*Research Exhibition in Mathematics and Computer Sciences (REMACS 6.0)/*
*ISBN: 978-629-97440-5-4*

# ANALYZING THE PERFORMANCE OF INTEGERS BASED TEXT STEGANOGRAPHY PROTOTYPE

Saiyyidah Nafisah Bakri and Muhamad Arif Hashim
*College of Computing, Informatics and Mathematics,*
*Universiti Teknologi MARA, Perlis Branch*
*saiyyidahbakri@gmail.com, and muhamadarif487@uitm.edu.my*

**ABSTRACT** – Information security is the technique of preventing digital data from being accessed by unauthorized parties, being corrupted, or being stolen at any point in its lifecycle. Information security can be divided into two categories; Cryptography and Information Hiding. There are two types of information hiding, which are watermarking and steganography. This research is focusing on steganography, which is a technique that involves encrypting data inside multimedia files, sometimes known as cover files, to hide the existence of sensitive information. The hidden information can only be accessed and retrieved by the intended receiver, who is aware that it is included in the cover file. Within a range of multimedia files, including music, video, and photos, the steganography approach can be applied. The objective of this research is to develop a text steganography based on integers. It is also to identify the amount of hidden space when using a text cover file. Other than that, the performance of the developed text steganography prototype will be evaluated by the end of the research.

**Keywords:** Steganography, Data Hiding, Text Steganography, Hidden Message, Cover Text File

## 1. INTRODUCTION

Steganography is a method of hiding sensitive information by encrypting it within multimedia files, like images, videos, or audio. Only the intended recipient, who knows where the hidden message is located, can access and extract the information. Text steganography specifically hides secret messages within cover texts using linguistic rules, structure, and other characters. There are two types: word-rule based and feature-based. Word-rule based approaches use line-shift coding to hide messages vertically within the text, calculating positions based on distances between texts. Feature-based approaches alter letter size, form, and placement to make them less noticeable within the text structure. The cover text containing the hidden message is called stego text and is sent to the recipient, who can extract the message without others knowing.

## 2. METHODOLOGY

The development of the integers based text steganography prototype involved the design and implementation of text steganography specific in hiding the integers. Jupyter Notebook was used with Python language to create the prototype by implementing encoding and decoding hidden messages into the cover text file. The data entered was embedded in the cover text file and by decoding the hidden data, the user can retrieve the hidden message. Other than that, GUI was used to create interfaces for the text steganography. The user can easily use the prototype to create a stego file and send the important data to another person. The stego file contains important messages to receive by the receiver securely with interruption from the intruder.

## 3. RESULTS

As the prototype has been developed, the testing was done by encoding the hidden message into the cover text file. The testing began by inserting different numbers of input (integers) into the cover text file (.txt) to analyze how many integers can be hidden and where the hidden message has been encoded in the cover text file. The figure 1 below shows the comparison of the original cover text file and the cover text file that have 10 numbers of integers. It displays two cover text files: the left one is the original file (37,000 bytes), while the right one contains an encoded message. The hidden message consists of 10 integers (260 bytes) placed at the beginning of the text. The message is encoded as unreadable words to prevent unauthorized access and data theft.

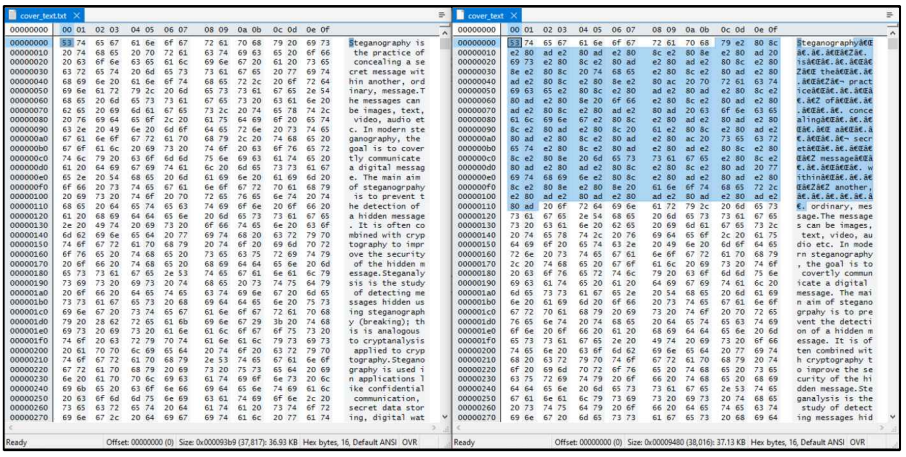

**Figure 1.** Comparison cover text file

## 4. NOVELTY OF RESEARCH / PRODUCT

As for the research on steganography, the text steganography that has been done was combining all the types of text. The integers based text steganography prototype was focused on embedding the integers into the cover text file. The performance of the prototype was analyzed to find the size of integers encoded into the text file. The capacity of the stego file and the hidden data was calculated. There is the difference of the size of the cover text file before and after embedding the hidden data which are without and with spacing between the digits.

## 5. CONCLUSION

What this study reveals is, the research of text steganography is a secure technique in transferring data from the sender to the receiver. With the hidden message that has been encoded, even when the attacker interrupts the transaction of the data, it cannot retrieve the important data. So that, the messages are well secured and the attacker would not be able to access and make alteration on the messages. The message will safely arrive to the receiver.

## REFERENCES

Majeed, M. A., Sulaiman, R., Shukur, Z., & Hasan, M. K. (2021). A Review on Text Steganography Techniques. *Mathematics*, *9*(21), 2829. https://doi.org/10.3390/math9212829

Mohd Hilal Muhammad, Hanizan Shaker Hussain, Din, R., Samad, H., & Sunariya Utama. (2023). Review on feature-based method performance in text steganography. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 427–433. https://www.beei.org/index.php/EEI/article/view/2508/1908

Mshir, S., & Varol, A. (2019). A New Model for Creating Layer Planes Using Steganography for Text Hiding. *2019 7th International Symposium on Digital Forensics and Security (ISDFS)*. https://doi.org/10.1109/isdfs.2019.8757498