SCIENTIST
Journal of Security, Computer, Information, Embedded, Network, and Intelligence System

P-ISSN : 3024-8701
E-ISSN : 3024-8329

(SCIENTIST) Journal of Security, Computer, Information,
Embedded, Network, and Intelligence System
Vol. 1, No. 1, 2023

Performance Analysis of The Last Significant Bit (LSB) Method in Steganography for Data Hiding in Image Data

Fadhlirrahman Baso
Pend. Teknik Informatika dan Komputer
Universitas Negeri Makassar
Makassar, Indonesia
fadhlirrahman.baso@unm.ac.id

ARTICLE INFO

Received : 29 October 2023
Accepted : 28 November 2023
Published : 09 December 2023

ABSTRACT

Technology as a means of conveying information can have significant implications for the security and confidentiality of data and information content. When a sender wishes to convey a message to someone and does not want the message to be easily visible, the concealment of this message becomes crucial for the sender. One commonly used method for data concealment is the Least Significant Bit (LSB) method in steganography. The LSB method is preferred for its simplicity, fast process, and greater capacity. Messages are embedded by replacing the least significant bit in the host image with the message bits, with the rule that the number of message bits does not exceed the number of bits in the host image. Based on research findings, the results of steganography are difficult to distinguish from the original content through visual observation. Therefore, it can be concluded that the steganography method is highly effective for concealing a message.

Keywords: *Steganography, Least Significant Bit (LSB), Image*

ABSTRAK

Teknologi sebagai sarana untuk penyampaian informasi akan dapat menimbulkan dampak pada keamanan dan kerahasian dari isi data dan informasi. Saat pengirim ingin memberikan sebuah pesan kepada seseorang dan pengirim tidak ingin pesan yang dikirimnya terlihat begitu saja, karena hal ini penyembunyian pesan ini sangat dibutuhkan oleh pengirim. Salah satu metode untuk penyembunyian data itu ada metode Least Significant Bit (LSB) pada steganografi. Metode LSB merupakan metode yang biasanya digunakan karena lebih sederhana, prosesnya yang cepat, dan memiliki daya yang lebih besat. Pesan akan tersisip dengan melalui cara penggantian bit terakhir pada citra penampung dengan bit pesan, dengan aturan bahwa jumlah bit pada pesan tidak melebihi bit citra penampung. Dengan berdasarkan hasil penelitian, hasil steganografi jika dibandingkan dengan awalnya itu sulit untuk dibedakan melalui penglihatan mata. Sehingga dapat disimpulkan jika metode steganografi ini sangat baik untuk menyembunyikan sebuah pesan.

Kata kunci: *Steganografi, Least Significant Bit (LSB), Gambar*

I. INTRODUCTION

Data security is the most important factor in the advancement of information and communication technology. Steganography is one method that can be used for hidden communication. Steganography is the process of hiding or inserting messages using container media, or digital graphics. Steganography functions by randomly inserting messages into digital images in the form of pixel fragments. Using digital images as a storage medium has advantages, as human vision is limited in terms of color and it may be difficult to differentiate between genuine digital photos and digital images containing hidden messages[1].

The science of analyzing, investigating and creating methods to hide information is known as steganography. Steganography can be categorized as one of the fields of communication science. The Greek term "steganography" means "hidden writing". Steganography is the process and skill of hiding digital data and information behind other digital data in the digital information era, so that the digital data is practically invisible [2]. The ancient Greeks used this art and science to hide messages by tattooing the herald's bald head and then waiting for his hair to grow out[3].

The Least Significant Bit (LSB) technique is used to apply steganography to photos. It works by replacing hidden information bits with original image bits, providing output that looks identical to the original when viewed through the human senses[4].

One of the benefits of Steganography is that the Cover-Image and Stego-Image are identical to each other. Media that has information embedded in it. Secrets can be expressed verbally, visually, sonically, or visually. The possibility of spreading suspicious information through digital media exchange is low due to the large volume of media data transferred [2].

Information messages can be inserted into image files using steganography techniques such as the LSB (Least Significant Bit) approach. The bit in a binary data sequence (base 2) with the lowest or least significant value is called the least significant bit. It is located at the end of the bit sequence on the right. When entering data into other digital media, the least important bits are used[1].

II. METHODS

One of the steganography methods most commonly used to hide data in image media is the Least Significant Bit (LSB) method. Although LSB may seem insignificant, it has various uses in the digital world:

1) Data Hiding (Data Hiding)

LSB is used to hide data in other digital media, such as images, audio, or video. This process is called steganography. The hidden data can be text, images, or even other files.

Data is hidden by slightly changing the LSB value of the original digital media. These changes are so small that they are almost invisible to the human eye. However, special software can detect these changes and extract hidden data.

For example, a photographer wants to hide a secret message in a photo. The photographer changes the LSB value of some pixels of the photo. These changes are invisible to the human eye, but special software can detect these changes and extract secret messages.

2) Data Compression

LSB is used to compress digital data. This process is called dithering. Dithering works by reducing the number of bits used to represent color or value in a digital file.

LSB is most often targeted for reduction because its impact on the overall value of the file is small. This bit reduction does not significantly affect file quality, but can drastically reduce file size.

For example, an image compression program wants to reduce the size of an image file. The program analyzes the image and identifies areas where changes in LSB values would not be visible to the human eye. Then, the program reduces the LSB value in that area, thereby reducing the overall image file size.

3) Security and Forensics

LSB can be used to hide malware or viruses in digital files. This is because changes in LSB values are difficult to detect by antivirus software.

Apart from that, LSB is also used to track the source and spread of viruses or malware. This is done by adding a "digital signature" to the digital file, which is stored on the file's LSB. These digital signatures can be used to trace the origins of files and identify who created or distributed them.

For example, a cyber criminal wants to hide a virus in an image file. These criminals change the LSB values of some pixels of the image to hide the virus code. The virus can then be activated when the image file is executed.

4) Steganalysis

Steganalysis is the process of detecting and extracting data hidden in digital media. Steganalysis is used for a variety of purposes, such as criminal investigations, intellectual property protection, and cybersecurity.

Steganalysis can be carried out using statistical analysis techniques or by using special algorithms. These algorithms are designed to detect abnormal-looking patterns in digital data, which could indicate that data has been hidden.

For example, a law enforcement officer wants to detect the presence of confidential data in files confiscated from a suspected criminal. These law enforcers use steganalysis software to analyze these files and look for signs of hidden data.

Even though it has the smallest value, LSB plays an important role in several things, including:

- Determining the value of the binary number: Changing the LSB value from 0 to 1 will increase the value of the binary number by 1.
- Steganography: LSB is used in steganography techniques to hide secret data inside other files. This is done by changing the LSB value of an image or audio file without significantly affecting its quality.
- Data compression: LSB is also used in lossy data compression techniques, where less significant bits are discarded to reduce file size.
- Randomization: LSB can be used to generate random numbers by changing their values randomly.

LSB and Data Security

Because LSB can be changed easily, it is sometimes the target of attacks in the world of data security. Cybercriminals can modify LSB data to hide malware, change content, or steal information.

To prevent this, various data security techniques are implemented, such as encryption, hashing, and watermarking.

Encryption converts data into a format that cannot be read without a decryption key. This helps protect data from unwanted modifications.

Hashing is a technique that generates a unique character string from data. Each change to the data will result in a different hash, allowing detection of data manipulation.

Watermarking is a technique of embedding confidential information in data, such as a logo or digital signature. This helps to identify data owners and prevent forgery.

In images, this method uses the least significant bit of each color element (such as red, green, and blue) to input data without significantly compromising visual quality. The LSB method in steganography allows message insertion without visibly changing the digital image. This allows message insertion by replacing the last row of data bits in the image segment with the row of message bits to be inserted [3]. This method allows messages to be hidden in digital images so that they are difficult for humans to detect [5].

With the LSB method, steganography can be done by inserting data into the desired image. The process is to combine data bits into digital image bits, so that the data bits can be hidden in the digital image container bits [6].

This Least Significant Bit method is very easy and not complicated, and the hidden message is also quite safe [7]. Covertext is a type of digital image that uses the Least Significant Bit hiding technique. File pixels are each one to three bytes in size, with one byte equal to eight bits[8]. Bitmap images consist of pixels which are a collection of dots. Each image has pixels with different values [9].

The LSB Research Method for Image Data Hiding can be seen as follows[10]:

1) Data Collection

Choose datasets that have a variety of objects, backgrounds, and different levels of visual complexity when using images; for example, the ImageNet or COCO datasets provide very different sets of images.

2) Implementation of the LSB Method

The LSB method should be applied to the least important bits of image pixels. This ensures that the changed pixel values do not distort the visual structure or color of the image.

3) Performance Evaluation

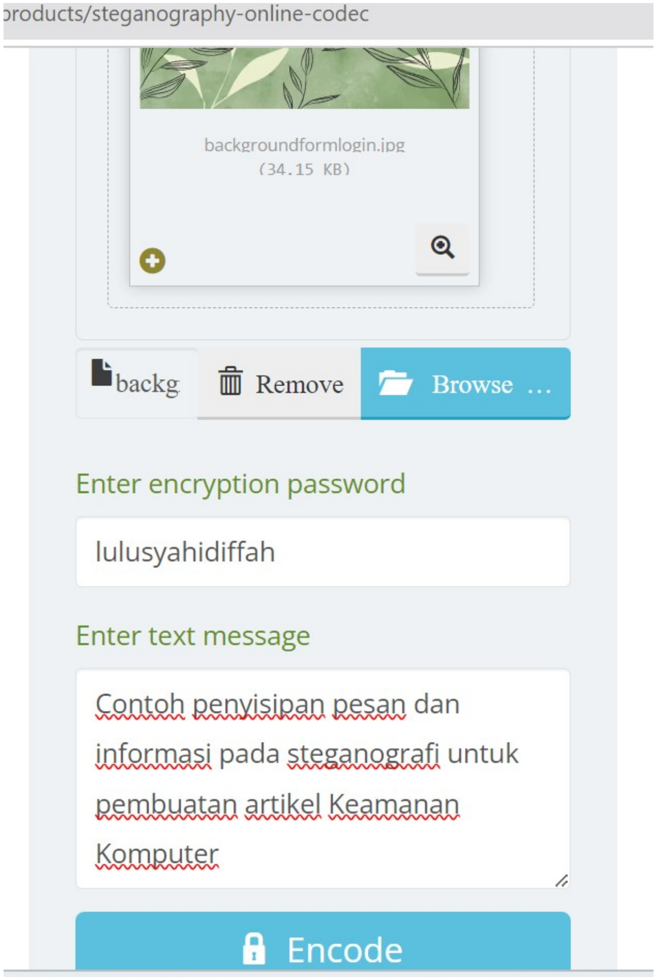
a) Data Hiding Capacity: evaluates data hiding capabilities across all media. Calculate the amount of data that can be entered without reducing media quality.
b) Steganography Detection: Test the method's robustness to steganography detection approaches by comparing detection performance on media including data.
c) Visual and Auditive Analysis: To ensure that data masking using the LSB method does not result in significant distortion or significant reduction in media quality, perform visual analysis of the image.

III. RESULT AND DISCUSSION

To keep information and messages secure, hidden text is used, which is similar to the purpose of Steganography. To use this method, Steganography requires a special application, and in this study we chose Pelock.

Steganographic analysis involves changing bits in each color byte in each pixel. This is done by replacing the bits of information you want to hide with the bits that currently exist. All data is considered to have been hidden successfully once all bits are included in the file. To reveal secret information, each modified part is taken and reassembled into complete information. The length of the secret data to be hidden is adjusted to determine the bits sequentially, starting from the first byte to the last byte. The changed byte value is only affected by the bit change, which does not affect sound or visual perception. The changed byte value is only slightly higher or lower than the previous value. Two processes, embedding and extraction, are used to analyze information embedding messages in images.

The research results of inserting information in an image that is used for information security can be seen on Figure 1 and Figure 2.



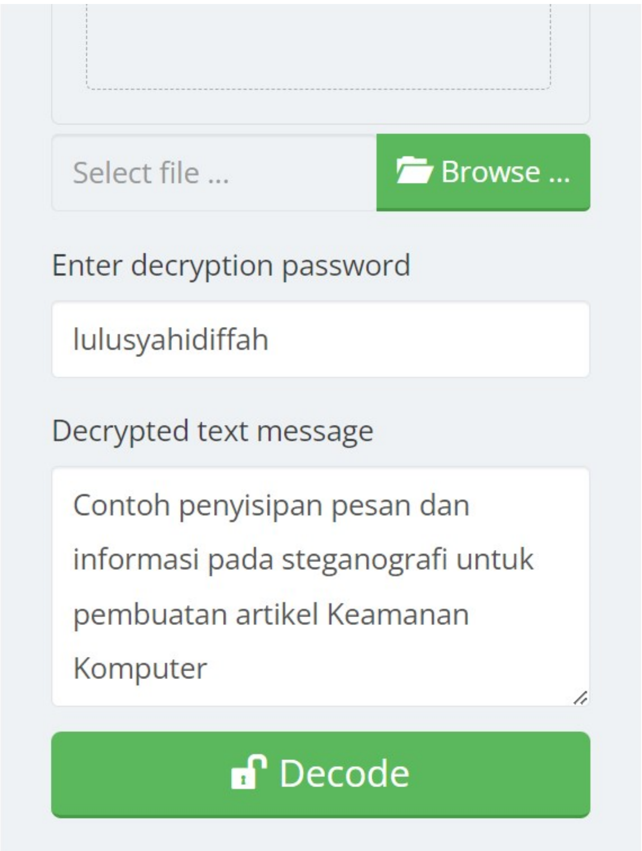
Enter encryption password

lulusyahidiffah

Enter text message

Contoh penyisipan pesan dan informasi pada steganografi untuk pembuatan artikel Keamanan Komputer

Fig. 1. Display Before Encoding



Enter decryption password

lulusyahidiffah

Decrypted text message

Contoh penyisipan pesan dan informasi pada steganografi untuk pembuatan artikel Keamanan Komputer

Fig. 2. Results After The Image is Decoded

For the quality of images that have had messages and information inserted and those that have not been inserted, please see on Figure 3 and Figure 4.

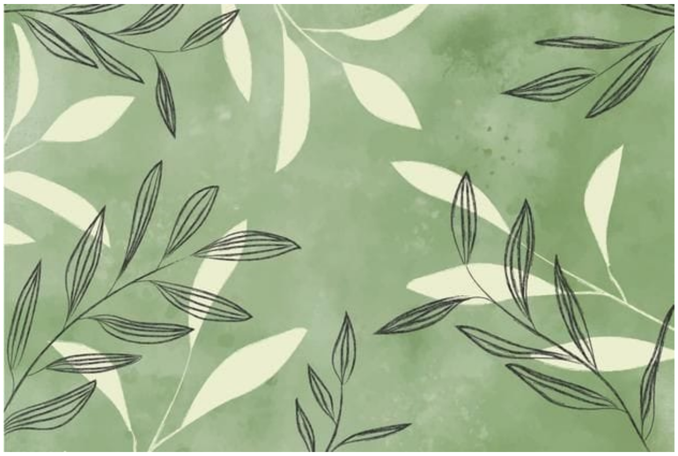


Fig. 3. Before Inserting Messages and Information

Fig. 4. After Inserting a Message and Information

IV. CONCLUTION

Steganography using the Least Significant Bit (LSB) method is very useful for someone who wants to store or provide messages and information to other people without data leaks. Apart from maintaining security, the process is also very easy to do, and the image quality is also very good.

Based on the results obtained, the author would like to provide suggestions to future researchers so that they can conduct research using applications, because in this research the author used a website. In addition, to increase message or information security, the author suggests future researchers to combine the steganography approach with a more secure cryptographic coding process, such as the RSA algorithm, which uses two keys.

REFERENCES

[1] Garno & Adam, RI. Skema Penyembunyian Data pada Gambar Berbasis Interpolasi Kubik B-Spline Menggunakan Metode Least Significant Bit (LSB). *Jurnal Edukasi dan Penelitian Informatika*, Vol. 5, No. 3, ISSN(e): 2548-9364 / ISSN(p) : 2460-0741. 2019.

[2] Ramadhani, A.M & Hasanuddin, T. Modifikasi Least Significant pada Gambar sebagai Data Hiding Steganography. *JURNAL SAINS DAN SENI ITS*, Vol. 8, No. 1 (2019), 2337-3520 (2301-928X Print). 2021.

[3] Azlansyah, M & Setiyono, B. Penyisipan Pesan Pada Citra Digital Menggunakan Metode Least Significant Bit. *Journal of Data and Science (IJODAS)*, Vol 2, No 2, July 2021, pp. 91-102, ISSN: 2715-9930. 2019.

[4] Setiawan, A.E. & Pasaribu, A. Penerapan Steganografi Pada Citra Digital Menggunakan Metode Least Significant Bit (LSB) Kombinasi RC4 Berbasis Mobile Android. *Journal h Journal of Informatics and Electrical Engineering*, Volume 2 Issue 1, p-ISSN: 2686-0139, e-ISSN: 2685-9556. (2020).

[5] Yanti, F & Budayawan, K. Implementasi Steganografi Menggunakan Metode Least Significant Bit (Lsb) dalam Pengamatan Informasi pada Citra Digital. *Jurnal Vocational Teknik Elektronika dan Informatika* , Vol. 11, No. 1, Maret 2023, P- ISSN: 2302-3295, E-ISSN : 2716-3989. 2023.

[6] Hafiz, A. Steganografi Berbasis Citra Digital Untuk Menyembunyikan Data Menggunakan Metode Least Significant Bit (LSB). *Jurnal Cendikia*, Vol. XVII Cendikia 2019, P-ISSN:0216-9436, E-ISSN:2622-6782. 2019.

[7] Ratnasari, A.P. & Dwiyanto, F.A. Metode steganografi citra digital. *Sains, Aplikasi, Komputasi dan Teknologi Informasi*, Vol 2, No 2, pp. 52-56, ISSN: 2684-8473. (2020)

[8] Nugroho, C. & Muslihudin. Steganografi Pada Pengiriman Teks Pesan Gambar dengan Metode Least Significant Bit & Steghide. *Jurnal Ilmu Siber*, Vol. 1, No. 4, ISSN(e): 2828-6065. (2022)

[9] Nirmala, E. Penerapan Steganografi File Gambar Menggunakan Metode Least Significant Bit (LSB) dan Algoritma Kriptografi Advanced Encryption Standard (AES) Berbasis Android. *Jurnal Informatika Universitas Pamulang*, Vol. 5, No. 1, ISSN: 2541-1004, e-ISSN: 2622-4615. (2020)

[10] Khan, S., & Ahmad, S. "Secure Audio Steganography Using LSB Substitution and Chaotic Maps." *Journal of Signal Processing Systems*, 94(2), 189-201. DOI: 10.1007/s11265-021-01750-5. 2022.