Survey on Securing Data using Text Steganography & Cryptography

Dhiral G.Parghi[1], Krunal Panchal[2]

[1]Research Scholar, Post Graduate Department, L.J. Institute of Engineering & Technology, Gujarat, India
[2]Assistant Professor, Post Graduate Department, L.J. Institute of Engineering & Technology, Gujarat, India

ABSTRACT

In current era of information technology, it is difficult to secure information from unlawful activities because of these reasons different strategies like Cryptography & Steganography are used .Cryptography is an area to encrypt & decrypt information & Steganography is methodology to hide the existence of a message from user eyes. By using Cryptography we can convert the original message into unreadable form & By Applying Text Steganography message can be hidden inside text cover message so both techniques can help to increase security of a message. In this paper we have mention some of text Steganography techniques and related work that had done to secure data using text Steganography.

Keywords: *Text Steganography, Cryptography, Data Security.*

1. INTRODUCTION:

With the development of computer & its use in different area of life & work the issue of securing information has gained special significance .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.

I. Text Steganography

Text Steganography is a technique of hiding a message over text cover medium. Advantage of preferring text Steganography over other Steganography is its smaller memory requirement and simpler communication. It is most difficult Steganography because of lacking of redundant bit in text file compare to audio and Image file.

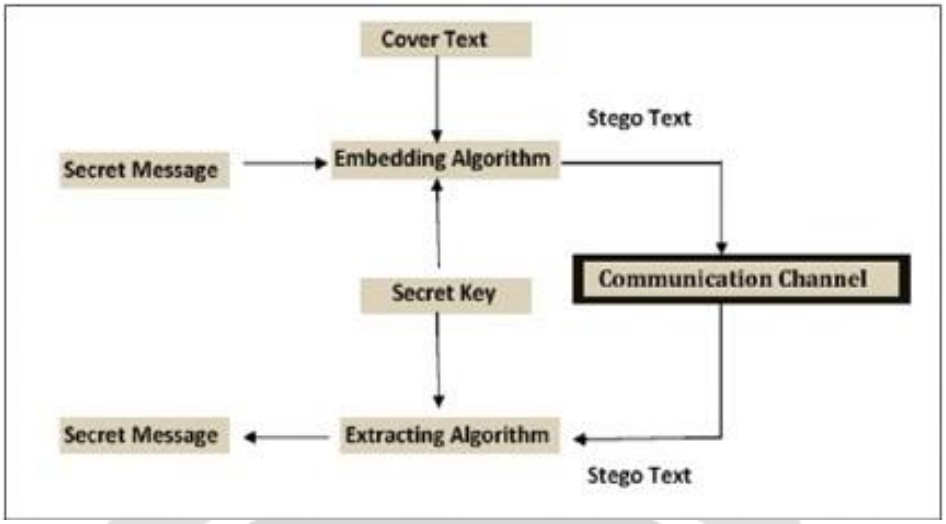

Fig 1.Generic Text Steganography model [9]

In Text Steganography Secret message is embedded into Cover text by using Embedding algorithm and generated Stego text is transfer to receiver via Communication channel. User who has a Secret key for extracting algorithm only can extract the secret message from Stego text. So for other users the Stego text is looks like a normal text message or content and secret message is transfer between two users.

II. Types of Text Steganography

Text Steganography mainly classify into 3 types:

a. Format based :
It uses a physical formatting of a space to hide the secret information. Like line shifting & word shifting. It changes the word horizontally, lines vertically and adjusts distance between words to hide data.

b. Random and statistical base:
This method generates cover text according to statistical property of text like character sequence and word sequence. This method use example grammars to produce cover text in natural language.

c. Linguistic method:
It uses linguistic property of text. It is combination of syntax and semantic methods. In syntax it checks that sentence structure is syntactically correct or not & in semantic it assigns values to synonyms of secret text & hides it into cover text.

III. Cryptography

Cryptography involves creating written or a generated code that allows information to be kept secret [10] .Cryptography is a technique where the existence of a message is not concealed although format of a message is not concealed by eavesdropper [3] .Cipher text generated after cryptography is visible to everyone so it shows suspiciousness of having secret information.

Cryptographic algorithms are divided into three groups

a. Symmetric encryption:
It is form of encryption in which encryption and decryption are performed using the same key [10].It is also called as traditional encryption algorithm. Using single key shared by sender and receiver & decryption algorithm original message can be regenerated from cipher text. Examples: AES, DES

b. Asymmetric encryption:
It is form of encryption in which encryption and decryption is performed using two keys- public key and private key. It is also known as public key encryption algorithm. Using paired key and decryption algorithm original message can be regenerated from cipher text. Example: RSA

c. Hash function:

It maps a variable length message into fixed length value [10].hash functions are not using any key but it creates a fixed length hash value from a message so it is not possible to recover a message or length of a message. So it is use determine whether data is changed or not. Example: SHA

2. RELATED WORK:

2.1 A high capacity text Steganography schema based on LZW compression and color coding.

Authors [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.

2.2 An unique data security using text Steganography.

In this research Authors [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.

2.3 Developing an efficient solution to information hiding through text Steganography along with cryptography.

In these paper Authors [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.

2.4 ECR (Encryption with cover text & Reordering based text Steganography).

In this paper Authors [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.

2.5 Text Steganography based on feature Coding method.

In this paper Authors [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.

2.6 A Novel Approach of secret message passing through text steganography.

In this paper Authors [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.

3. Comparative Study

We have Analysis and compare the existing approaches in the Table 1.

	Title	Method	Advantages	Disadvantages
1	A high capacity text Steganography schema based on	Format based text Steganography with	Increase embedding capacity & reduce	Not secure

	LZW compression and color coding.	LZW compression	computational complexity	
2	An unique data security using text Steganography.	Font & color based text Steganography with XOR operation	Require less memory	Size of cover text is increased, less secure
3	Developing an efficient solution to information hiding through text Steganography along with cryptography.	Format based Text Steganography with DES Encryption	High security because of DES	Computational time is high
4	ECR (Encryption with cover text & Reordering based text Steganography).	XOR encryption with text Steganography	hiding message in fix cover text & take less time for encryption & decryption	Less Secure
5	Text Steganography based on feature Coding method	Feature coding and random character generation Steganography	Data hiding capacity is increase	Not secure
6	A Novel Approach of secret message passing through text steganography	Text steganography with number system representation	Not using any traditional steganography method. Can use with cover message of any language	Data can hide as number system only so data hiding capacity is low. Not secure.

TABLE1: Comparison of existing approach

4. CONCLUSION:

In this paper we have discuss text Steganography model and different types of text Steganography methods & Cryptography. Different researchers has used different approaches and modified them to provide higher level of security and to increase data hiding capacity of traditional Steganography method. Comparative study shown in table 1 gives us an advantages and disadvantages of the research work & as we can see these methods is still suffering from having lower level of security, low data hiding capacity & larger cover size that shows a requirement for research in these areas.

5. REFERENCES:

Papers

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

Website

9. https://www.researchgate.net/figure/236953226_fig2_Figure-2-Generic-form-of-Text-Steganography [Accessed:22-11-2017

Book

10. William Stallings, fifth edition;"Cryptography and network security" Pearson, Pages:32,56,352