Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 4, April 2015, pg.802 – 805

REVIEW ARTICLE

Data Hiding Using Steganography and Cryptography

Varsha[1], Dr. Rajender Singh Chhillar[2]

[1]M.Tech Student, Department of Computer Science & Application, M.D. University, Rohtak-124001

[2]Professor & Former Head, Department of Computer Science & Application, M.D. University, Rohtak-124001

[1]Email Id: munesh.kataria@gmail.com

***Abstract* — *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. This paper discussed a technique used on the advanced LSB (least significant bit) and RSA algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it*.**

Keywords*— *RSA algorithm, cryptography, steganography, LSB method

I. INTRODUCTION

The growing use of Internet among public masses and availability of public and private digital data and its sharing has driven industry professionals and researchers to pay a particular attention to information security. Internet users frequently need to store, send, or receive private information and this private information needs to be protected against unauthorized access and attacks. Presently, three main methods of information security being used: watermarking, cryptography and steganography. In watermarking, data are hidden to convey some information about the cover medium such as ownership and copyright. Cryptography techniques are based on rendering the content of a message garbled to unauthorized people. Steganography techniques are based on hiding the existence of information by embedding the secret message in another cover medium. While all three are information security techniques cryptography and steganography are having wide application as watermarking is limited to having information particularly about the cover medium. With the growth of computer network, security of data has become a major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets.

2. Proposed System

The aim of proposed scheme is to make a more secure and robust method of information exchange so that confidential and private data must be protected against attacks and illegal access. To order in achieve the required robustness and security cryptography and steganography is combined. Image is taken as a cover medium for steganography and RSA algorithm is used for encryption.

In this proposed method our advanced LSB bit manipulation method is used for embedding the message in the image file and the message is itself encrypted using the existing RSA encryption method. For embedding the text in image file firstly both the text and image file are converted into binary equivalent and then text is encrypted using RSA. The encrypted text is then embedded into the image file using our advanced LSB algorithm.

2.1 Cryptography

Cryptography is the art and science of achieving security by encoding messages to make them non readable. In this, the structure of message is scrambled to make it meaningless and unintelligible unless the decryption key is available. 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 something or someone. Cryptanalysis is the reverse engineering of cryptography.

There are several ways of classifying cryptographic algorithms. The three types of algorithms are:

(1) Secret key Cryptography: Uses a single key for both encryption and decryption

(2) Public Key Cryptography: Uses one key for encryption and another for decryption.

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

2.1.1 RSA Algorithm

The algorithm was given by three MIT's Rivest, Shamir & Adelman. RSA algorithm is a message encryption cryptosystem in which two prime numbers are taken initially and then the product of these values is used to create a public and a private key, which is further used in encryption and decryption. The RSA algorithm could be used in combination with advanced LSB in a way that original text is embedded in the cover image in the form of cipher text. By using the RSA algorithm we are increasing the security to a level above. In case of steganalysis only cipher text could be extracted which is in the encrypted form and is not readable, therefore will be secure.

RSA algorithm procedure can be illustrated in brief as follows:

1. Choose two large prime no. p & q.
2. Calculate N=p*q
3. Calculate f(z)=(p-1)*(q-1)Find a random number e satisfying 1 < e < f (n) and relatively prime to f (n) i.e., gcd (e, f (z)) = 1.
4. Calculate a number d such that d = e-1 mod f (n).
5. Encryption: Enter message to get cipher text. Ciphertext c= mod ((message. ^e), N).
6. Decryption: The cipher text is decrypted by :

   Message=mod ((c. ^d), N) [5]

2.2 Steganography

Steganography is a very old technique of information hiding. Steganography refers to the science of invisible communication. Unlike cryptography, where the goal is to secure communications from an eavesdropper, steganographic techniques strive to hide the very presence of the message itself from an observer. The term Steganography is forked from the Greek words ―steganos meaning ―cover and ―graphia meaning ―writing defining it as ―covered writing. Before performing steganography we need three primary accessories which are Secret message, Cover medium and one or more embedding algorithm(s) besides these we can also use secret key for better security purpose. In the process of steganography the cover medium can be a text file, an image, an audio file or it can be a video file but among these most popular is the Image steganography, so here are the some advantages of using images as cover medium in performing steganography.

2.2.1 LSB Technique

A simple approach for embedding information in cover image is using Least Significant Bits (LSB). The simplest steganography 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. To hide a secret message inside an image, a proper cover image is needed. Because this method uses bits of each pixel in the image, it is necessary to use a lossless compression format, otherwise the hidden information will get lost in the transformations of a lossy compression algorithm. When using a 24-bit color image, a bit of each of the red, green and blue color components can be used, so a total of 3 bits can be stored in each pixel.

For example, the following grid can be considered as 3 pixels of a 24-bit color image, using 9 bytes of memory:

(00100111 11101001 11001000)

(00100111 11001000 11101001)

(11001000 00100111 11101001)

When the character A, which binary value equals 10000001, is inserted, the following grid results:

(0010011**1** 1110100**0** 1100100**0**)

(0010011**0** 1100100**0** 1110100**0**)

(1100100**0** 0010011**1** 11101001)

In this case, only three bits needed to be changed to insert the character successfully. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximal cover size. The result changes that are made to the least significant bits are too small to be recognized by the human visual system (HVS), so the message is effectively hidden.

2.3 COMBINATION OF CRYPTOGRAPHY & STEGANOGRAPHY

Steganography must not be confused with cryptography that involves transforming the message so as to make its meaning obscure to malicious people who intercept it. In this context, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. According to, steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated.

However, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an audio or any other media with the help of stego key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The figure below depicts the combination of cryptography and steganography.

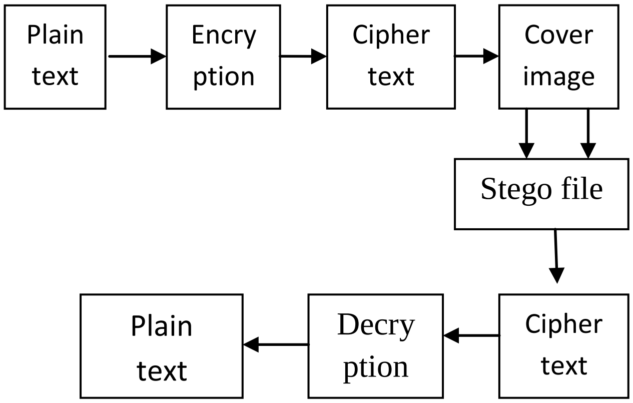

Fig 1: Combination of Cryptography and Steganography

3. Conclusion

A secured ADVANCED based LSB technique for image steganography has been proposed. An efficient steganographic method for embedding secret messages into cover images without producing any major changes has been accomplished through ADVANCED-LSB method. In this work, a new way of hiding information in an image with less variation in image bits have been proposed, which makes our technique secure and more efficient than LSB. This technique also applies a cryptographic method i.e. RSA algorithm to secure the secret message so that it is not easy to break the encryption without the key. RSA algorithm itself is very secure that's why we used in this technique to increase the security of the secret message.

References

[1] K.Hemachandran, "Study *of Image Steganography using LSB, DFT and DWT",* International Journal of Computers & Technology, vol 11, oct.25 2013, pp. 2618-2627
[2] Zin.w, soe. N **"***Implementation and Analysis of three Steganographic Approaches*", University of Computer Studies, Mandalay, 2011, pp. 456-460
[3] Manoj.s,"Cryptography *and Steganography*", International Journal of Computer Applications (0975-8887), 2010, vo1-no.12, pp. 63-68
[4] Adewole Kayode S. and Oladipupo Ayotunde J. *"Efficient Data Hiding System using Cryptography and Steganography*", International Journal of Applied Information Systems (IJAIS), Volume 4– No.11, December 2012, pp. 6-11
[5] Anil kumar, Rohini Sharma "*A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique"* International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013
[6] Kumar S P , K. Anusha, R.Venkata Ramana, "*A Novel Approach to Enhance Robustness in Steganography Using Multiple Watermark Embedding Algorithm*". International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307 (Online), Volume-1, Issue-1, March 2011
[7] Masoud Nosrati , Ronak Karimi "*An Introduction to Steganography Methods"* World Applied Programming, journal, Vol (1)-No (3), August 2011. 191-195
[8]Applicationof steganography. Internet source http://www.datahide.com/BPCSe/applications-e.html