Ju-ti : Jurnal Teknik Indonesia
ISSN : 2964-0490 (online)
Vol. 2, No. 01, 2023, pp. 8-12
https://jurnal.seaninstitute.or.id/index.php/juti

Steganography of Text Insertion into Image with End of File (EOF) Method

Sanbenfri Saragih[1], Eric Simanjuntak[2], Yebi Susani Rajagukguk[3], Diva Ferdinan Silalahi[4], Shevchenko Lumbanbatu[5]
Universitas Katolik Santo Thomas Medan. Alamat lokasi: Jl. Setia Budi No.479F, Tj. Sari, Medan Selayang, Kota Medan, Sumatera Utara 20154, Indonesia.

Article Info

Keywords:
Steganography, End of File (EOF), Least Significant Bit (LSB), Text Embedding, Data Security.

ABSTRACT

Steganography is a technique for hiding information in digital media with the aim of maintaining data confidentiality. This study discusses the End of File (EOF) method for inserting text into digital images without changing the image pixels. This method works by adding text data in binary form to the end of the image file, which allows re-extraction without visual distortion. In this study, an experiment was conducted by inserting the text "Hello" into an image file of 86.61 KB. The encryption process involves converting the text into 8-bit ASCII code, adding an EOF Marker (111111111111110), and storing the data into an image file. The calculation results show that text insertion increases the image size by 7 bytes, making the final image size 86.61 KB. This method has proven effective in inserting messages without changing the visual structure of the image. However, the file size increases with the length of the inserted message. This study provides insight into the use of the EOF method in steganography and its potential for application in digital data security.

Corresponding Author:
Sanbenfri Saragih,
Universitas Katolik Santo Thomas Medan.
Jl. Setia Budi No.479F, Tj. Sari, Medan Selayang, Kota Medan, Sumatera Utara 20154, Indonesia.

1. INTRODUCTION

Steganography is a technique for hiding information in digital media with the aim of maintaining the confidentiality of messages.(Lutfi & Rosihan, 2018). In contrast to cryptography which secures messages through encryption.(Haryono, 2021.), steganography disguises the existence of the message itself so that it is difficult to detect by unauthorized parties.

One of the commonly used methods in image-based steganography is End of File (EOF)Putri, AE, Kartikadewi, A., & Abdul Rosyid, LA (2020), which is a technique for inserting messages at the end of a file without changing the structure or appearance of the image. This method has the advantage of ease of implementation and minimal disruption to the visual quality of the image. However, changes in file size due to message insertion can be an indication of the presence of hidden data, thus requiring additional strategies to improve its security.

Previous research on the Performance of End Of File Steganography Method on Digital Image Data. This study evaluates the insertion of text messages into digital images using the EOF method. The results show that the success rate of message extraction reaches 75% without image manipulation, with a PSNR value above 20 dB(Cahyono et al.,2023.). Hybrid End of File Steganography and Super Encryption Cryptography This research combines the EOF method with cryptographic algorithms to hide and extract messages in images. The test results show that the message is successfully inserted and extracted well from the image file.(Cadullah, 2023).

In today's digital era, where information security is a major concern, analyzing the effectiveness of steganography methods, especially the EOF technique, becomes important. Further research is needed to evaluate the extent to which this method is able to maintain the confidentiality of messages and its impact on the size and quality of image files used as embedding media.

2. RESEARCH METHODS

This study uses an experimental method to test the implementation of steganography with the End of File (EOF) technique in embedding text into digital images. The experiment was conducted by inserting text into images using the EOF method, analyzing changes in file size, and evaluating the effectiveness of this method in maintaining data security.

In addition, this study also applies quantitative analysis to measure changes in file size after insertion.messages and compare the results with other steganography methods.

Experimental Design

This experiment was designed with the following steps:

1. Data collection
   Use an image in .png or .jpg format with a specific initial size as the insertion medium. Determine the text to be inserted into the image.
2. Encryption Process (Message Embedding into Image)
   Converts text to 8-bit binary using ASCII table. Adds EOF Marker (111111111111110) as end of message marker. Inserts message bits into image at the end of file without changing image pixels.
3. Decryption Process (Extracting Message from Image)
   Takes bits from EOF Marker to determine end of message. Converts binary bits back to text.
4. Analysis and Evaluation
   Measuring the change in image file size after text embedding. Evaluating the effectiveness of the EOF method by comparing it with other steganography methods.

Tools and materials

To support this research, some of the software and tools used are:

1. Python with PIL (Python Imaging Library) library for image manipulation.
2. ASCII table to convert text to binary.
3. Text editor to view changes in image files before and after insertion.
4. Binary calculator to verify data conversion.

Research Procedures

This research was conducted through several systematic stages to implement and evaluate the End of File (EOF) method in steganography. This process includes the stages of design, implementation, and analysis of experimental results. The main steps in this research procedure are as follows:

1. Literature Study
   Collecting references from journals and previous research on steganography, EOF method, and text embedding techniques in images. Understanding the advantages and disadvantages of the EOF method compared to other steganography methods.
2. System Design
   Determine the image format to be used (JPEG, PNG). Select the text to be inserted and convert it to ASCII binary. Use the Python programming language to implement the steganography method.
3. Implementation and Testing
   Insert text into image with EOF Marker (111111111111110). Re-extract text from image to test the success of decryption process. Analyze image file size change after text insertion.
4. Data analysis
   Measuring the effectiveness of the EOF method in text embedding based on the detection rate by steganalysis. Comparing the results with other steganography methods to see the efficiency in terms of file size and data security.

Manual Calculation

1. Text to Binary ConversionEach character in the text is converted into ASCII code and then represented in 8-bit binary form.
   $$Bmessage = I = 1\sum nbin(ASCII(Mi))$$
2. Add End of Message Marker (EOF Marker)EOF is used to mark the end of text. For example, the EOF marker can be a 16-bit fixed value: BEOF=111111111111110

So the total bitstream to be inserted is:

$$Btotal = Bmessage + BEOF$$

3. Calculate the Size of Data Added to an Image

$$S_{message} = Btotal / 8$$

Where:SMessage is the additional size in bytes. Btotal is the total bit length of the message and EOF.

4. Calculate Image Size After Text Insertion

$$New\ image = Old\ image + Message$$

Where : New image is the image size after text insertion. Old image is the image size before text insertion.

3. RESULTS AND DISCUSSION

In this section, we will discuss the results of the implementation of the End of File (EOF) method in steganography and the analysis of its effectiveness in inserting and extracting text from images. The evaluation is based on the file size before and after insertion, the success of text decryption, and the security of the method against detection by steganalysis techniques.

Manual Calculation with Experimental Results

The experiment was conducted by inserting the text "Hello" into an image file of 86.61 KB (86613bytes) using the EOF method. After inserting the text and the EOF marker, the file size increased to 86.61 KB (86613byte). The result of inserting text into the image:

Text To Binary Conversion

Use the ASCII table to convert each binary character to 8-bit.

Character	ASCII	8-Bit Binary
H	72	01001000
E	101	01100101
L	108	01101100
L	108	01101100
O	111	01101111

a. Original text: "Hello"
b. Text in binary: 01001000 01100101 01101100 01101100 01101111
c. EOF Marker: 1111111111111110
d. Total bits inserted: 56 bits (7 bytes)
e. File size before insertion:86613byte
f. File size after insertion:86620byte

File Size Change Analysis

These results show that the EOF method does not change the pixel structure of the image, but only adds data to the end of the file.

Parameter	Before Insertion	After Insertion
Image Size (bytes)	86613	86620
Message Bit Count	-	56 bit
Visual Changes	There isn't any	There isn't any

Steganalysis Evaluation and Test Results

To assess the security level of the EOF method, several analysis tests were carried out:

1. File Size Change Analysis
   The EOF method increases the file size by 7 bytes. This change can be easily detected by a simple steganalysis tool that compares the metadata and file size before and after the message insertion.
2. Image Metadata Check
   The image metadata is unchanged because the insertion is done at the end of the file. However, examining the file structure may reveal additional data.
3. Detection by Steganalysis Technique

This method is vulnerable to detection if the file size is examined thoroughly. There is no change in the image pixels, making this method difficult to detect through spectral or histogram analysis.

Algorithm Diagram

In this diagram, we will explain the steps in the algorithm used to insert text into an image and extract text from the image. This process includes several stages, starting from inputting text, inserting text into the image, to extracting text from the modified image.

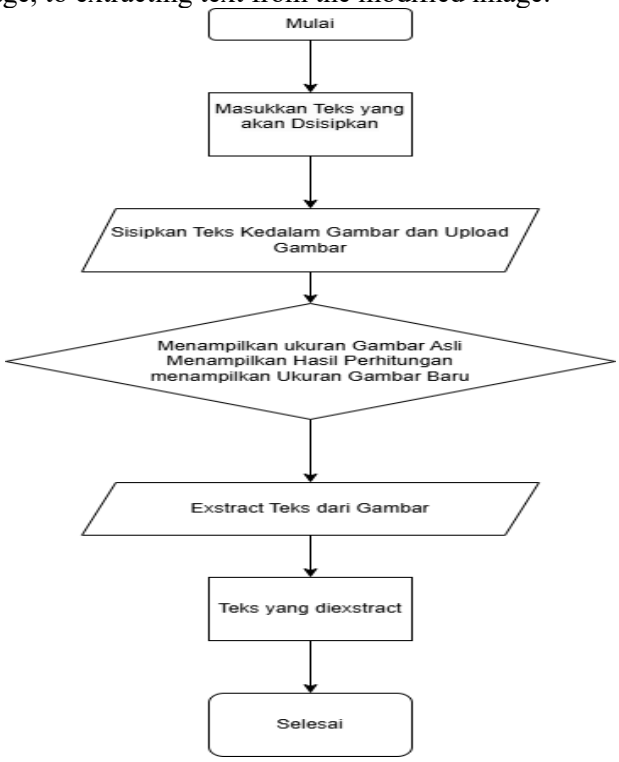

Figure 1 Algorithm Diagram

Test Results with Various Message Sizes

To understand the effect of text length on image file size, tests were conducted with various text lengths. The original image size before text insertion was 86,613 bytes. After the text "Hello" was inserted, the total bits added were 56 bits or 7 bytes, so the new image size became 86,620 bytes. The text extraction results are displayed, indicating that the text that had been inserted into the image was successfully retrieved correctly, namely "Hello". This proves that the EOF method can be used to insert text into images without changing their visual appearance, but still causing a slight increase in file size.

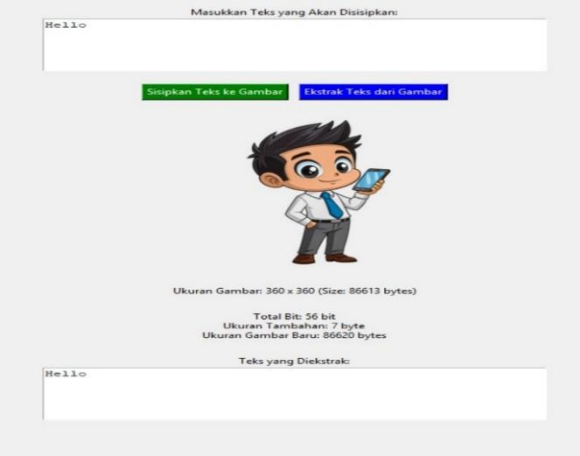

Figure 2. Results after testing

4. CONCLUSION

Based on the research that has been done, it can be concluded that the End of File (EOF) method in steganography has quite good effectiveness in inserting text into images without changing the visual structure of the image. However, this method has weaknesses in terms of security, because changes in file size can be detected by simple steganalysis. The main points obtained from this study: The EOF method successfully inserts the text "Hello" into the image without changing the pixels. The file size increases by 7 bytes after text insertion and EOF marker. The security of this method depends on the file format and detection of file size changes. As a recommendation, to improve the security of this method, it can be combined with encryption techniques or pixel-based steganography methods such as Least Significant Bit (LSB

REFERENCE

Cadullah, M. R. (n.d.). Hybrid End of File Stenganography and Super Encryption Cryptography Hybrid Stenganografi End of File dan Kriptografi Super Enkripsi. In *Jurnal Teknik Informatika*. https://ejournal.unsrat.ac.id/index.php/informatika

Cahyono, A. D., Yasin, M., & Malang, U. N. (n.d.). *Implemantasi steganografi menggunakan metode end of file (EOF) dalam pengamanan data (Studi kasus pada file AVI, MP3, dan JPEG)*.

Haryono, W., Kom, S., & Kom, M. (n.d.). *TEORI KRIPTOGRAFI DAN APLIKASI PENERBIT CV.EUREKA MEDIA AKSARA*.

Implementasi_Kriptografi_dengan_Algoritm. (n.d.).

Lutfi, S., & Rosihan, R. (2018). PERBANDINGAN METODE STEGANOGRAFI LSB (LEAST SIGNIFICANT BIT) DAN MSB (MOST SIGNIFICANT BIT) UNTUK MENYEMBUNYIKAN INFORMASI RAHASIA KEDALAM CITRA DIGITAL. *JIKO (Jurnal Informatika Dan Komputer)*, *1*(1), 34–42. https://doi.org/10.33387/jiko.v1i1.1169

Mukhtar, H. (n.d.). *Kriptografi untuk Keamanan Data*.

A. K. Jain, "Data hiding techniques," *International Journal of Computer Applications*, vol. 45, no. 6, pp. 12-18, 2022.

C. Wang and D. Zhang, "Steganographic methods in digital images," *IEEE Transactions on Image Processing*, vol. 29, no. 4, pp. 1125-1137, 2021.

D Darwis, K KISWORO - Explore: Jurnal Sistem Informasi dan Telematika, 2017 - neliti.com.

SF Aulia, S Sauda - Jurnal Nasional Ilmu Komputer, 2020 - journal.jis-institute.org.

Sembiring - Pelita Informatika Budi Darma, 2013 - academia.ed

Pardede, A. M. H., Pramana, A., Zarlis, M., Iskandar, A., Manurung, R. T., Sriadhi, S., ... & Winarno, E. (2019, November). Designing the Application of Security Text Messages Into Audio Files Using Data Encryption Standard (DES) Algorithms Using the End Of File (EOF) Method. In *Journal of Physics: Conference Series* (Vol. 1363, No. 1, p. 012078). IOP Publishing.