International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 5, May 2015, PP 45-49
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

A Study on Combined Cryptography and Steganography

Vishnu S Babu
Dept. of Computer Science
GEC Thrissur, Kerala
vishnussudarsanam@gmail.com

Prof. Helen K J
Dept. of Computer Science
GEC Thrissur, Kerala
helenkj28@gmail.com

Abstract: *The digital communication has become an essential part of our daily life, a lot of applications are Internet-based and it is important that communication be made secret. We know cryptography and steganography are two methods used for data protection. The cryptography distorts the data and steganography hides the existence of data. But both of them have their own vulnerabilities, in this paper we are focused to combine cryptography and steganography in various ways to enhance the security of data.*

Keywords: *DWT,DCT.*

1. INTRODUCTION

The cryptography and steganography are two widely used techniques for confidentiality of data exchange. Cryptography is used to cipher information and steganography is used to hide the existence of data communication. Cryptography scrambles the information by using a key so that a third person cannot access the information without the key. Steganography hides the information by using a cover medium so that a third person cannot identify the communication.

Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, entity authentication, integrity of data and message origin authentication. Cryptography is also known as the science of secret writing. The goal of cryptography is to make data unreadable by a third party. Cryptography algorithms are divided into symmetric (secret-key) and asymmetric (public-key) network security protocols. Symmetric algorithms are used to encrypt and decrypt original messages (plaintext) by using the same key. While Asymmetric algorithms uses public-key cryptosystem to exchange key and then use faster secret key algorithms to ensure confidentiality of stream data. In Public-key encryption algorithms, there is a pair of keys, one key is known to the public, and is used to encrypt information to be sent to a receiver who owns the corresponding private key. The private and public keys are both different and need for key exchange.

Steganography is the art and science of writing hidden messages in such a way that no one, except the sender and intended recipient, suspects the existence of the message, a form of security through hiding the message.ie., Steganography is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such way that only carrier is visible which is sent from transmitter to receiver without scrambling. Like cryptography different types steganography techniques are available based on the hiding techniques, cover medium used etc.

Individually cryptography and steganography provides confidentiality to the data but they have some vulnerability. So as a third option we can go for a combination of cryptography and steganography There are different kinds of cryptographic and steganography techniques available so we can have different combinations of cryptography and steganography, in this paper we are comparing the different combinations based on their security. We are focused on image based steganography i.e. the cover medium is image.

2. CRYPTOGRAPHIC TECHNIQUES

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. It is performed by converting messages or data into a different form, such that no-one can read them without having access to the 'key'. All

encryption algorithms are based on two general principles: substitution, in which each element of the plaintext is mapped into another element, and transposition, in which elements of the plaintext are rearranged. The fundamental requirement is that no information be lost

Secret Key (Symmetric): With secret key cryptography, a single key is used for both encryption and decryption. The sender uses the key to encrypt the plaintext and sends the cipher text to the receiver. The receiver applies the same key to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called as symmetric encryption.

Public Key: In public key cryptography encryption and decryption are performed using different keys. The sender need not send the decryption key. In this system a user can have public key and private key, the public key is known to all other users and private key known only for the user itself. So encryption is performed using receiver's public key so that the receiver can decrypt it with his private key.

DES algorithm for cryptography

Data Encryption Standard (DES) is a standard for the encryption of electronic data. It is a symmetric-key algorithm invented in the early 1970 at IBM. DES is now considered to be insecure for many applications because the DES algorithm [3] uses a 56-bit key for encryption which is too small. DES can be cracked using brute force attack. DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm.

1) RSA algorithm for cryptography

RSA is one of the earliest public-key cryptosystems and it is widely used for securing data transmission. RSA was first described in 1977 by Ron Rivest, Adi Shamir and Leonard Adleman of the Massachusetts Institute of Technology. Here encryption key is public and decryption key is private, it kept secret. RSA is based on factorizing two large prime numbers. The public and the private key-generation algorithm is the most complex part of RSA cryptography. We can generate two large prime numbers, x and y, using the Rabin-Miller primality test algorithm. A modulus is calculated by multiplying x and y. This number is used by both the public and private keys and provides the link between them. Its length is called the key length.

2) AES algorithm for cryptography

Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. The U.S. government held in 1997 and now use in worldwide. AES is a symmetric-key algorithm which means that the same key is used both of sender and receiver. This AES standard specifies the Rijndael[13] algorithm, a symmetric block cipher that can process data blocks of 128 bits, using key size of 128, 192, and 256 bits. The input, the output and the cipher key are used in Rijndael. It takes an input and output of certain block size of only 128 bits.

3. STEGANOGRAPHY TECHNIQUES

Steganography [9] is concealed writing and is the scientific approach of inserting the secret data within a cover media such that the unauthorized viewers do not get an idea of any information hidden in it. Steganography is an alternative to cryptography in which the secrete data is embedded into the carrier in such a way that only carrier is visible which is sent from transmitter to receiver without scrambling. Steganography is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but it can be used to improve the security of cryptography.

1) LSB –Steganography.

In Least Significant Bit (LSB) steganography [8] embed the text message in least significant bits of digital picture. In which data is embedded by replacing the LSB of cover carrier with the data to be send.ie first read the cover image and text message which is to be hidden in the cover image, then convert text message in binary. Calculate LSB of each pixels of cover image. Replace LSB of cover image with each bit of secret message one by one so we get an image in which data is hidden.

2) DCT - Steganography

The hidden message is converted into binary stream of "1" and "0" are insert the into the DCT domain of the cover image. The color-based transformation converts the image (cover image) into 8x8

blocks of pixels. [8] Next, take larger positive coefficients need to embed in the cover image in the low-mid frequency range. DCT can divide the image into high, middle and low frequency components. As the high frequency coefficients are vulnerable and less robust on the quality of image. The main issue of this work is robustness against with high quality of image, thus the low and mid frequency coefficients are the most appropriate. The selected coefficients ci are modified by the corresponding bit in the message stream. This K quantity represents the persistence factor. As soon as the ith term of message bit s(i) is "1", the coefficient of the image is added with a quantity K; otherwise the same quantity is subtracted from it.

3) DWT-Steganography

A discrete wavelet transform (DWT) is any wavelet transform [6] for which the wavelets are discretely sampled. This is one of the frequency domains in which steganography can be implemented. DCT is calculated on blocks of independent pixels, a coding error causes discontinuity between blocks resulting in annoying blocking artifact.[] This drawback of DCT is eliminated using DWT because DWT applies on entire image. DWT offers better energy compaction than DCT without any blocking artifact. DWT splits component into numerous frequency bands called sub bands known as

LL – Horizontally and vertically low pass

LH – Horizontally low pass and vertically high pass

HL - Horizontally high pass and vertically low pass

HH - Horizontally and vertically high pass

Since Human eyes are much more sensitive to the low frequency part (LL sub band) we can hide secret message in other three parts without making any alteration in LL sub band. As other three sub-bands are high frequency sub-band they contain insignificant data. Hiding secret data in these sub-bands doesn't degrade image quality that much.

4. COMBINED CRYPTOGRAPHY AND STEGANOGRAPHY

The cryptography and steganography has their own vulnerabilities so combining them can be used as a third option instead of using them individually. Using cryptography can hide the information from the user but it cannot hide the existence of communication. Different types of steganography and cryptography are available so we can have several combinations.

1) A simple combination

The information or data from the sender is taken as the plain text. Then the plain text converted into cipher text using any encryption method. The transformed cipher text can be used as the input for steganography. The key of cryptography is kept secret. Then the cipher text is embedded into the cover medium using steganography techniques. The cover image is transmitted to the receiver

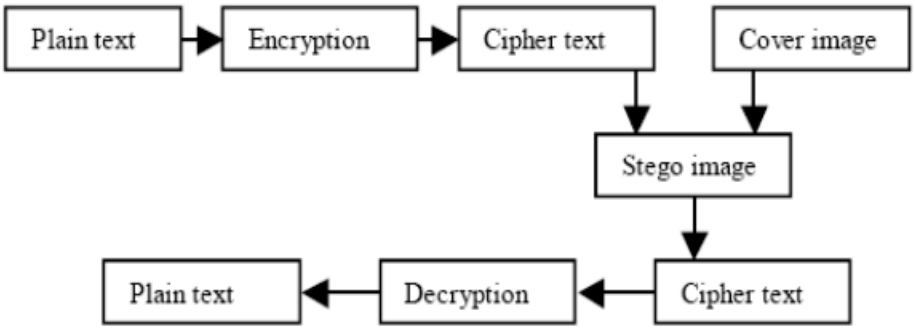

Figure 1. *Combined cryptography and Steganography*

This is a direct approach[1] in which both the methods are combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The generated stego-image can be transmitted without revealing that secret information is being exchanged. Now in order to improve the security we can apply various combinations of cryptography and steganography.

2) DES with LSB Steganography

Here DES algorithm is used to encrypt the data to be transferred then the encrypted information i.e. cipher text is hide within a cover carrier. Here an image can be used as a the cover carrier. The embedding process performed using LSB steganography. First of all the secret data is converted using DES cryptography thus we get cipher text. The cipher text is converted into binary. The [9]LSB (Least Significant Bit) of cover image is replaced with the binary cipher text. Then the image is transmitted to the receiver. One of the major disadvantages associated with LSB method is that the intruder can change the least significant bit of all the image pixels and the information gets destroyed. This method cannot tolerate noise and image compression.

3) AES with LSB Steganography

Here AES algorithm is used to encrypt the data to be transferred then cipher text is embedded into a cover carrier. Here 24 bit image can be used as cover carrier. The embedding process performed using [10] LSB steganography. First the information is converted using AES cryptography thus we get cipher text. The cipher text is converted into binary. For each 8 bit data, the first three bits of the data are replaced by the three least significant bits of the red byte, the second three data bits are replaced by the three least significant bits of the green byte, the last two data bits are replaced by the two least significant bits of the blue byte. Then the image is transmitted to the receiver.

4) AES with DCT-Steganography

Here AES algorithm is used to encrypt the data, the cipher text is generated from the plain text using AES encryption. The cipher text then embedded into the cover image using DCT based steganography [5]in which a DCT transformation is applied on the cover image so the image get divided into high, middle and low frequency components. As the high frequency coefficients are vulnerable and less robust on the quality of image, we can use the low and mid frequency coefficients. The selected coefficients are modified by the corresponding bit in the message stream. If ith term of message bit s(i) is "1", the coefficient of the image is added with a quantity K; otherwise the same quantity is subtracted from it. The main issue associated with this method is as the size of data increases image quality decreases.

5) AES-DCT-Steganography with cipher text splitting

Here to reduce size of data embedded on the image we embed only a part of the cipher text. AES algorithm is used to encrypt the data, the cipher text is generated from the plain text using AES encryption. The cipher text do not embedded into the cover image directly instead the cipher text is split. The cipher text generated from the AES encryption is of hexadecimal form, it contains 0 to 9 digits and 'a' to 'f' alphabets. First the digits and alphabets are separated and the position is kept as a key. First seven alphabets are embedded on the cover image using DCT based steganography. Remaining alphabets are combined and kept as another key. So the cipher text can be retained only by using the two keys. The main drawback of the system is it uses two extra keys which are very large compared to the part of data embedded in the cover image, so key exchange should be expensive.

6) AES with DWT-steganography

Here AES algorithm is used to encrypt the data, the cipher text is generated from the plain text using AES encryption. The cipher text then embedded into the cover image using DWT based steganography [6] in which a DWT transformation is applied on the cover image so the image get divided into four sub bands, Since Human eyes are much more sensitive to the low frequency part we can hide secret message in high frequency part without making any alteration in low frequency sub band. DWT steganography can hold more data without distortion to the cover image.

5. CONCLUSION

Cryptography and steganography are well known methods for data security. To enhance the security we can use combined cryptography and steganography instead of using cryptography or steganography alone. In this paper we have reviewed various combinations of cryptography and steganography methods. Here we are dealing with image based steganography so reduce the image quality degradation is the main task in order to improve security. From the above comparison we can infer that DWT based steganography with AES encryption can provide better security because this method can retain the image quality.

REFERENCES

[1]. A. Joseph Raphael Dr. V. Sundaram, "A Survey on cryptography and steganography", Int. J. Comp. Tech. Appl., Vol 2 (3), ISSN:2229-6093

[2]. Dipti Kapoor Sarmah, Neha bajpai, " Proposed System for Data Hhiding Using Cryptography and Steganography", International Journal of Computer Applications (0975 – 8887), Volume 8 – No. 9, October 2010.

[3]. Sashikala Channalli and Ajay Jadhav, "Steganography An Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009.

[4]. Ramakrishna Mathe, Veera RaghavaRao Atukuri, Dr. Srinivasa Kumar Deviredd "Securing Information: Cryptography and Steganography", International Journal of Computer Science and Information Technologies, Vol. 3 (3), 2012.

[5]. Khalil Challita and Hikmat Farhat, "Combining Steganography and Cryptography: New Directions", The Society of Digital Information and Wireless Communications, 2011 (ISSN 2220-9085).

[6]. Anjali A. Shejul, Prof. U.L Kulkarni, "A DWT based Approach for Steganography Using Biometrics" 2010 International Conference on Data Storage and Data Engineering.

[7]. C.P.Sumathi, T.Santanam and G.Umamaheswari "A Study of Various Steganographic Techniques Used for Information Hiding" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013.

[8]. Dr. Ekta Walia a , Payal Jain b , Navdeep c, "An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology Vol. 10 Issue 1 (Ver 1.0), April 2010.

[9]. Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May, 2013.

[10]. Rahul Joshi ,Lokesh Gagnani , Salony Pandey, "Image Steganography With LSB" International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 1, January 2013.

[11]. Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, (2010) March 1.

[12]. B B Zaidan, A.A Zaidan, A.K. Al-Frajat and H.A. Jalab, "On the Differences between Hiding Information and Cryptography Techniques: An Overview", Journal of Applied Sciences 10(15): 1650-1655, 2010.

[13]. Secure Data Transmission using Stegnography and Encryption Technique, Shamim Ahmed Laskar and Kattamanchi Hemachandran, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.3, September 2012.