptography, including Authentication, Privacy/confidentiality, and Integrity Non-repudiation. The three types of algorithms are described:

(A) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption

(B)Public Key Cryptography (PKC): Uses one key for encryption and another for decryption

(C)Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

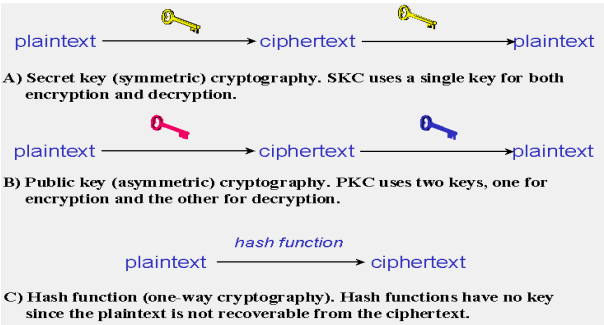

Fig . Encryption and Decryption

Steganography is the other technique for secured communication. It encompasses methods of transmitting secret messages through innocuous cover carriers in such a manner that the very existence of the embedded messages is undetectable. Information can be hidden in images [5], audio, video, text, or some other digitally representative code. Steganography systems can be grouped by the type of covers [6] used (graphics, sound, text, executables) or by the techniques used to modify the covers a) Substitution system

b) Transform domain techniques

c) Spread spectrum techniques

d) Statistical method

e) Distortion techniques

f) Cover generation methods

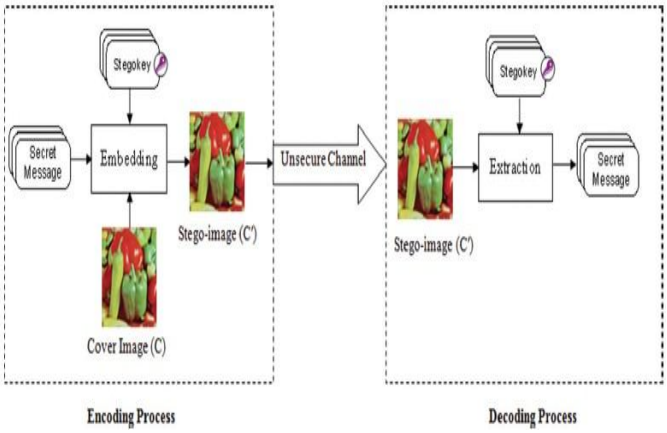

Fig. Encoding and Decoding Process

Materials and Method :

(A) AES algorithm for Cryptography :

This standard specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. The input, the output and the cipher key for Rijndael are each bit sequences containing 128, 192 or 256 bits with the constraint that the input and output sequences have the same length. In general the

length of the input and output sequences can be any of the three allowed values but for the Advanced Encryption Standard (AES) the only length allowed is 128.

(B) DCT frequency domain algorithm for Steganography

According to the method presented in this paper, the message is inserted into the DCT domain of the host image. The hidden message is a stream of "1" and "0" giving a total number of 56 bits. The transform is applied to the image as a multiple factor of 8x8 blocks. The next step of the technique after the DCT is to select the 56 larger positive coefficients, in the low-mid frequency range. The high frequency coefficients represent the image details and are vulnerable to most common image manipulation like filtering compression etc. Of course one might argue that this is the place where changes that come from watermarking are more imperceptible, but this is true only if we're speaking of small sized blocks. Our scheme is applied to the whole image and since robustness is the main issue, the low and mid frequency coefficients are the most appropriate. The selected coefficients *ci* are ordered by magnitude and then modified by the corresponding bit in the message stream. If the *i*th message bit *s(i)* to be embedded is "1", a quantity *D* is added to the coefficient. This *D* quantity represents the persistence factor. If the message bit is "0", the same quantity is subtracted from the coefficient. Thus the replaced DCT coefficients are

DCT (new) = DCT+1*D for s(i)=1;

Else

DCT (new) =DCT-1*D for s(i)=0. DCT can separate the Image into High, Middle and Low Frequency components. To hide information we need to set a threshold value for the DCT coefficients depending on the quality of the images.

RESULT AND DISCUSSION:

In this section, we show the experimental results of our proposed scheme with different logistic maps using a Lenna colour Image. *Look-Up-Table* concept in the proposed scheme makes the decryption time to be much faster

The Figures. 2,3,4 are the experimental results of our proposed scheme. We have shown the encryption and decryption results.

(a) (b) (c)

Fig. Encryption and decryption of the Image by our proposed Scheme using Logistic map. (a) Original Lenna Image, (b) Encrypted Lenna Image and (c) Decrypted Lenna Image.

A shows the used embedding grayscale image of the size 100 × 100. Fig. b shows the cover 24-bit image of the size 300 × 300 that is used in embedding and Fig.c shows the stego-image produced by embedding the secret image in the cover. The experimental results showed that the proposed algorithm reserved the image quality (PSNR = 48.0601 dB).

Fig.(a) Secret image (LENA); (b) Cover image (PEPPERS) and (c) Stego-image (PSNR = 48.0601 dB).

CONLUSION:

The main advantage of this Crypto/Stegno System is that the method used for encryption, AES, is very secure and the DCT transformation Steganography techniques are very hard to detect.

Steganography, especially combined with cryptography, is a powerful tool which enables people to communicate without possible eavesdroppers even knowing there is a form of communication in the first place. The proposed method provides acceptable image quality with very little distortion in the image. In this paper two layers of security i.e. cryptography and steganography are used which makes it difficult to detect the presence of hidden message. But in some cases if the evedropper has attacked the carrier of message then he will not be able to get the original message as all the relevant data here is in encrypted form.

REFERENCES:

1. R. Anderson, F. Petitcolas. On the limits of steganography. In IEEE Journal on Selected Areas in Communications, volume 16, number 4, 1998.

2. M. G. J. Fridrich. Practical steganalysis of digital images - state of the art. Security and Watermarking of Multimedia Contents IV, 4675:1–13, 2002

3. H. Farhat, K. Challita, J. Zalaket. Static parsing steganography. In Proceedings of Digital Information and Communication Technology and Its Applications, (DICTAP 2011), pages 485–492, 2011.

4. Ajit Singh, Aarti Nandal, Swati Malik "Implementation of Caesar Cipher with Rail Fence for Enhancing Data Security "IJARCSSE Dec,2012

5. Atul Kahate (2009), Cryptography and Network Security, second edition, McGraw-Hill.

6. Vijay Kumar Sharma ,Vishal Shrivastav" A steganography algorithm for hiding image in image by improved LSB substitution by minimize detection "Journal of Theoretical and Applied Information Technology 15th February 2012.

7. Gurjeevan Singh Ashwani Kr. Singla K.S. Sandha Superiority of Blowfish Algorithm in Wireless Networks International Journal of Computer Applications (0975 – 8887) Volume 44– No11, April 2012

8. Lokeswara Reddy Dr. A. Subramanyam Dr.P. Chenna Reddy" Implementation of LSB Steganography and its Evaluation for Various File Formats" Int. J. Advanced Networking and Applications Volume: 02, Issue: 05, Pages: 868-872 (2011)

9. Domenico Daniele Bloisi , Luca Iocchi: Image based Steganography and cryptography, Computer Vision theory and applications volume 1 , pp. 127-134 .

10. Kharrazi, M., Sencar, H. T., and Memon, N. (2004). Image Steganography: Concepts and practice. In WSPC Lecture Notes Series

11. D.R. Stinson, Cryptography: Theory and Practice, Boca Raton, CRC Press, 1995. ISBN: 0849385210

12. Provos, N. and Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE SECURITY & PRIVACY