International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 7 ǁ July 2022 ǁ PP. 16-18

A Review Paper on Text steganography

Samruddhi Deshmukh
UG Student
Government College of Engineering Amravati (Electronics and TelecommunicationDepartment)

Mitalee Manware
UG Student
Government College of Engineering Amravati (Electronics and TelecommunicationDepartment)

Radhika Chhablani
UG Student
Government College of Engineering Amravati (Electronics and TelecommunicationDepartment)

Shweta Meshram
Assistant Professor
Government College of Engineering Amravati (Electronics and Telecommunication Department)

Abstract:*When a data or an information is transferred over a media there is a lack of security. Steganographyis a technique for concealing data. Over a past few decades many methods have been developed for achieving the steganography. This paper provides the study of steganographic techniques from year 2016.*

Date of Submission: 18-06-2022 Date of acceptance: 02-07-2022

I. Introduction:

Security is main concern nowadays and this can be achieved using cryptography and steganography. Cryptography is a process where a secret message in converted into unreadable format. Then the unreadable format is transferred from sender to receiver. Thus, in cryptography there is encryption of information in sender's side and decryption happens on the receiver side. But here in cryptography doubt arises that some information is shared. Steganography is then coming into limelight. It eliminates the traces that some data is shared. Steganography hides the information in any form of media. A secret message or data is hidden into another form of data. It is used for security purpose as only intendent recipient gets the secret message. Many a times a combination of cryptography and steganography is used for better security. Various methods in steganography differ from each other by the embedding capacity of the secret data.

Types of steganography:

A. Steganography of images: Here, in this type of steganography, secret image is embedded into an image. The stego-image is then transferred over.

B. Steganography in Audio: In this type of steganography, secret message in embedded into an audio signal. Here the cover medium is an audio.

C. Steganography in Video: In this type of steganography, secret message is embedded into an video and then the video is shared.

D. Text steganography:In this type of steganography, secret message is embedded into the text. Text is the cover medium in this steganography.

II. Literature Review:

The Huffman compression, which has a reversible property, was combined with an email-based text steganography system in [1]. The email IDs are divided into a group of email addresses with four characters before the "@" sign. The sender and recipient of the mail share this. The set of second portions of email IDs, such as gmail.com, yahoo.com, etc., are then concealed in the secret message. The extra characters that are added in order to meet the requirements of secret data bits are also taken from the secret data. As a result, the hiding capacity is improved without increasing the cover text's overhead. A statistical text steganography method that combines steganography and cryptography to guarantee secure data transmission was suggested in [2].

In order to use the suggested method, Data Encryption Standard (DES) is used. By moving the concealing bit, which is based on how frequently letters appear in the cover text, the encrypted data is concealed. The security of the proposed algorithm's output was examined once these two mechanisms were put into place by putting the output to a number of tests.

a number of different cyber-attacks. The analysis's findings suggest that the algorithm contributes to high levels of data security. Using colour coding and the Lempel-Ziv-Welch (LZW) compression technique, Aruna et almodel .'s was suggested by them [3]. The approach used the forward mail as a cover medium to hide the secret information.After first compressing the secret information, the method conceals it in the email addresses and the email's cover message. The cover text (or message) is coloured using a color-coding table, which embeds the secret data bits within it. The study's findings showed that the technique was less computationally complex than previous methods and had a higher embedding capability. Utilizing stego keys also significantly improves the security of the suggested method.

A statistical text steganography method based on the HC and MC model was proposed in [4], and it can automatically synthesise steganographic text. With regard to secret information that needs to be integrated, it can automatically build fluid text carriers. The suggested approach creates a good approximation of the statistical linguistic model by learning from a number of public samples. Results of the experiments indicate that the recommended model performs more effectively in terms of information hiding than any of the equivalent strategies used before. Similar work was done in [5], where the covert message is concealed in a large number of email addresses created by the email body. The suggested method compresses the concealed message using lossless LZW compression techniques.The level of security using the proposed method is further enhanced by the use of various stego keys. The proposed method, which was also applied in another study, was demonstrated to significantly boost the hiding capability for a generic sample. Using single bit rules based on the MC model, a coverless statistical steganography method was given in [5]. Using this method, the model is made to allow the hidden data to travel through it, and the associated steganographic contents are then produced. The goal of developing steganographic text that more closely resembled the training text was to emphasise the importance of transition probability and utilise it to its fullest extent during the text production process.

Maximum variable bit embedding, as opposed to traditional fixed bit embedding, is used in the procedure. This method does not insert a single piece of secret information into each word of the text. The proposed strategy has a good ability to conceal, according to the results of the experiments. However, it fell short of the variable bit embedding strategy employed in the earlier technique.The statistical text steganography method Wu et al. [6] proposed increases the hidden message capacity. In order to achieve this, a mapping between character sequences' ASCII values and corresponding binary values is used to create metadata and insert header information in the first few bytes of the cover contents. The next step is to optimally process and store the secret message in cover bits so that it may be evaluated by looking at its character sequences. By using synonym replacement, a unique technique to improve the embedding capability of linguistic steganography was proposed in [7].The change-tracking procedure was altered to use HC to conceal the message inside MS Word files. Commonly used synonyms regularly conceal information and dispel suspicion to guarantee that a third party is ignorant of the existence of a communication. The study in [8] is focused on frequency modulation techniques. Character spacing and font characteristics are used to encrypt information. One out of every three characters is frequently hidden using this strategy. There are eight different ways to conceal one character and improve embedding capacity given this coding frequency.

Literature Review on related works on text steganography

Author Name	Published date	Technique used	Improvement
Kumar, R.; Malik, A.; Singh, S.; Chand, S	2016	A high-capacity email-based text steganography scheme using Huffman compression	Capacity
Bhat, D.; Krithi, V.; Manjunath, K.N.; Prabhu, S.; Renuka	2017	Information hiding through dynamic text steganography and cryptography	Security
Malik, A.; Sikka, G.; Verma, H.K.	2017	A high-capacity text steganography scheme based on LZW compression and color coding	Security
Yang, Z.; Jin, S.; Huang, Y.; Zhang, Y.; Li, H.	2018	Automatically generate steganographic text based on Markov model and Huffman coding	Capacity
Fateh, M.; Rezvani, M.	2018	Email-based high-capacity text steganography using repeating characters	Capacity
Wu, N.; Shang, P.; Fan, J.; Yang, Z.; Ma, W.; Liu, Z.	2019	Research on coverless text steganography based on single bit rules	Capacity
Jayapandiyan, J.R.; Kavitha, C.; Sakthivel, K.	2020	Enhanced least significant bit replacement algorithm in the spatial domain of steganography using character sequence optimization	Capacity
Mahato, S.; Khan, D.A.; Yadav, D.K.	2020	A modified approach to data hiding in Microsoft word documents by Change-tracking technique	Capacity

Shah, S.T.A.; Khan, A.; Hussain, A	2020	Text steganography using character spacing after normalization	Capacity

III. Conclusion:

This paper provides the study of various techniques on text steganography. Here the improvement in each method is described. Steganography has become an important technology for mankind as security has always been the concern. From the above study it is observed that Security and capacity has been improving day by day. Thus, giving us the best result on steganography.

References:

[1]. R. Kumar, A. Malik, S. Singh and S. Chand, "A high capacity email based text steganography scheme using Huffman compression," 2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN), 2016, pp. 53-56, doi: 10.1109/SPIN.2016.7566661.

[2]. D. Bhat, V. Krithi, K. N. Manjunath, S. Prabhu and A. Renuka, "Information hiding through dynamic text steganography and cryptography: Computing and Informatics," 2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2017, pp. 1826-1831, doi: 10.1109/ICACCI.2017.8126110.

[3]. A high capacity text steganography scheme based on LZW compression and color coding Author links open overlay panelArunaMalikGeetaSikkaHarshK.Verma

[4]. Automatically Generate Steganographic Text Based on Markov Model and Huffman CodingZhongliang Yang, ShuyuJin, Yongfeng Huang, Yujin Zhang, Hui Li

[5]. Fateh, M.; Rezvani, M. An email-based high capacity text steganography using repeating characters. Int. J. Comput. Appl. 2021, 43, 226–232.

[6]. Wu, N.; Shang, P.; Fan, J.; Yang, Z.; Ma, W.; Liu, Z. Research on coverless text steganography based on single bit rules. J. Physics Conf. Ser. 2019, 1237.

[7]. Jayapandiyan, J.R.; Kavitha, C.; Sakthivel, K. Enhanced least significant bit replacement algorithm in spatial domain of steganography using character sequence optimization. IEEE Access 2020, 8, 136537–136545.

[8]. Mahato, S.; Khan, D.A.; Yadav, D.K. A modified approach to data hiding in Microsoft Word documents by change-tracking technique. J. King Saud Univ.-Comput. Inf. Sci. 2020, 32, 216–224.

[9]. Shah, S.T.A.; Khan, A.; Hussain, A. Text steganography using character spacing after normalization. Int. J. Sci. Eng. Res. 2020, 11, 949–957.

[10]. abdul.m, Mohammed &Sulaiman, Rossilawati&Shukur, Zarina & Hasan, Mohammad. (2021). A Review on Text Steganography Techniques. Mathematics. 9. 2829. 10.3390/math9212829.