International Journal of Scientific Research in Science and Technology
Print ISSN: 2395-6011 | Online ISSN: 2395-602X (www.ijsrst.com)
doi : https://doi.org/10.32628/IJSRST

A Survey of Text Steganography Methods

Vivek Sharma S[1], Monika Raj[2], Swathi S[2]

[1]Assistant Professor, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

[2]B.E Student, Nagarjuna College of Engineering and Technology, Bangalore, Karnataka, India

ABSTRACT

Article Info
Volume 8, Issue 3
Page Number : 238-241

Publication Issue
May-June-2021

Article History
Accepted : 14 May 2021
Published : 22 May 2021

Phishing is that the most typical and most dangerous attack among cybercrimes. The aim of these attacks is to steal the data that's utilized by people and organizations to perform transactions or any vital info. The goal of this is often to perform an Extreme Learning Sending encrypted messages frequently will draw the attention of third parties, i.e. hackers, perhaps causing attempts to break and reveal the original messages. In a digital world, steganography is introduced to hide the existence of the communication by concealing a secret message inside another unsuspicious message. This paper presents an overview of text steganography and a brief history of steganography along with various existing text-based steganography techniques.

Keywords : Steganography, data hiding, steganography text in text, media, information, security.

I. INTRODUCTION

Steganography is the art of hiding data or information in ways that prevent the detection of hidden messages. In computing a computer files, message, image or video is concealed within another file, message, image or video. The historic use of steganography is the concealing of communications. This has been accomplished in a number of ways from microdot printing and invisible ink to spread spectrum communications. This differs from cryptography in that cryptosystems assume that the enemy can access and modify the communication if possible. Steganography can augment cryptography by obscuring communication and prevent the enemy from knowing a communication is even being sent. However, it should not be considered a replacement for cryptography. Using computers to hide data or information on a hard drive is easily done with free tools. The world of computing has developed some interesting applications for steganography that instead of hiding information seeks to fingerprint or watermarking. These techniques can be used to protect distributed intellectual property such as films, audio recordings, books, and multimedia products by embedding copyright information.

Basic theory - This section will focus on the history of steganography, steganography on text, text steganography methods, mechanism of text steganography.

II. HISTORY OF STEGANOGRAPHY

The first recorded uses of steganography can be traces back to 440 BC when Herodotus mentions two examples in his Histories. Histiaeus sent a message to his vassal, Aristagoras, by shaving the head of the his most trusted servant, marking the message onto his scalp, then sending him on his way once his hair had regrown, with the instruction, when thou art come to Miletus, bid Aristagoras shave thy head, and look thereon. Additionally, demarcates sent a warning about a forthcoming attack to Greece by writing it directly on the wooden backing of a wax tablet before applying its beeswax surface. Wax tablets were in common use then as reusable writing surfaces, sometimes used for shorthand. Steganography has been widely used for centuries. Here are some examples of hidden messages within a wax tablet: in ancient people wrote messages on wood and covered it with wax bore an innocent covering message. Hidden messages on paper written in secret inks, under other messages or on the blank parts of other messages. Messages written in Morse code on yarn and then knitted into piece of clothing worn by a courier. Messages written on envelopes in the area covered by postage stamps. In the early days of the printing press, it was common mix different typefaces on a printed page because the printer did not have enough copies of some letters in one typeface. Thus, a message could be hidden by using two or more different typefaces, such as normal or italic. During and after World War II, espionage agents used photographically produced microdots to send information back and forth. Microdots were typically minute, approximately less than the size of the period produced by a typewriter WWII microdots needed to be embedded in then paper and covered with an adhesive. This was reflective and thus detectable by viewing against glancing light. Alternative techniques included inserting microdots into slits cut into the edge of post cards. During the American Revolutionary War both the British and American forces used various forms of Invisible Inks. Invisible Ink involved common sources, this included milk, vinegar, fruit juice, and urine, for the hidden text. To decipher these hidden messages required light or heat. Null ciphers were also used to pass secret messages. Null ciphers are unencrypted messages with real messages embedded in the current text.

The types of steganography are: -

Text Steganography: In the steganography algorithm that uses text as its insertion medium usually used technique is Natural Language Processing (NLP), so that, the text that has been inserted secret messages will not be suspicious to the person who saw it.

Video Steganography: Process of authenticated communication by hiding secret data form unauthorized user(s) through a video file as a cover medium.

Image Steganography: This is most commonly used format because this format is one file format that is often exchange in the internet world.

Audio Steganography: Voice formats are often used because usually files with this format are relatively large. So can accommodate a large number of secret messages as well.

III. TEXT STEGANOGRAPHY

It hides the text behind some other files. Changing the format of an existing text within a file, to change the words within the text or to generate random character sequences. Basically we use text file as cover media to embed the secret information. It is more vulnerable to attack as it can be easy for an attacker to detect the pattern, text steganography itself has this following three categories such as:

a. **Format Based Methods** - in this method text data is embedded in the carrier text by changing the format ofthe cover text itself.

b. **Linguistic Methods** - in this method just doing analysis the linguistic.

c. **Random and Statistical generation methods** – generating its carrier text according to the statistical and embedding the information in randomsequence of characters.

Text steganography is the most difficult kind of steganography because a text file lacks a large scale redundancy of information in comparison to other digital medium like image, audio and video. Many languages are used to hide data like Persian, Arabic, Hindi, English etc. There is characteristic of English language such as inflexion, use of periphrases and fixed word order. Conversion means that with minimum change of the word will make the relationship of the words into a sentence may be indicated.

IV. TEXT STEGANOGRAPHY METHODS

There are various techniques of text steganography:

a. **Selective Hiding** – hides the character on the first or any other specific location characters of the words to combine the character and helps to extract the text. This technique requires huge amount of plain text.

b. **Hiding Using Whitespaces** -Smaller number of whitespaces between words can be determined that whitespace is 0, but if more numbers of whitespaces betweenwords may determine 1.

c. **HTML Web Pages** – Hide the text by using the attributes in HTML, the character is then used to retrieve the original text.

d. **Semantic Hiding** – Uses synonyms to hide the message.

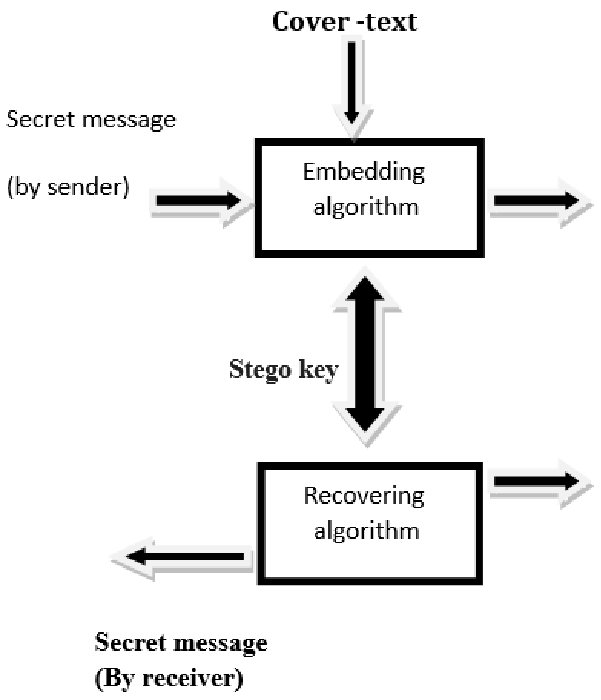

Fig. 1 : The Mechanism of TextSteganography

Secret message (By receiver)

Figure 1 shows the basic text steganography mechanism. Firstly, a secret message (or an embedded data) will be concealed in a cover- text by applying an embedding algorithm to produce a stego-text. The stego-text will then be transmitted by a communication channel, e.g. Internet or mobile device to a receiver. For recovering the secret which sent by the sender, the receiver needs to use a recovering algorithm which is parameterized by a stego- key to extract the secret message. A stego- key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to parties who know it.

V. REFERENCES

[1]. Gupta, S. and R. Jain, 2015. An innovative method of Text Steganography. Proceedings of the 2015 3rd International Conference on Image Information Processing (ICIIP'15), December 21-24, 2015, IEEE, Waknaghat, India, pp: 60-64

[2]. Mandal, K.K., A. Jana and V. Agarwal, 2014. A new approach of text Steganography based on mathematical model of number system. Proceedings of the 2014 International Conference on Circuits, Power and Computing Technologies (ICCPCT'14), March 20-21, 2014, IEEE, Nagercoil, India,pp: 1737-1741.

[3]. Jaeyoung Kim, Hanhoon Park, Jong-Il Park, "Image Steganography Based on Blcok Matching in DWT Domain".