International Journal of Advanced Technology in Engineering and Science
Vol. No.5, Issue No. 02, February 2017
www.ijates.com
ijates
ISSN 2348 - 7550

MULTILAYER DATA HIDING USING SLS COMBINED WITH LSB TECHNIQUE FOR IMAGE CRYPTO-STEGANOGRAPHY

Mr. Abhale Babasaheb A[1], Ms. Jyoti Bhagwat[2], Ms. Priyanka Dopare[3]

[1,2,3] SND COE & RC ,Savitribai Phule Pune University(India)

ABSTRACT

Now a day's the data or information transmission filed the security must be important. Cryptography and steganography there are two important aspects that deal with a data or information transmission. Cryptography is to hide the message. Steganography is to hide the message in image. We can use Stochastic Local Search (SLS) combined with least significant Bit (LSB) technique for steganography. First we can use only LSB technique to hide the information in JPEG image. But image size can be increase the LSB technique will not be more effective in JPEG image. In order to improve the performance, we added a meta-heuristic approach in LSB technique.Now in this technique we can add cryptography and steganography is called as crypto-steganography. This crypto-steganography image is secure for transmission. A crypto-steganography uses a new technology that is multilayer crypto-steganography. In this technique use two cover file they are strongly hide the data. The size of this image is large for data transmission so we can use compression technique.

Keyword: Encryption, Decryption, Compression, Decompression, Multilayer Steganography, Cryptography.

I INTRODUCTION

Now a day's for data transmission is used to internet various transmission media to send the data for sender to receiver like email, social sites etc. in this type of transmission the attack can easily attack on this message. The attacker can miss use of this message. So in order to transmit the sensitive or secure data to the receiver use the cryptography and steganography method. Why attacker can easily attack on the message reason is that they have opportunity to read and comprehend most of the information from the system. The solution of this problem is that use the cryptography and steganography.

1) Cryptography

Cryptography is hide the message nobody can read this message only person read they can hold the key. Cryptography comes from Greek word where "Crypto" means "Secrete" and "Graphy" means "Writhing". Cryptography provides the security for data file.

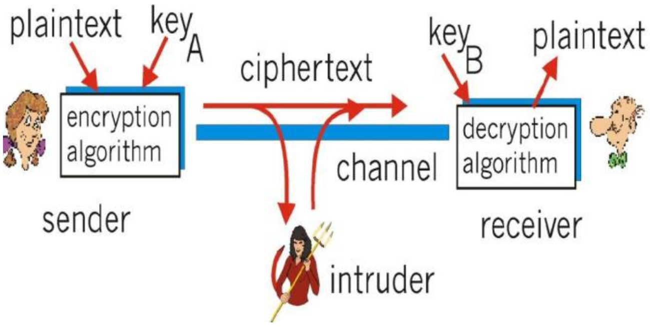


Fig1.1.1: cryptography

The sender can send the plain text file which is readable form using one encryption algorithm file can be convert the chipper text which is unreadable forms. The attacker cannot see the actual data the receiver can receive this file. In the cipher text file apply the one decryption algorithm used for converting cipher text file back to the plain text file. Receiver can see the actual data. Cryptography uses the key for encryption or decryption purpose.

2) Steganography

Steganography is to hide the content of message. The word steganography comes from Greek word where “Steganos” means “Covered” and “Graphy” means “Writing”. Steganography consist of various forms thos are image, audio, video etc.

Following are the components of steganography:

1) Carrier image

2) The Message

3) Key

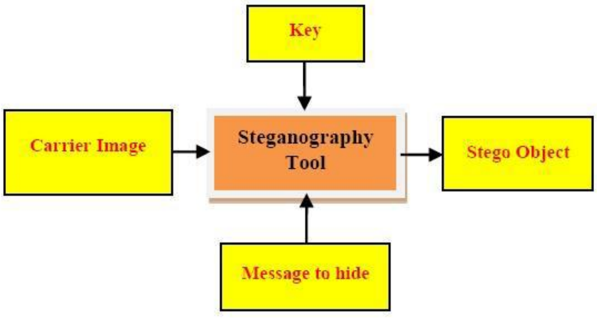


Fig1.2.1: Steganography

- The Carrier image: The cover object contains hidden message that is called as carrier image.
- The Message: A message consists of anything like data, file or image etc.
- The Key: A key is utilizing decode/decipher/discover the hidden message.

3) Compression

Compression is the reducing the number of bits its need to be store or transmit data. Lossless and lossy are the type of compression technique. Lossless is text or program and lossy is image, audio, video.

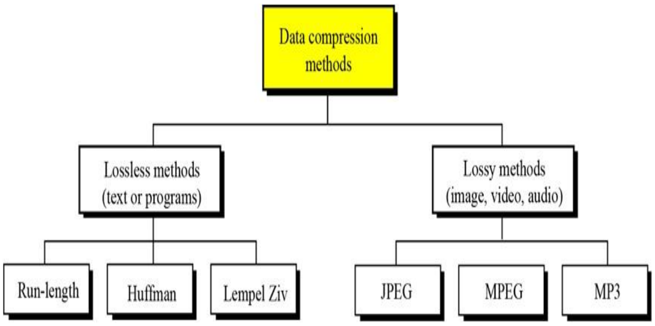

Data compression methods
Lossless methods (text or programs)
Lossy methods (image, video, audio)
Run-length
Huffman
Lempel Ziv
JPEG
MPEG
MP3

Fig1.3.1: Method for data compression

II LITERATURE REVIEW

In this portion we discourse the methodologies Review, Literature Review and Motivation Outcome from it.

2.1 Review of Methodology

- SMS-texting language is a new method for secure communication using text-steganography [1].
- Cryptography and steganography is the two technique combine to overcome the limitation and weakness [2].
- Encrypt and decrypt the data audio video sequence utilizing optical crypto technology which is based on double random phase encoding algorithm [3].
- New stego base algorithm based on hiding the max amount of data file into color Bitmap Image (BMP) for construction and implementation [4].
- For performing the significant attention with alternate way to ensure the security provide the new approach-data layer security data hiding [5].
- Execution of the different cryptography algorithm utilizing 32-bit RISC processor block, the security has been built a data storage device for real time data [6].

2.2 Motivational Outcomes

Following are the different outcomes are motivated for the current system:

- For providing the need of data security using cryptography technique to convert the readable data into unreadable form because the chance of hacking the secrete message.
- There is less chances of breaking stenography by stego-analysis but for more certainty of data security it needed to design new technology that is multilayer stenography.
- In these multi-layering techniques the data size is increase to solve this problem we need to design data compression technique for this system.
- There is less chances of breaking stenography by stego-analysis but for more certainty of data security it

needed to design new technology that is multilayer stenography.

III PROPOSE SYSTEM

3.1 Introduction

The Basic Crypto-Stego-Encoder and Crypto-Stego-Decoder Architecture:

In this system the sender side perform the encoding of data and receiver side perform decoding of data. First massage in plain text format encrypted using encryption algorithm using key. The message is converted into cipher text and taking the cover image for applying the steganography generates the crypto-stego image. Then we are taking the master cover image for applying double layer steganography and generate the multilayer crypto-stego image. This data file obviously size is increase we apply the compression technique generate the compress multilayer crypto-stego image this image is more secure.

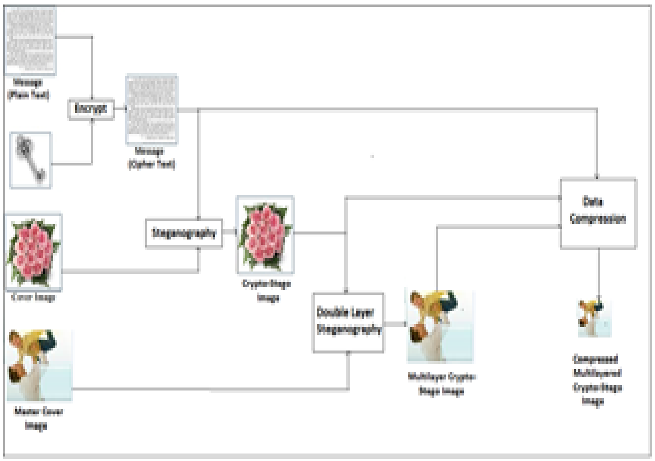


Fig3.1.1: The Working of a Multilayer Crypto-Steganography Data Hiding Encoder Architecture.

Following fig shows the decoder architecture in this decodes the message by using decoding algorithm. Compressed multilayer crypto-stego image applying the decompression algorithm and generate the master cover file. Select the master cover file and generate the cover file. Select and remove the primary cover file and generate the cipher text applying the decoding algorithm and generate actual data.

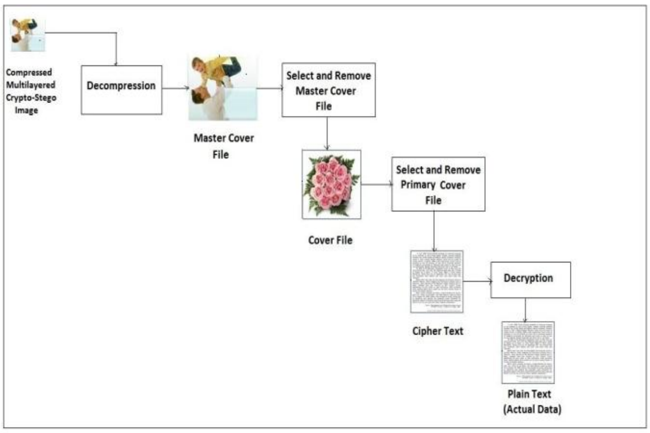


Fig3.1.2: The Working of a Multilayer Crypto Steganography Data Hiding Decoder Architecture

3.2 Algorithm

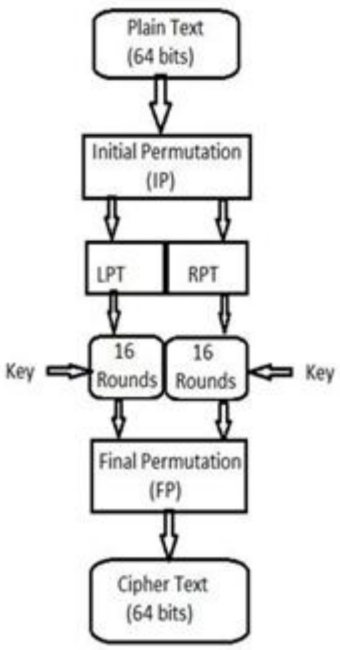
Following are the algorithm applies for this system:

1) DES (Data Encryption Standard)

2) LSB+SLS

3) RLE (Run Length Encoding)

1) DES



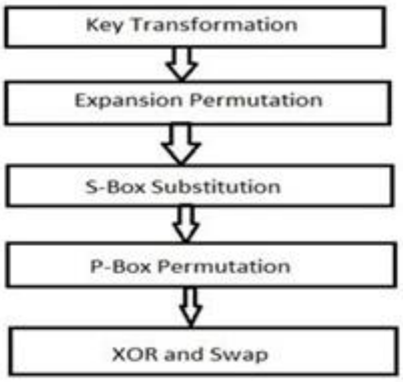


Fig3.2.1: steps for DES algorithm **Fig3.2.2: Rounds in DES**

1) It contains the 16 round 64-bit plain text block use for initial permutation.

2) IP produces two halves they are LPT (Left Plain Text) and RPT (Right Plain Text).

3) Encryption is performed by LPT and RPT goes through the 16 rounds of process, they have its own key.

4) At the end LPT and RPT are rejoined then final permutation is performed.

5) Then final result is 64-Bit cipher text.

The first bit of original plain text is 58th IP replaces 8th bit of original plain text and second bit with 50th and so on. The IP operation done, the resulting 64 bit are divide into two part each bock is 32 bit (LPT and RPT) 16 rounds performed on this two block.

2) LSB+SLS Steganography technique uses the List significant Bit combine with Stochastic Local Search.

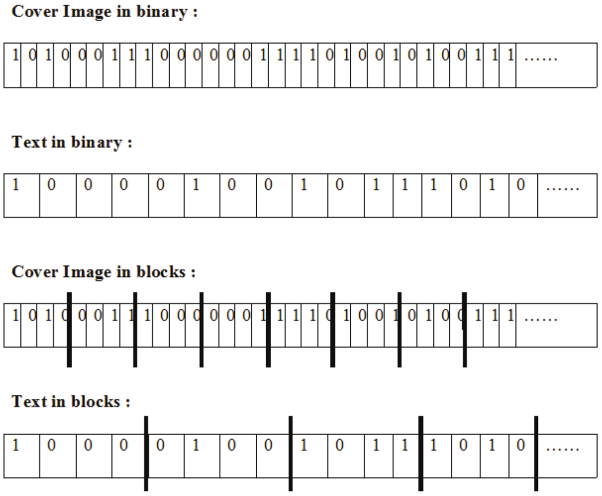


Fig3.2.3: Cutting the message and the cover image in blocks.

In this algorithm the cover image is converted into binary form. These binary forms are decomposing into 4 bit block. In this binary form the message and image bits are matching they are combing.

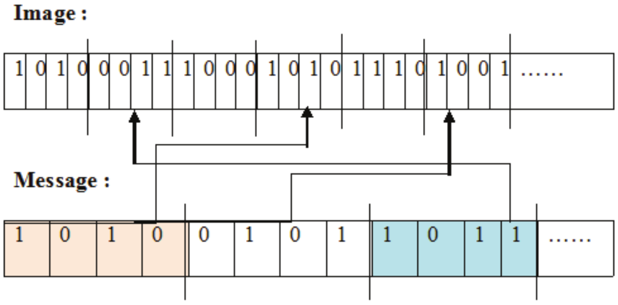


Fig3.2.4: The solution representation

IV CONCLUSION

A new high capacity with newly high secure data hiding has been presented. For wide range of data security providing master cover file is more essential for data security as multi-layer Steganography including Cryptography. This system produce good quality of stego image for a fairly high amount of payload with compression based system.

REFERENCES

[1] Shirali-Shahreza, M.H. ; Dept. of Comput. Eng., Yazd Univ., Yazd ; Shirali- Shahreza, M., *"Text Steganography in chat"*, Internet, 2007. ICI 2007. 3rd IEEE/IFIP 47 International Conference in Central Asia on , pp.1 - 5.

[2] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "*A Crypto-Steganography: A Survey*", In IJACSA, Vol.5, No.7, 2014, pp. 149 - 155.

[3] Guizani, S. ; Coll. of Eng., Alfaisal Univ., Riyadh, Saudi Arabia ; Nasser, N. , *"An audio/video crypto Adaptive optical steganography technique"*, In Wireless Communications and Mobile Computing Conference (IWCMC), 2012 8th International , pp. 1057 - 1062.

[4] Nameer N. EL-Emam, "*Hiding a Large Amount of Data with High Security Using Steganography Algorithm."*, Journal of Computer Science 3 (4): 223-232, 2007 ISSN 1549-3636, pp.223 - 232.

[5] Shabir A. Parah, Javaid A. Sheikh, Abdul M. Hafiz and G.M. Bhat, *"Data hiding in scrambled images : A new double layer security data hiding technique"* , In computers and electrical engineering , Vol.40, 2014, pp. 70 - 82.

[6] HoWon Kim, Member, IEEE, and Sunggu Lee, Member, IEEE*, "Design and Implementation of a Private and Public Key Crypto Processor and Application to a Security System"*, In IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, FEBRUARY 2004 pp. 214 - 224.

[7] Stochastic Local Search Combined with LSB Technique for Image Steganography Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi LRIA-USTHB, Department of Computer Science University of Sciences and Technology Houari Boumediene BP 32 El-alia, Bab-Ezzouar, 16111 Algiers, Algeria.

[8] Alvaro Martn, Guillermo Sapiro, and Gadiel Seroussi, Fellow, IEEE., *"Is Image Steganography Natural?, In IEEE Transaction On Image Processing"*, VOL. 14, NO. 12, DECEMBER 2005, pp. 2040 - 2050.

[9] Jessica Fridrich, Miroslav Goljan, Petr Lisonek, and David Soukal, *"Writing on Wet Paper, In IEEE Transactions On Signal Processing"*, VOL. 53, NO. 10, OCTOBER 2005, pp.3923 - 3935.

[10] Jamshed Hasan, *"Security Issues of IEEE 802.16 (WiMAX)"*, Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006.

[11] Naji, A.W. Dept. of Electr. and Comput. Eng., Int. Islamic Univ. Malaysia, Kuala Lumpur, Malaysia, Gunawan, T.S. , Hameed, S.A. , Zaidan, B.B. more authors , "*Stego- Analysis Chain, Session One Investigations on Steganography Weakness vs Stego- Analysis System for Multimedia File*", Computer Science and Information Technology - Spring Conference, 2009. IACSITSC 09., pp. 405 - 409.