

## Implementation of Least Significant Bit Steganography to Secure Text Messages in Images

Wiyana Herra Herviana<sup>1\*</sup>, Djuniadi<sup>2</sup>

<sup>1</sup>Department of Computer Science, Universitas Negeri Semarang, Indonesia

<sup>2</sup>Department of Electrical Engineering, Universitas Negeri Semarang, Indonesia

DOI: <https://doi.org/10.52465/joiser.v2i2.438>

Received 27 July 2024; Accepted 30 July 2024; Available online 31 July 2024

### Article Info

#### Keywords:

Least significant bit;  
Text message security;  
Steganography

### Abstract

Steganography is a technique of securing secret messages in other messages that are not known. Simulation of the steganography method using the Least Significant Bit technique is used to change the last bit in one byte of data by using a text message as the container medium. This study aims to implement the security of text messages in images using the Least Significant Bit technique which is supported by the steganography method. Simulation techniques are used to conduct studies using Cryptool2 which can describe the concept of cryptography. The results obtained from this study regarding the security of text message insertion into an image in \*.jpg and \*.png format with 5 sampling trials are (1) the encrypted image cannot be distinguished directly through human eyes, (2) there is an increase in file size the image after being encrypted with an average for five trials is 0.31%, this increase depends on the length of the text message and a key to be inserted, the longer the insertion, the larger the resulting file size, (3) The higher the resolution of the image where the description encryption is inserted, the longer the process required, (4) The simulation time of steganographic decryption is faster than steganographic encryption. The decryption simulation process is the same as 50% of the encryption process.



This is an open-access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

## 1. Introduction

The rapid advancement of technology has had an impact on the way people live, such as in communicating with each other. This progress is supported by internet technology. Humans can easily exchange information via the internet by sending email messages or using online media platforms such as Instagram, Facebook, Twitter, Line, and WhatsApp [1]. One of the negative consequences along with technological advances is digital crime. Digital crime can target various sites, social media, and various computer programs so that it is very dangerous for various user activities, both agencies or individuals

### \* Corresponding Author:

Wiyana Herra Herviana,  
Department of Computer Science,  
Universitas Negeri Semarang,  
Semarang, Indonesia.  
Email: [wiyanherraherviana@gmail.com](mailto:wiyanherraherviana@gmail.com)

based on the internet. The threat of digital conflict can be secured by using a method to keep data confidential. There are two types of cryptography used in this simulation, namely modern cryptography and classic cryptography. In this simulation, the two cryptographic algorithms are combined to increase security in a message. Therefore, a technique is needed to hide the message so that it is not known by outsiders. This technique is steganography, which is a technique for hiding secret messages in other messages, making it difficult for outsiders to interpret the contents of the message [2].

Currently steganography is used to hide messages using digital media, namely image media as a connecting medium for humans to interact and communicate in conveying information [3]. Humans use images to share stories or experiences either directly or through other online media platforms. Therefore, images are chosen as the media capacity to hide messages in this simulation [4].

The method applied is Least Significant Bit which uses steganography techniques. This method hides messages in bit transformations on the final digits in byte units determining the text message for the media capacity to contain it [5], [6].

This simulation aims to implement and analyze encryption for embedding text messages in images through the application of the steganography method with the Least Significant Bit technique. Then get instant messages sent from sender to recipient by embedding instant messages into images using the \*.jpg and \*.png formats. The product used in the application of the steganography algorithm is cryptool2 software. Cryptool2 is open source software used in describing a cryptography concept [7].

Steganography has special properties as a space to hide secret messages that will later be hidden [8]. In general, the media required are videos, sounds, images, or texts that are used to hide secret messages. These messages can be in the form of images, program codes, texts, or other messages [9], [10].

There are several types of images that can be inserted in steganography algorithms, including [11]:

1. PNG is a type of information data created as another option with GIF design that utilizes LZW pressure calculations
2. JPG/JPEG is a type of data developed by JPEG which is already a standard for competent photographers.

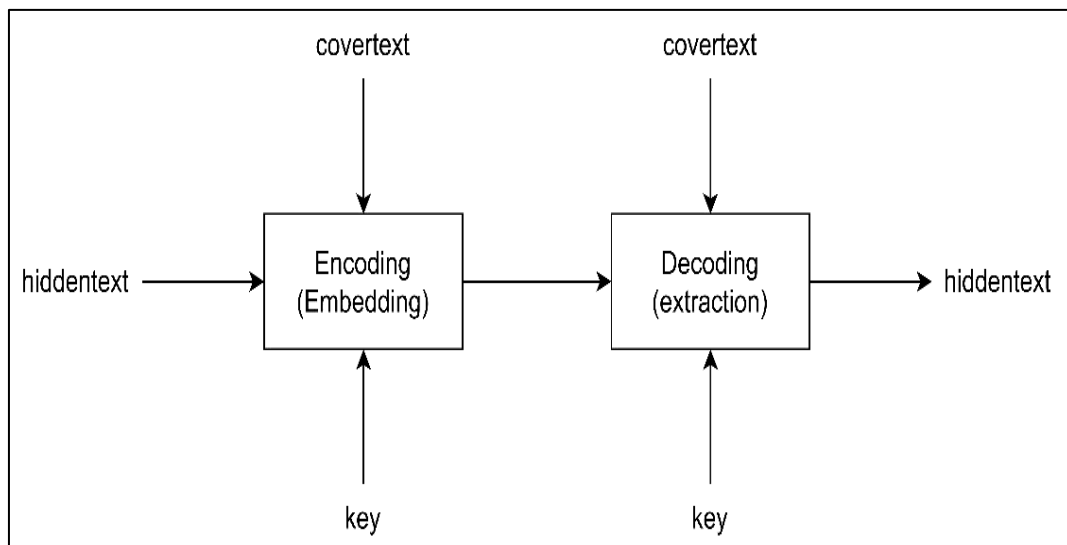


Figure 1. Steganography Properties [12]

Steganography has 3 criteria that need to be considered in order to hide text, sound or images as follows [13]:

1. Fidelity  
The quality is no different from the original where there is an insertion of a message with the results of this steganography actually looking good which does not affect the observer if there is a secret message in the image.
2. Robustness  
The hidden message will survive any manipulation later. If there is an image that performs an operation processing action then the data will not encounter any damage in it.

### 3. Recovery

The message that has been hidden can be returned with a steganographic purpose itself as data hiding. Therefore, when secret data is needed, the data can be used again for later follow-up.

## 2. Method

Encryption and description design in steganography in hiding text messages in images with the Least Significant Bit technique. The approach in this simulation uses quantitative methods and literature studies. The quantitative method uses experimental techniques as an analysis of input factors for further results with additional literature studies on hiding techniques (extraction and embedding) using the Least Significant Bit technique [14]. Experimental simulation is a type of exploration where analysts deliberately test objects contained in the software, then observe and record the results of the tests carried out by paying attention to their relationships [15]. This steganography simulation is completed by carrying out two processes, namely encryption and description. The most common method for embedding text messages in images is encryption while description is the extraction process used to remove text messages in images [16]. The test is used to study the workflow of a steganography algorithm at the time of encryption and description of text messages in images with the Least Significant Bit technique [17]. The following is a flowchart of encryption using Least Significant Bit in inserting text messages in images.

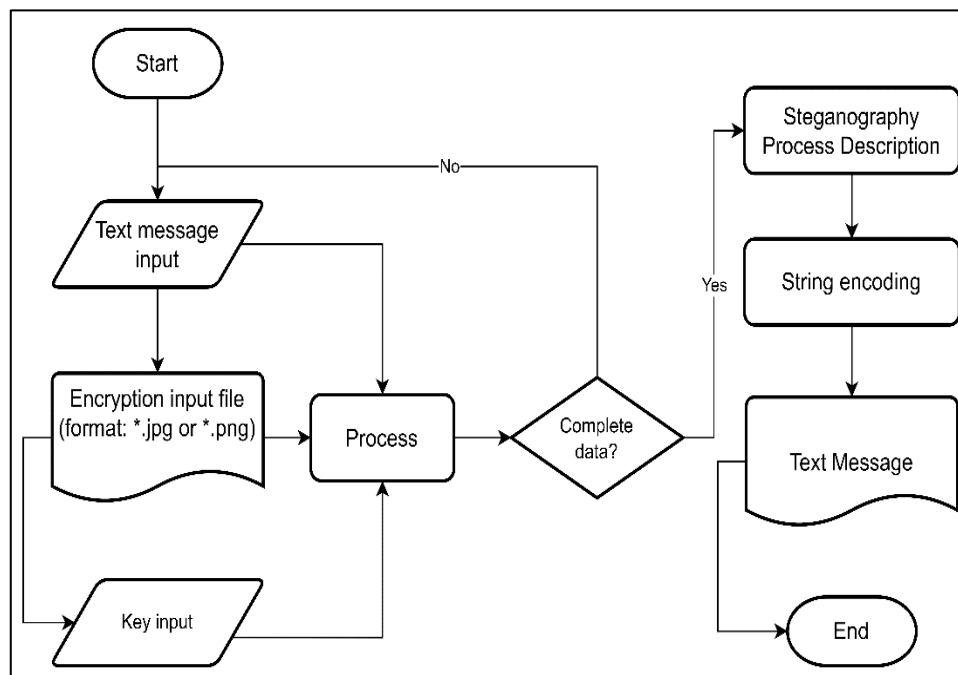


Figure 2. Steganography Encryption Flowchart

Look at Figure 2, the initial stage in completing the steganography encryption simulation process is by inputting a text message, inputting an image file in the form of \*.png or \*.jpg that has been previously determined and then inputting a key. After all the information is inputted, the following process will perform steganography encryption using the Least Significant Bit technique which produces an image in the form of \*.png or \*.jpg. The flowchart below illustrates the description of the steganography algorithm using the Least Significant Bit technique inserted into the text message.

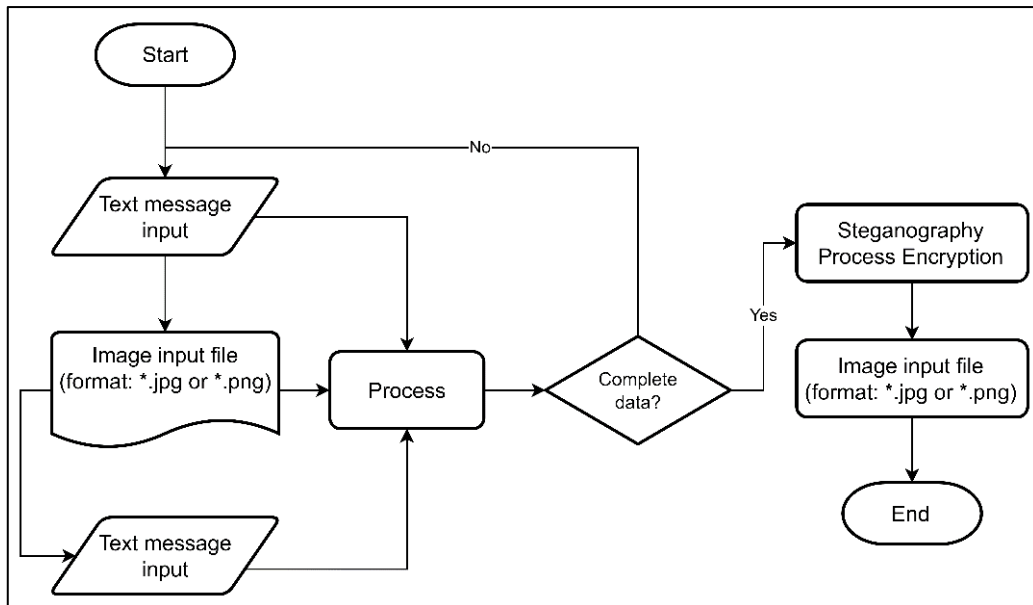


Figure 3. Flowchart of Steganography Description

In Figure 3, the secret message item in the image by entering the information file as a result of the steganography encryption image. Then, after all the data has been inputted, it is continued with the next process regarding the Least Significant Bit method which will later produce output in a text message.

### 3. Results and Discussion

Steganography encryption simulation using cryptool2 with the Least Significant Bit technique, requires several Tools/Properties, namely

1. Input text of two to insert a text message in an image. Then used to input a steganography key.
2. Input file is used to input images in the format: \*.png or \*.jpg.
3. Select one Least Significant Bit steganography whose action is encrypt and the output is in the format: \*.png or \*.jpg.
4. Output file used as a storage medium for an image file after steganography encryption is carried out in the form of \*.png or \*.jpg. The encryption simulation design can be seen in Figure 4.



Figure 4. Steganography Encryption Simulation Process

Steganography design using the Least Significant Bit technique based on cryptool2 as shown in Figure 5. There are several Tools/Properties required, including:

1. Text input of one is used to input a steganography key.
2. Input file of one is used to input an image that has been previously inserted into a text message in the format: \*.png or \*.jpg.
3. Input one Least Significant Bit Steganography whose action is decrypt (description) and the output is in the format: \*.png or \*.jpg.
4. Input one string encode is used to change a message into text.
5. Input one text output to display the contents of a text message from the steganography description simulation process.

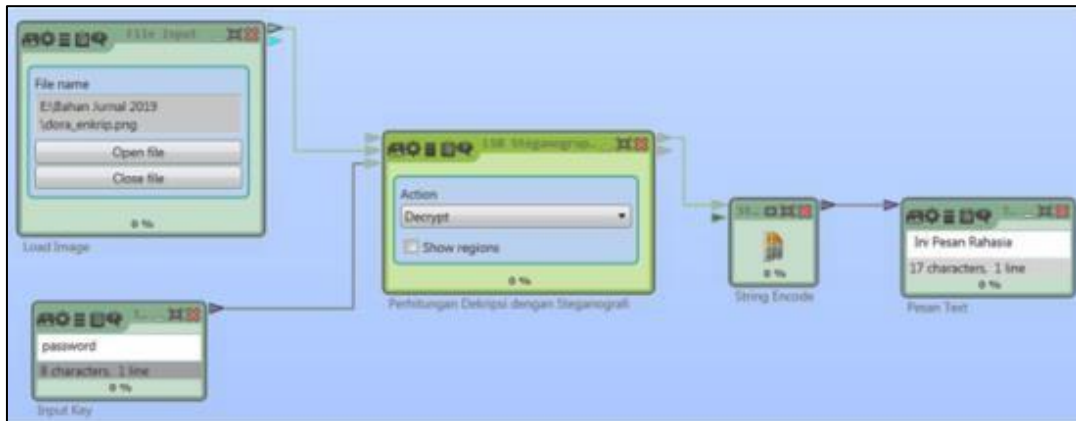


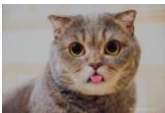
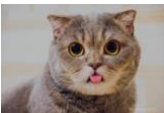
Figure 5. Steganography Description Simulation Process



Figure 6. Encryption Simulation and Steganography Description

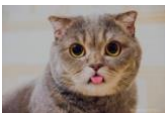
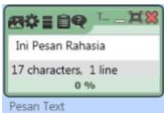
The encryption simulation process and steganography description can be seen in Figure 6. The study conducted is a trial of encryption simulation and steganography description with the Least Significant Bit technique based on cryptool2. The test was conducted by comparing the original image and the image that had been inserted with a text message previously with the Least Significant Bit technique.

Table 1. Results of Steganography Encryption Simulation Process Testing

		
Image	Original	Encryption Results
Text Message	-	<i>Ini Pesan Rahasia</i>
Key	-	password
Format	*.jpg	*.jpg
Image Resolution	451 x 300 pixels	451 x 300 pixels
Processing Size	24 KB	35 KB
Processing Time	5 second	

The results of the steganography encryption test simulation using the Cryptool2-based Least Significant Bit technique are shown in Table 1. Based on the data, there is a slight difference between the original image and the results after encryption using the \*.jpg format, the results of which cannot be seen directly through human vision. There is a difference in the size of the \*.jpg file which was originally 24 KB for the original image to 35 KB. The encrypted image has increased in size by 0.11%. The handling time to embed a text message in the original image into the image after encryption takes 5 seconds, while the image resolution is 300 pixels for height and 451 pixels for width. Next, the steganography description process is tested using the Cryptool2-based Least Significant Bit technique shown in Table 2. Based on the data in Table 2, it is very clear that the contents of the text message "This is a Secret Message" show the results shown in Cryptool2 in the 3-second process, much faster than the previous steganography encryption simulation.

Table 2. Results of Steganography Description Simulation Process Testing

		
Image	Encryption Results	-
Text Message	<i>Ini Pesan Rahasia</i>	<i>Ini Pesan Rahasia</i>
Key	password	-
Format	*.jpg	-
Image Resolution	451 x 300 pixels	-
Processing Size	35 KB	-
Processing Time	3 second	

Furthermore, the trial was conducted 5 times for each encryption process and steganography description with the Least Significant Bit technique in the \*.png image format, accompanied by a sampling test of 5 pieces. The test results are shown in Table 3.

Table 3. Sampling Test Results in the Steganography Encryption and Decryption Simulation Process

No.	Image		Steganography Encryption			Steganography Description	Processing Time (second)	
	Resolution (Pixels)	Image Size	Key	File size		Text Message		
				Original	Encryption Results			Processing Time (second)
1.	1051 x 1500	3R	password	110	141	0.082	<i>Ini Pesan Rahasia1</i>	0.041
2.	1205 x 1795	4R		121	152	0.132	<i>Ini Pesan Rahasia2</i>	0.066
3.	1500 x 2102	5R		143	174	0.971	<i>Ini Pesan Rahasia3</i>	0.486
4.	1795 x 2551	6R		165	196	2.421	<i>Ini Pesan Rahasia4</i>	1.211
5.	3300 x 5100	S11R		319	350	17.116	<i>Ini Pesan Rahasia5</i>	8.558

The results of the experiment showed that the first experiment the original file size was 110 KB after encryption increased to 141 KB, then the second experiment the original size of 121 KB increased to 152 KB, the third experiment the original size of 143 KB increased to 174 KB, the fourth experiment the original size of 165 KB increased to 196 KB and in the fifth experiment the original file size of 319 KB also increased to 350 KB. Then, in 5 times the sampling experiment of the encryption process and steganography description, the results obtained an average image size increase of 0.31%. This increase in file size depends on the length of the text message and a key that will be inserted. The longer the insertion, the larger the resulting file size will be.

#### 4. Conclusion

Based on the results of the steganography encryption and decryption tests using the Least Significant Bit technique with 5 sampling, the following conclusions can be drawn:

1. The image produced in the steganography encryption process using the Least Significant Bit technique is an image that cannot be distinguished directly through human vision.
2. There is an increase in the size of the image file between before and after encryption. Repeating 5 times the sampling experiment of the encryption and steganography description process, the results showed that the image size experienced an average increase of 0.31%. This increase in file size depends on the length of the text message and a key that will be inserted, the longer it will be inserted, the larger the resulting file size will be.
3. The higher the resolution of the image that will be encrypted and described, the longer the process required.
4. The simulation time of steganography decryption using the Least Significant Bit technique is much faster than steganography encryption. This is clearly seen from the test results, where the simulation process of decryption takes the same time as 50% of the encryption process time.

#### References

- [1] R. Fernando and R. R. Simanjuntak, "Digital Language Use in Bangka as Contribution to Digital Culture and Heritage," in E3S Web of Conferences, EDP Sciences, 2023, p. 4014.
- [2] T. A. Satrio, W. A. Prabowo, and T. Yuniati, "Hiding Document Format Files Using Video Steganography Techniques with Least Significant Bit Method," in 2022 IEEE International Conference on Communication, Networks and Satellite (COMNETSAT), IEEE, 2022, pp. 399–406.

- [3] C. Caesar, "Municipal land allocations: integrating planning and selection of developers while transferring public land for housing in Sweden," *Journal of housing and the built environment*, vol. 31, pp. 257–275, 2016.
- [4] D. Darwis, A. Junaidi, and D. A. Shofiana, "A new digital image steganography based on center embedded pixel positioning," *Cybernetics and Information Technologies*, vol. 21, no. 2, pp. 89–104, 2021.
- [5] B. Bakir and H. Hozairi, "Implementasi Metode Least Significant Bit (LSB) Dengan Enkripsi Cipher Caesar Pada Steganografi Menggunakan Image Processing," *JUSTINDO (Jurnal Sistem dan Teknologi Informasi Indonesia)*, vol. 3, no. 2, pp. 75–81, 2018.
- [6] D. A. A. Pertiwi and D. Djuniadi, "Simulations of text encryption and decryption by applying vertical bit rotation algorithm," *Journal of Soft Computing Exploration*, vol. 2, no. 2, pp. 61–66, 2021.
- [7] N. Kopal, "Solving Classical Ciphers with CrypTool 2.," in *HistoCrypt*, 2018, pp. 10–149.
- [8] S. Pramanik and R. P. Singh, "Role of steganography in security issues," *International Journal of Advance Research in Science and Engineering*, vol. 6, no. 1, pp. 1119–1124, 2017.
- [9] J. K. Su, F. Hartung, and B. Girod, "Digital watermarking of text, image, and video documents," *Comput Graph*, vol. 22, no. 6, pp. 687–695, 1998.
- [10] S. Bhattacharyya, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier," *Journal of global research in computer science*, vol. 2, no. 4, 2011.
- [11] T. Lestari, N. Nurmaesa, and A. R. Mariana, "Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image," *Jurnal Sisfotek Global*, vol. 7, no. 2, 2017.
- [12] N. Rismawati and M. F. Mulya, "Analisis dan Perancangan Simulasi Enkripsi dan Dekripsi pada Algoritma Steganografi untuk Penyisipan Pesan Text pada Image menggunakan Metode Least Significant Bit (LSB) Berbasis Cryptool2," *Faktor Exacta*, vol. 12, no. 2, pp. 132–144, 2019.
- [13] Y. Zhang et al., "A highly reliable encoding and decoding communication framework based on semantic information," *Digital Communications and Networks*, vol. 10, no. 3, pp. 509–518, 2024.
- [14] D. Darwis and N. B. Pamungkas, "Comparison of Least Significant Bit, Pixel Value Differencing, and Modulus Function on Steganography to Measure Image Quality, Storage Capacity, and Robustness," in *Journal of Physics: Conference Series*, IOP Publishing, 2021, p. 12039.
- [15] B. V. Indriyono, "Penerapan Keamanan Penyampaian Informasi Melalui Citra dengan Kriptografi Rijndael dan Steganografi LSB," *Creative Information Technology Journal*, vol. 3, no. 3, pp. 228–241, 2016.
- [16] K. N. Jassim et al., "Hybrid cryptography and steganography method to embed encrypted text message within image," in *Journal of Physics: Conference Series*, IOP Publishing, 2019, p. 12061.
- [17] G. Sugandhi and C. P. Subha, "Efficient steganography using least significant bit and encryption technique," in *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, IEEE, 2016, pp. 1–6.