Advance Data Encryption and Decryption Approach to Enhance Security Using Text Steganography & Cryptography

Dhiral Parghi[1], Krunal Panchal[2]
[1]Student LJIET, Ahmedabad, India, [2]Assistant Prof. LJIET, Ahmedabad
[1]Computer Engineering
[1] LJIET, Ahmedabad, India.

***Abstract**:In Current era of information technology it is difficult to secure information from unlawful activities for this reason different strategies including cryptography, steganography have been utilized. Cryptography is an area to encrypt and decrypt information to convert information into unreadable form & steganography is use to hide the existence of a message from playing eyes. Because of lesser memory requirement & lower complexity text is highly used communication medium so in this research work we will focus on securing a text data. In this paper we propose a method that adds additional loss less compression technique to hide secure data. Apply advance approach to encrypt and decrypt data by combining Cryptography & Steganography technique.*

Keywords: Data security, Text Steganography, Cryptography.

I. INTRODUCTION

With Increasing use of computer in different area of life & work the issue of securing information has gained special importance. Two basic terms use for security is Cryptography & Steganography. Cryptography is an art of converting information into a format that can only be easily readable by those who have secret key to decrypt the message. But it has limitation that the encrypted message is visible to everyone so it is suspicious by anyone for having secret information. Steganography is technique to hide a secrete message within other message in such a way that other cannot discrete the presence of hidden message So Steganography can overcome the limitation of cryptography by hiding cipher text into other message which helps to give a higher level of security.

Our goal is to empower users by a providing secure and efficient system that helps them to provide a data hiding method by applying Steganography. To improve data hiding capacity of a cover text compression will apply first to user data then compressed data is encrypted by applying an encryption algorithm that helps to increase security and at the end encrypted data is hidden inside other text document using steganography method in such a way that other user except sender and receiver cannot see any secret data hidden inside a document.

In our system to hide a data over cover text we have use a Whitespace character based text steganography method. Traditional whitespace character method add additional whitespace character at end of line, start of paragraph and between words too that results in size of a Stego text. Instead of adding extra whitespace at cover text, in proposed method we are using original whitespace of cover text to hide data so it will not affect size of cover text that much. Changes in Whitespaces are not easily visible to human eyes so it also helps to reduce imperceptibility & reduce suspiciousness of having secret information hidden inside a text leads to improve a security.

II. RELATED WORK

Aruna Malik et al.,[1] discuss a format based text Steganography approach with compression. They hide the data into forward email address& cover message of email. To increase data hiding capacity LZW compression is directly applied to secret text and obtain bit stream is hidden into email ids and the message of email [1].color mapping table is used to hide the secret data bit into the cover text of email .email ids can be generated by applying mathematical formula on bit stream generated from LZW compression.

Savita D Torvi et al.,[2] provide data security using text Steganography with XOR encryption. Here text is first encrypted with XOR operation using password (key). Two methods are given as Color and font base Steganography. User can choose method base on his requirement. Color base Steganography method change font color of secret text and cover text in such a way that change of color is not easily recognized from neck eye. Similarly Font Steganography changes the size of the font of cover text and secret text.

Md. Palash Uddin et al.[3]Propose data hiding using format based text Steganography along with DES encryption algorithm. Cover text is made explicitly in such a way that it looks like ordinary text consisting of all English characters [3]. Original message is encrypted using DES Algorithm. Characters position and frequency of cipher text is added as alphanumeric puzzle in cover text.

Sahil Kataria et al.[4] provide text Steganography approach which works on encryption using XOR operation between original message and cover text. Encrypted text is reorder using eight bit random key. Random key contains four number of 0's & four number of 1's.0 bit describe cover text & 1 bit describe original text. At the end of encipher text random key is appended.

Sunita Chaudhary et al.[5] use feature coding and random character generation text Steganography method. They use a shape of alphabetic character of English language & name method as "Capital Alphabet shape encoding method" .here every character of secret message is encoded in 8 bit binary number & replace by equivalent ASCII character. They had divided Capital letters of English character into groups like letters with vertical straight line, letters with horizontal lines, letter with curve, letters with curve and horizontal lines, letters with curve horizontal & vertical lines, letters with no curve horizontal & vertical line. They use English characters, symbols and digits for random generation of cover text.

Santanu Koley et al.[6]provides a number system based text steganography approach .they are dividing numbers into a group in such a manner that the first group restrain only one number and so on n^{th} group can enclose n numbers digit [6].Character of secret message is converted into ASCII value and ASCII value is represented as value pair of (M, N) where M is number of group that fully completed & N is number of extra element from left side of group. This value pair is represented as a date & month format into a cover message.

III. PROPOSED WORK

In Proposed system, Secret information is taken from sender side in text format. Text information is applied for LZW compression to reduce the data size. After that compressed data is applied for AES encryption to generate a cipher text. Cover text is generated to hide the cipher text. Cipher data is hidden inside a cover text using Whitespace character based text steganography.

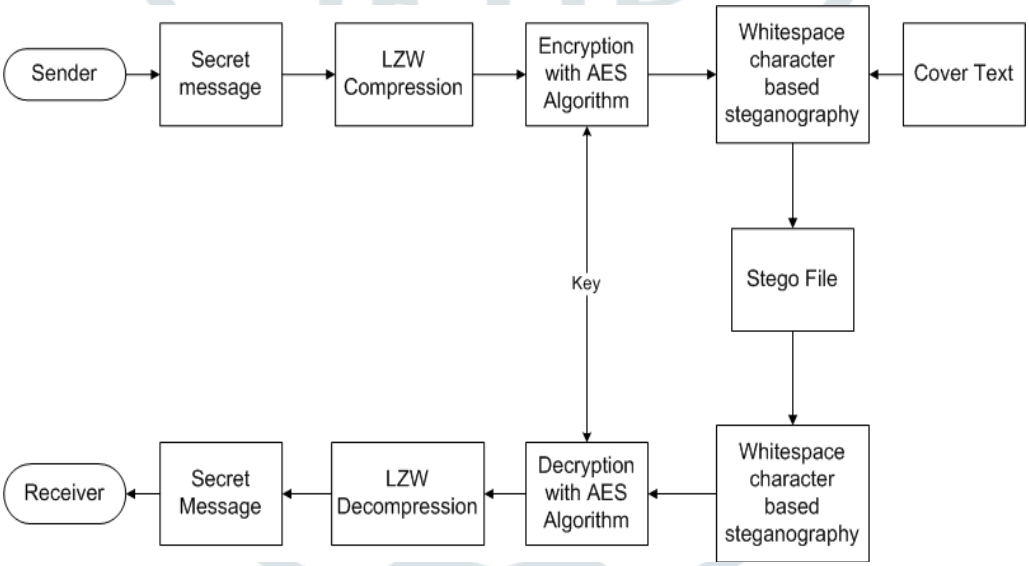

Figure 1: Proposed Method

The Lempel-Ziv-Welsh (LZW) is a lossless data Compression technique which builds a dictionary of frequently use character. LZW uses fixed-length code words to represent variable-length strings of symbols/characters that commonly occur together, e.g., words in English text. LZW places longer and longer repeated entries into a dictionary, and then emits the code for an element, rather than the string itself, if the element has already been placed in the dictionary. Here 256 bits are stored for single value of ASCII code. String is parsed & character group are added to dictionary & data is encoded on base of occurrence of character.

AES(Advance Encryption Standard) is a Symmetric key Cryptography algorithm that follows 128 bit block structure and provides encryption using 128,192 or 256 bit key value. It consists of 4 functions: Substitute byte transfer, Shift row transformation, Mix Column, Add Round key.

Whitespace character Based Steganography is method of text steganography in which the data hiding is performing using whitespace characters of a cover text. Traditional whitespace characters method whitespaces are adjoin inside the real text after last part of every line, conclusion of each paragraph or among the words.

Steps of proposed method are as follow:

Step 1: Take a plain text or secret information from sender.
Step 2: Apply LZW compression over secret information.
Step 3: Compressed message is encrypted using an AES Algorithm.
Step 4: Take a cover text & scan whitespace, hide cipher text inside a cover text using whitespace character based text steganography method & generate Stego file.
Step 5: transmit Stego text to receiver.

Step 6: Get cipher text from Stego text by applying whitespace character based steganography.
Step 7: Decrypt cipher text by applying AES Algorithm to generate compressed text.
Step 8: Decompress the text by applying LZW decompression algorithm.
Step 9: Decompressed text is original secret message to receiver

IV. RESULT ANALYSIS

Experiment of proposed method is executed on computer having Intel (R) Core (TM) i5-5200U CPU@2.20GHz with 4GB RAM having Windows 8.1(64 bit) operating system.In Text Steganography Data hiding capacity is a major Parameter for performance analysis. In this section data hiding capacity is calculated and compared with other researchers developed method. Execution time required for different compression technique and Encryption algorithm with whitespace steganography method are also shown in table 2.

$$\text{Equation for calculating data hiding capacity} = \frac{\text{Bits of secret message}}{\text{Bits of Stego cover}}$$

Method	Data Hiding capacity
Sun et al.[11]	2.17
Wang et al.[13]	3.53
Rajeev et al.[12]	7.21
Aruna Malik et al[1]	13.43
Proposed method	18.82

Table 1: Comparison of Data hiding Capacity

Compression Technique	Encryption Algorithm	Execution time
LZW	AES	0.167602
Huffman	AES	0.268744
LZW	RSA	2.032618
Huffman	RSA	2.173399

Table 2: Execution time of whitespace steganography method with different Compression & Encryption technique

V. CONCLUSION

In Literature survey it is seen that text steganography methods are still suffering from having lower level of security & low data hiding capacity. In proposed method we have combine a steganography & Cryptography approach to enhance security.Use of compression technique increases the data hiding capacity of the proposed work. In this paper we have used whitespace text steganography method to hide a secret data that is invisible to user so it will reduce suspiciousness of having secret data.

VI. REFERENCES

[1] Aruna Malik , Geeta Sikka, Harsh K. Verma" A high capacity text Steganography scheme based on LZW compression and color coding", Engineering Science and Technology, an International Journal 20 (2017) Elsevier http://dx.doi.org/10.1016/j.jestch.2016.06.005, Year:2016, Pages:72-79

[2] Savitha D Torvi; K. B. ShivaKumar; Rupam Das" An unique data security using text Steganography " IEEE 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)Year: 2016,ISBN**:** 978-9-3805-4421-2, Pages: 3834 – 3838

[3] Yanchen Liu, Jian Wang, Zhibin Wang, Qifeng Qu, Shun Yu," Developing an efficient solution to information hiding through text Steganography along with Cryptography" IEEE Lecture Notes in Computer Science, vol. 10039, ISSN 0302-9743, ISBN 978-3-319-48670-3, Year:2014 Pages: 178.

[4] Sahil Kataria; Tarun Kumar; Kavita Singh; Maninder Singh Nehra" ECR (encryption with cover text and reordering) based text steganography" 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013),DOI: 10.1109/ICIIP.2013.6707666, Year: 2013 Pages: 612 - 616

[5] Sunita Chaudhary, Dr. Meenu Dave, Dr. Amit Sanghi" Text Steganography Based on Feature Coding Method" 2016 ACM. ISBN 978-1-4503-4213-1/16/08, DOI: http://dx.doi.org/10.1145/2979779.2979786

[6] Santanu Koley, Kunal Kumar Mandal" A Novel Approach of secret message passing through text steganography" 2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES), Year: 2016 , DOI: 10.1109/SCOPES.2016.7955624Pages:1164-1169.

[7] Rina Mishra , Praveen Bhanodiya "A Review on Steganography and Cryptography" IEEE 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) DOI: 10.1109/ICACEA.2015.7164679, Pages: 119 - 122

[8] M.Saritha, Sushravya.M, Vishwanath.M.Khadabadi. "Image and Text Steganography with Cryptography using MATLAB",2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES) , ISBN: 978-1-5090-4621-8 , DOI: 10.1109/SCOPES.2016.7955506, Pages: 584 – 587

[9] Rina Mishra , Praveen Bhanodiya "A Review on Steganography and Cryptography" IEEE 2015 International Conference on Advances in Computer Engineering and Applications (ICACEA) DOI: 10.1109/ICACEA.2015.7164679, Pages: 119 – 122

[10] .Dr .Souvik bhattacharya, Dr Indradeep Banerjee, Dr Gautam Banyal "Bengali Steganography with a Novel Bengali Word processer" Research get https://www.researchgate.net/figure/236953226_fig2_Figure-2-Generic-form-of-Text-Steganography [Accessed:22-9-2017]

[11] R. Kumar, S.Chand ,S. Singh,"A high Capacity Email Based text steganography scheme using Huffman compression"IEEE 2016 International Conference on Signal Processing & Integrated Networks ,DOI:10.1109/SPIN.2016.7566661, Pages:123-129

[12] X.M. Sun,G. Luo,G. Haung "Component Based Digital Watermarking of Chinese Text" ACMISBN:1-58113-955-1 Pages:76-81

[13] Zhi-Hui Wang, The Duc Kieu, Chin-Chen Chang "Emoticon based text steganography in chat"IEEE 2010 Computational Intelligence and Industrial Applications, 2009. PACIIA 2009. Asia-Pacific Conference on DOI: 10.1109/PACIIA.2009.5406559 Pages:457-460